



TechNet Augusta

August 19–23, 2019 | Augusta Marriott at the Convention Center | Augusta, GA

2019 SOLUTIONS SHOWCASE

#AFCEATechNet

AFCEA TechNet Augusta Solutions Reviews

AFCEA International is pleased to host TechNet Augusta to assist the military as it faces challenges from peer and near-peer adversaries not only on the sea and land as well as in the air but also in cyberspace. With assistance from the U.S. Army Cyber Center of Excellence and industry experts, the conference is designed to keep the lines of communication open among the cyber professionals who face complex tasks in training and maintaining the expertise required to protect and fight in numerous domains simultaneously.

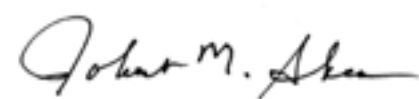
To bring industry into the discussion prior to TechNet Augusta 2019, the service identified the following areas as opportunities for the commercial sector to offer potential solutions for the best ways to achieve this goal. Companies were invited to offer their ideas about:

- **Advanced analytics** 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.
- **Low probability of detection/low probability of attribution** to enable signature masking and reduction.
- **Development of elastic compute, storage and services** to scale and tailor resources as dictated by mission requirements, which will be an important asset for success in future large-scale combat operations.
- **Development of tactical terminals utilizing digital RF** to reduce the overall footprint of the terminal/dish size while emulating the gain of larger dishes.
- **Enhance SATCOM resiliency** to enable SATCOM ground terminals to perform multi-beam operation with the ability to utilize LEO/MEO/GEO satellites both at the halt and on the move.
- **Low probability of intercept/low probability of detection** capabilities to reduce platform and electromagnetic signatures in all conditions and operating environments.
- **A more efficient encryption module** over current technologies in terms of reducing power, heat and costs to support up to secret classified voice and data tactical communications.
- **Man-portable electronic attack capability** to provide complementary capabilities to large EW systems deployed on trucks and aerial platforms.
- **Class III UAV Electronic Attack** so EW systems can continue sensing and collecting electromagnetic emissions while conducting electronic attack missions.
- **Small Form-Factor Long-Range Sensors** are needed to provide battlefield situational awareness to the commander.

AFCEA International received nearly 80 potential solutions to address these problem areas from a range of industry partners and conference participants. AFCEA reviewed and evaluated all of the submissions based on criteria such as innovation, potential effectiveness and maturity of solution. It selected several abstracts to be presented at the conference in a Solution Reviews format.

We encourage you to review these solutions to understand both the military's requirements and industry's creative approaches to address how to build a multi-domain force.

Sincerely,



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

Problem Statements

Advanced Analytics

Problem Statement 1: The Army requires advanced analytics utilizing/including 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 a 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 time to reconfigure, react to an adversary or change techniques and/or tools to support a mission. In addition, these advanced analytics would reduce the cognitive workload and manpower intensity of analytic functions. For example, cyber electromagnetic activity (CEMA) planners and the offensive and defensive cyberspace operators should not require data-scientist skills to accomplish their mission. Advanced analytics would enable autonomous active cyber operations and reduce the time gap between human reaction and dynamic threat response. The Army needs this capability to enable the military decision making process (MDMP) for multi-domain operations (MDO) to increase speed and responsiveness as well as pre-authorized/managed cyber payload deployment.

Cyberspace Modeling and Simulation

Problem Statement 2: The Army requires cyberspace modeling and simulation (M&S) in support of cyber mission planning, proficiency training, cyberspace operations (CO) 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. For example, the M&S capability must include a high fidelity of user activity and system interactions, both commercial and military, and generate realistic traffic. This traffic should include adversarial cyberspace effects, anomalous network activity and insider threats. M&S is necessary for cyberspace situational understanding (cyber SU) to blend seamlessly with mission/maneuver command for the military decision making process driving course of action (COA) analysis development. This is a time-dependent requirement for available staff planning and COA validation through modeling and simulation. Currently, ongoing M&S environments are 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 CO training. This will enable persistent cyber training integration with the synthetic training environment (STE).

Low Probability of Detection/Low Probability of Attribution

Problem Statement 3: The Army requires low probability of detection/low probability of attribution (LPD/LPA) enabling signature masking and reduction.

Why it is important: Force protection of tactical cyber mission forces (CMF) is required in a peer/near-peer fight in multi-domain battle to assure mission success. Protection capabilities will enable the CMF to screen/guard against adversary network defenders, and CMF capabilities enhanced with an automated identification of friend/foe can protect CMF actions in and through cyberspace to counter the cyber threat in front of friendly network boundaries. In addition, LPD/LPA capabilities enable cyberspace operations deception and counter infiltration actions.

Development of Elastic Compute, Storage and Services

Problem Statement 4: What progress has industry made toward the development of elastic compute, storage and services in a contested communications environment?

Why it is important: The U.S. recognizes that adversaries will contest all domains and U.S. dominance is not assured. Multi-domain formations will require the capacity, capability and endurance necessary to operate across multiple domains in contested spaces against a near-peer adversary. The ability to scale and tailor resources as dictated by mission requirements will be an important asset for success in future large-scale combat operations.

Developing Tactical Terminals Utilizing Digital RF

Problem Statement 5: What efforts are currently being made toward developing tactical terminals utilizing digital RF to reduce the overall footprint of the terminal/dish size while emulating the gain of larger dishes?

Why it is important: Commanders will require the ability to maneuver anywhere on the battlefield and maintain connectivity to the network without the need to stop and set up communications, which would make them vulnerable to attacks. Combat vehicles integrated with lower footprint terminals may be leveraged to provide the on-the-move communications, mission command and situational awareness that commanders need to lead from anywhere on the battlefield. Managing the trade space between terminal/dish transportability and operational and range effectiveness will be critical when balancing requirements and resources available.

Enhance SATCOM Resiliency

Problem Statement 6: What are the efforts/initiatives that industry is pursuing to enhance SATCOM resiliency so forces can perform in multi-domain operations? Describe your efforts in developing capabilities that will enable SATCOM ground terminals to perform multi-beam operation with the ability to utilize LEO/MEO/GEO satellites both at-the-halt and on-the-move.

Why it is important: Without a protected SATCOM capability, the warfighter will not be able to communicate effectively via SATCOM links in a contested (jamming) environment. U.S. forces will require options that provide protection against interference, either intentional or unintentional, in large-scale ground combat operations.

Low Probability of Detection/Low Probability of Intercept

Problem Statement 7: The Army requires communication systems with low probability of detection/low probability of intercept (LPD/LPI) capabilities to reduce platform and electromagnetic signature.

Why it is important: Force protection of tactical cyber mission forces (CMF) is required in a peer/near-peer fight in a multi-domain battle to assure mission success. LPD/LPI enables assured communication in all conditions and operating environments. It reduces electromagnetic signature when conducting military operations and conceals location when maneuvering to positions of advantage.

More Efficient Encryption Module

Problem Statement 8: The Army requires a more efficient (less power, heat and cost) encryption module over current technologies to support up to secret classified voice and data tactical communications.

Why it is important: A more efficient encryption module is required to decrease the cost of overall force modernization and sustainment and to reduce soldier load and heat signature of operating tactical communications in a peer/near-peer fight.

Man-Portable Electronic Attack

Problem Statement 9: The Army requires a man-portable electronic attack capability that can be easily transported and rapidly deployed.

Why it is important: Man-portable systems must be developed to provide complementary capabilities to large EW systems that are deployed on trucks and aerial platforms. These systems are inherently transportable over differing terrains with the supported soldiers and persistent in presence regardless of weather or other factors.

Class III UAV Electronic Attack

Problem Statement 10: The Army requires aerial electronic warfare (EW) systems capable of conducting simultaneous electronic attack (EA) and electronic warfare support (ES) from the same platform.

Why it is important: EW systems need to be able to continue sensing and collecting electromagnetic emissions while conducting EA (jamming) missions to maintain direction finding and continue to geo-locate the adversary for situational awareness and further targeting. Class III UASs operate at the brigade combat team level and provide aerial ISR. These systems also must integrate electronic attack capabilities.

Small Form-Factor Long Range Sensor

Problem Statement 11: The Army requires long-range EW sensors built in a small deployable form factor that can achieve ranges greater than 40 kilometers.

Why it is important: EW systems need form factors that are as small as possible and still provide battlefield situational awareness to the commander. The system must be transportable and deployable.

Table of Contents

Highlighted abstracts selected as presenters at conference as of August 9, 2019.

ADVANCED ANALYTICS

Cyber Common Operating Picture Jamie Miller, Protégé, All Points	13
Self-Service Data Analytics Chris Hauter, Federal Account Executive, Alteryx.....	15
Device Intelligence and Artificial Intelligence: The New Way Forward to Combat Cyber Threats on the Battlefield of the Future Liz Howard, Director, Federal Sales, Armis	16
Building Confidence and Trust in AI Systems Weiming Xiang, Assistant Professor, Augusta University	18
Quantum Cybersecurity Don Turner, DOD Global Sales Engineering Manager, Avaya Government Solutions.....	20
Leveraging End-To-End Invisible AI-Driven Cybersecurity to Enable Advanced Offensive and Defensive Cyberspace Operations Ken Tola, CEO, Bear Systems.....	21
Lessons in Advanced Analytics for Cyberspace at Scale Baron Rawlins, Cybersecurity Specialist, Cisco Systems.....	23
Sensitive Data Governance Gina Myers, Commvault.....	24
Artificial Intelligence Preparation of the Battlefield Stephanie Chenault, Chief Technology Officer, Corvus Consulting LLC.....	25
Balancing Zero Trust and Operational Expediency Kevin Jermyn, Federal Customer Success, CyberArk Software Inc.	27
Transforming Cyber Operations and Decision-Making with Cloud Analytics and AI/ML Daniel Prieto, Strategic Executive, Google Cloud Public Sector, Google	28
SIGINT at the Edge Using AI Jeff Winterich, DoD Account CT, Hewlett Packard Enterprise	30
Advanced Analytics Utilizing AI for Mission Analysis Andrew Edmondson, Principal Architect, U.S. Army Account, IBM	31

Bayesian Learning for Robust and Resilient Multi-Agent Control Lan Hoang, PhD, IBM Research	32
Using AI to Get Situational Awareness From Network Data Seraphin Calo, Distinguished Research Staff Member, IBM Research.....	33
AI for Modeling Cyber-Physical Object Movement at Scale Mudhakar Srivatsa, Distinguished Research Staff Member, IBM T.J. Watson Research Center	34
Employing AI and Analytics to Solve Digital Forensics Problems Across Multiple Domains Mary Anne (Harasim) DeHart, Director of Extended Enterprise, IntelliGenesis LLC	35
Multidomain Cyber Analytics-Driven Defense (MCAD) William Liu, Technical Director, LGS Innovations LLC, a wholly owned subsidiary of CACI Federal Inc.....	37
Cybersecurity Common Operating Picture Jamie Miller, CEO, Mission Multiplier	39
AI/ML/DL and Advanced Analytics: Whoever Owns the Data Is King Gregory Gardner, Chief Architect, Defense and Intelligence, NetApp	41
AI Development Principles for Army Missions Michael O’Brien, Algorithmic Warfare Unit Lead, Northrop Grumman	43
Advanced Identity Analytics to Integrate AI With Cyber Operations Andrew Whelchel, Principal Solutions Engineer, Okta	44
Asymmetric Advantage in Battlefield AI Roger Morin, Solutions Architect and Inventor, Phacil LLC	46
Inverse Properties to Create Cyber AI Matthew Maher, Lead Data Scientist, Processus Group and Corvus Consulting.....	48
Cyber Data Hub for Analytics and AI Zach Duncan, FlashBlade Specialist, DoD, Pure Storage	49
Autonomic Vulnerability and Compliance Suite Advanced Analytics Utilizing Artificial Intelligence Margaret Margle, Senior Executive Director, Sabre Systems Inc.	50
Digital Information Common Operating Picture (DICOP) Mark Campbell, Chief Marketing Officer, Sc2 Corp	52
AI Tools Deliver Faster, Better Decisions for Defense and Offense Ray Cruciana, Security Specialist, Splunk	54
Accelerating Cybersecurity With AI-Based Advanced Analytics Bradley Ward, Senior Director, U.S. Army Cybersecurity Solutions, Symantec	56
Vulnerability Analysis Using Machine Learning Zach Bennefield, Senior Security Engineer, Tenable.....	58

Expediting Operational AI With Automated, Self-Service Data Prep Brian Shealey, Director - DoD/IC, Trifact.....	59
The Intelligent Edge with 4G/5G: Using MEC to Meet the Mission Grant O’Brien, Manager, Federal Marketing, Verizon.....	60
Integrating the Analyst, the Logic and the Machine Into Defensive Cyberspace Operations Philip Mar, Vice President/CTO Gouvernement Systems, Viasat Inc.....	61
The Modernization of Protection Beyond the Firewall With AI Mike Price, Chief Technology Officer, ZeroFOX	63

CYBERSPACE MODELING AND SIMULATION

Cyberspace Modeling Using the Object Process Methodology Ahmad Jbara, Assistant Professor, Augusta University	66
SMEIR Ashley Furuta, Business Development Manager, IDS International	68
Modeling and Simulation of ICS Environments for Cyber Situational Understanding Mary Anne (Harasim) DeHart, Director of Extended Enterprise, IntelliGenesis LLC	69
Deeper Analysis Capability at the Speed of Cyber Jeremy Martin, Senior Solution Architect, NexTech Solutions.....	71
Cyber Operational Risk Tool (CORT) Geoffrey Embrey, Director of Army Programs, Noetic Strategies	73
Develop a Knowledge Graph of Spectral Data Matthew Maher, Lead Data Scientist, Processus Group and Corvus Consulting.....	75
GHOSTS, GreyBox and Other Tools to Enhance Exercise Realism Tyler Brooks, Cyber Security Engineer: Exercise Developer, Software Engineering Institute	76
State-of-the-Art Modeling and Simulation (M&S) Supports Mission Planning, Training Melissa Andrews, Staff Engineer, Splunk.....	77
Smart Base Network Interoperability with 5G Grant O’Brien, Manager, Federal Marketing, Verizon.....	78

LOW PROBABILITY OF DETECTION/LOW PROBABILITY OF ATTRIBUTION

Low Probability of Detection/Low Probability of Attribution Assurance Ron Chang, Public Sector, DoD Account Executive, BluVector.....	80
Conducting Secure Cyber Missions Using Network Obfuscation and Managed Attribution Tom Badders, Senior Product Manager, Telos	82

DEVELOPMENT OF ELASTIC COMPUTE, STORAGE AND SERVICES

Leveraging AWS’ Hyperscale Cloud for On-Demand Scalability and Elasticity Mike Colson, DoD Solutions Architect Manager, Amazon Web Services (AWS)	84
Modular Enterprise-Grade Computing Power and Scale for the Tactical Edge Duncan Stewart, Director of Strategic Development, Axellio Inc.....	86
High-Performance Edge Computing in a DIL and Contested Environment Bill Burnham, Chief Technology Officer, Public Sector, Hewlett Packard Enterprise.....	88
Recognizing and Adjusting Data Services in a Contested Communications Environment Brent White, Data Analytics Specialist, Iron Bow Technologies.....	89
Advanced Multi-Domain Cyber-Comms for Contested Tactical Environments Harris Nussbaum, Solutions Architect, Mission Solutions Group	91
Building a Resilient, Unified and Scalable Data Platform Ben Ogden, Architect, MongoDB.....	93
Multi-Domain Data Management in a Contested Communications Environment Gregory Gardner, Chief Architect, Defense and Intelligence, NetApp	95
Advancing Cloud Services in Contested Environment Using Secure Cloud Identity Andrew Whelchel, Principal Solutions Engineer, Okta	98
PacStar Modular Data Center Charlie Kawasaki, Chief Technical Officer, PacStar	100
Mobile Cloud Storage and Compute Advantage Nick Hopchak, Vice President, Phacil LLC	102
Defending Data in a Perimeter-less Domain Rick Tyrell, Senior Systems Engineer, Thales eSecurity.....	104
Enabling Multi-Domain Dominance: Deploying the Next of Generation Virtualization Capabilities Matt Holt, Army Account Executive, Trace Systems Inc.....	106

DEVELOPING TACTICAL TERMINALS UTILIZING DIGITAL RF

Understanding Electromagnetic Operations Framework to Address LPD/LPI
Sgt. Maj. Raymond Reyes, USA (Ret.), Chief Information and Business Development
Officer, Corvus Consulting LLC..... 109

Reduced Footprint Terminals
George Khoury, CTO, Government Services, Viasat Inc. 110

ENHANCE SATCOM RESILIENCY

Moving From Purpose-Built Communications and Data Analytics Products to
Virtualized Applications
Michael Beeler, Vice President, Waveform and Analytics Virtualization,
Envistacom LLC 113

Enhancing Resiliency via Enterprise Management and Control and DSSS
Protected Waveforms
Mark Dale, Business Development Director, Kratos RT Logic 115

Resilient Hybrid Adaptive Networking
Craig Miller, Vice President, Chief Technology Officer, Viasat..... 117

LOW PROBABILITY OF DETECTION/LOW PROBABILITY
OF INTERCEPT

Information Theoretic Secure VPN
Daniel Kay, Senior Director, Cyber Reliant Corporation 120

Secure Comms in a Zero Trust Environment
Herm Hasken, Partner and Senior Strategy Officer, MarkPoint Technologies LLC 121

Smartphones Could Compromise the Mission
Mike Fong, CEO and Founder, Privoro..... 122

A New Approach to LPD/LPI SATCOM
Lawrence Kingsley, SATCOM Systems Engineer, Viasat Inc..... 123

MORE EFFICIENT ENCRYPTION MODULE

Enabling Efficient Communication Protection Across Multiple Types of
Communication
Ken Tola, CEO, Bear Systems..... 126

Data-Protected Secure Communications
Daniel Kay, Senior Director, Cyber Reliant Corporation 128

21st Century Cryptography
Dylan Hand, Senior Hardware Research Engineer, Galois Inc. 130

SoCrypt: High Assurance Software Cryptography for SWaP-C Constrained
Applications
Hal Aldridge, CEO, Secmation 132

Data File-Centric Security
Richard Streeter, Senior Technology Consultant, Sertainty Inc..... 134

Efficient Encryption for the Tactical Edge
John Jaworski, Embedded Security Technical Lead, Viasat..... 136

MAN-PORTABLE ELECTRONIC ATTACK

CLASS III UAV ELECTRONIC ATTACK

Converged RF Solutions
Shane Clark, Scientist, BAE Systems 138

SMALL FORM-FACTOR LONG RANGE SENSOR

Emergent Microelectronic Technologies Enable New Paradigms for Small
Factor EW Payloads
Benjamin McMahon, Technology Development Manager, BAE Systems 141

CEMA Tactical Awareness Support Kit
Herm Hasken, Partner and Senior Strategy Officer, MarkPoint Technologies LLC 143

Lighter Than Air, Small Form, Hyper Range
Jonathan J. Gollogly, Principal Consultant, Microsoft 144

Fleet Defense: Powered and Unpowered Submersible Drones
Jonathan J. Gollogly, Principal Consultant, Microsoft 145

ADVANCED ANALYTICS

Cyber Common Operating Picture

Jamie Miller, Protégé, All Points • jmiller@missionmultiplier.com

ABSTRACT

All Points brings truly differentiated services in the area of cyber continuous monitoring and risk scoring/benchmarking. The company collaborated to develop an innovative solution called MI:COP that can present an accurate cyber “Common Operating Picture” that successfully has been recently deployed at NASA Marshall Space Flight Center. The MI:COP solution is unique in that it is focused on changing the behavior of cybersecurity practitioners by incentivizing them to pay attention to advanced analytics, or key effectiveness measures through risk scoring, implementation of a risk scoring dashboard and adoption of an overall “risk economy.”

The MI:COP solution is built on the philosophy that not all IT assets are created equal; organizational leaders should be tracking key data analytics related to those key IT assets (or key cyber terrain) and using real-time data through automated technology to inform more effective and efficient risk management decision-making.

All Points achieves this goal by first working to identify the key IT assets within the organization and defining analytics or effectiveness measures that are measurable, actionable and meaningful to the organization. Simultaneously, the company works to ensure that each organization possesses the tools/technology to collect that data/analytics that is needed to support the defined metrics. To normalize the data collected from the different automated tools, All Points leverages a common framework and nomenclature called secure content automated protocol (SCAP). Where SCAP does not currently support existing tools, the company can develop the custom SCAP through the Open Checklist Interactive Language. Using SCAP more easily enables an “apple-to-apples” comparison, which is not easily achieved when collecting data from different tools.

The data collected from the different sensors in the IT environment is then captured in a data warehouse where All Points runs tailored queries that help to generate the defined analytics or effectiveness measures. The information from the database is ultimately used to support the development of a dynamic risk scoring dashboard—the front-end of the MI:COP solution. The dashboard scores and tracks progress at the enterprise level and also enables the user to drill down to unique grades at the business unit level and even the specific IT system level. The dashboard results are updated in real-time based on the cadence of each scan coming from the different sensors.

The end result of MI:COP implementation is a customized and automated risk scoring solution that ties together data feeds from automated IT security scanning technologies to drive changes in the behavior of IT security practitioners, tying known vulnerabilities to risk scores at both the organization and individual level to focus on mitigating the “highest risks first.”

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

Miller possesses more than 19 years of experience and is a proven thought leader who 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. Miller's innovative cyber solutions—to include 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 was awarded the 2016 Emerging Entrepreneur of the Year by Innovate Huntsville and was nominated for the prestigious Russell G. Brown Award by the Huntsville Chamber in 2017, 2018 and 2019. He was most recently a finalist as Entrepreneur of the Year as part of the 2018 Economic Development Partnership of Alabama (EDPA) immerge Innovation Awards. He is a regular speaker at information security industry leading conferences (e.g., FOSE, GFIRST) and has published several industry articles, most recently writing about shared risk for the *Security* magazine.

Miller serves on the board of directors for Cyber Huntsville, a Tennessee Valley Initiative; CyberReach; and the Southeastern Cyber Security Foundation; and also serves as the National Cyber Summit Program co-chair. Miller is a proud member of the Leadership Huntsville Class of 29 and Focus Class 31. He holds an MBA in consulting from Thunderbird School of Global Management and a BA in international studies from American University.

Self-Service Data Analytics

Chris Hauter, Federal Account Executive, Alteryx • chauter@alteryx.com

ABSTRACT

The emergence of data as a strategic asset has transformed the scale and velocity at which data analytics needs to be applied to create actionable intelligence. In organizations like the U.S. Army, the imperative to develop insights from data in its multiple forms, different structure and quality is even more critical. The scope and sheer volume of data that needs analysis will quickly tax the brightest and most capable military or civilian analyst. There has been a lot of talk about how the infusion of artificial intelligence (AI) and machine learning (ML) will help balance the equation and augment human capability. While this has been the case, applying AI and ML capabilities has also come at the cost of needing to deploy scarce classically trained data scientists and complicated data models to fully leverage these capabilities.

With the availability self-service Assisted Modeling from Alteryx, the power of machine learning belongs to everyone. Now, even the least technical non-data scientist can build trustworthy predictive models without extensive training or specialty software.

Imagine the ability to break analytic barriers and answer new questions deployed to all an organization's analysts. Assisted Modeling can walk an analytic team through the process of building predictive models quickly and without coding. Dirty data, unstructured data from every source imaginable can now be transformed into forward-thinking models that can be leveraged to create new levels of insight.

Assisted Modeling amplifies the capabilities of analysts and data workers, delivering explainable AI and ML workflows in a code-free environment. Recognizing that a pervasive talent gap exists between data scientists and data workers in the line of business, Assisted Modeling helps teach data science with a guided walk-through and aims to help all data workers, regardless of technical acumen, advance their skill sets in the process of building machine learning models.

The availability self-service Assisted Modeling will guide analysts through the process of building machine learning models without extensive training, so they can better support critical missions with speed and scale.

While these AI and ML models enhance analytic horsepower, human-based resources remain in control. The guided data transformation process puts the organization's analysts in control of key decisions and visual comparisons making it easy to choose the right path as well as explain the finished model.

With Assisted Modeling, the human is kept at the center of analytic intelligence. The approach in building Assisted Modeling is to advance the skills of the data worker or analyst—civilian or uniformed—creating the next-level “citizen data scientists” who can build the AI and ML models required to tackle the advanced analytic challenges facing the U.S. Army with unprecedented speed and confidence.

Device Intelligence and Artificial Intelligence: The New Way Forward to Combat Cyber Threats on the Battlefield of the Future

Liz Howard, Director, Federal Sales, Armis • liz.howard@armis.com

ABSTRACT

The U.S. Army relies on a massive and growing network of systems, connected devices and sensors for everything from communications, operations and maintenance to industrial control and advanced weapons systems management. These range from high-risk defense systems and weapons to connected soldiers back to the connected infrastructure, smart buildings, as well as data centers—all bringing new data, intelligence and advantage from the front lines to the command center.

However, these devices are under constant attack by hostile nation-states, cyber criminals and even hacktivists. The sophistication of these attacks is unlike anything experienced by the private sector and their volume and velocity make reliance on human cyber defenders a risk to warfighters and national security. Unfortunately, adversaries have an advantage that must be defended against: Many of these new connected devices have no inherent security.

In a world where cyberattack resilience now requires an autonomous cyber defense strategy, the nation needs a new approach. The foundation of this strategy is based on three critical pillars. First, it needs to be agentless. This is the only way to address the breadth and scale of all the devices the U.S. Army is adding. Second, it must identify every device in an environment, whether that be on the battlefield or in an office building and include the ability to see any device on or off the network as well as identify direct device-to-device interaction. The third pillar is the ability to correlate the device and its activity, then determine if it is behaving in a suspicious or malicious manner.

The only way to achieve this third pillar is through advanced machine learning and artificial intelligence (AI), which enables at-scale, continuous and automated decision making. This new way forward in cyber defense is the only approach to support and secure the growing number of connected devices and technological advances expected on the battlefield of the future.

Such a platform evaluates device characteristics and behaviors on a massive scale, and it can inform threat defense systems about what it learns. These systems can then use that information for automatic threat identification and isolation, thereby reducing the workload and manpower needed to keep high-risk systems and devices secure while increasing the security posture.

Armis Co-founder and CTO Nadir Izrael will explain the explosive growth of connected devices from the battlefield to the command center to the office. Device intelligence and AI enables users to see every device in different environments, analyze their behavior and connection history and identify threats and attacks. AI helps keep devices and warfighters safe from cyber attacks, and a massive device behavioral knowledge base and AI can help cyber defense teams stay ahead of threats that could imperil national security.

BIO: Nadir Izrael guides the technology vision behind Armis. He has assembled a deep bench of top-tier technologists. He works directly with security teams across all segments from manufacturing to health care to retail to finance to government and more. Before Armis, Izrael worked at Google as a senior software manager.

Building Confidence and Trust in AI Systems

Weiming Xiang, Assistant Professor, Augusta University • xiangwming@gmail.com

ABSTRACT

Artificial intelligence (AI) and machine learning (ML) techniques are efficient in solving complex problems. Recent advances in AI techniques are radically changing the landscape of the military and intelligence community, but the vulnerability of AI systems against adversarial attacks and uncertainties in runtime operation restrict the applicability of AI technologies in security-focused and safety-critical systems.

As has been often observed in deep neural network applications, even well-trained neural networks are sometimes very sensitive to input perturbations and might react in unexpected and incorrect ways to even slight changes of their inputs. In other words, neural network systems can be easily fooled by simple adversarial attacks and faulty outputs could be produced if the input to the network is subject to slight changes in run time, even if it works well in design time. An ideal AI system should not only be efficient in solving complex problems but also invulnerable to adversarial attacks and robust to uncertainties.

Building confidence and trust in AI systems will lead to reliability, robustness, security and safety in systems embedded with AI/ML components. One key question for building confidence and trust in AI systems is: How can we determine if a given AI system satisfies certain properties regarding reliability, robustness, security and safety? Once this question can be answered, confidence and trust will be built for the AI system in use.

Augusta University explores:

- The overview and challenges of building confidence and trust in AI systems.
- How to use formal methods such as geometric and reachability, optimization-based methods in verification of AI systems, particularly in deep neural networks.
- How to employ those advanced verification techniques to build confidence and trust in engineering systems embedded with AI components, for instance, cyber-physical systems with neural network controllers in the loop.
- Future challenges besides verification of AI systems, such as robust design/training AI systems, falsification of AI systems and performance-guaranteed model reduction for AI systems.

A number of open unsolved problems exist in both theory and applications regarding security and safety in AI, which is one strong bottleneck for AI techniques to be used in security-focused and safety-critical systems. Augusta University's solution aims to provide theoretic fundamentals and technical tools in verification of AI systems, which helps to build confident and trustworthy AI systems.

BIO: Dr. Weiming Xiang is an assistant professor in the School of Computer and Cyber Sciences at Augusta University. He was a postdoctoral research scholar in the department of electrical engineering and computer science at Vanderbilt University from August 2016 to August 2019. Before joining Vanderbilt University, Xiang worked as a postdoctoral research associate in the department of computer science and engineering at the University of Texas at Arlington from November 2015 to August 2016 and a research associate in the department of mechanical engineering at the University of Hong Kong from May 2015 to October 2015.

Xiang's research interest is developing formal synthesis and verification techniques and software tools for cyber-physical systems (CPS). His current research centers on formal methods on the safety, security and reliability of learning-enabled CPS. He is also broadly interested in methods and applications across CPS domains, such as control synthesis, stability analysis, reachable set computation, hybrid systems, power and energy, transportation, fuzzy logic and neural networks. Xiang has published more than 100 papers on these methods and their applications. Xiang was an associate editor of neurocomputing and is the leading guest editor of *Special Issue: Recent Advances in Control and Verification for Hybrid Systems in IET Control Theory and Applications*. Xiang is an IEEE Senior Member.

Quantum Cybersecurity

Don Turner, DOD Global Sales Engineering Manager, Avaya Government Solutions • turnerd@avaya.com

ABSTRACT

Quantum computers will be capable of performing certain types of calculations that are simply inconceivable with today’s conventional computers. Unfortunately, the emergence of this computational power will present an exponential threat to the most widely used information security encryption algorithms. Avaya offers some of the leading technologies and proposed solutions that can be deployed to build a near-term defense against these new emerging threats.

BIO: Don Turner is currently the Defense Department Sales Engineering Manager at Avaya Government Solutions. The sales engineering team provides technical guidance to Defense Department customers worldwide. Turner’s key role is to evangelize technology trends and industry-wide shifts to create engaging, collaborative solutions for audio, web and video technologies that meet the demanding security requirements of the U.S. Defense Department.

Leveraging End-To-End Invisible AI-Driven Cybersecurity to Enable Advanced Offensive and Defensive Cyberspace Operations

Ken Tola, CEO, Bear Systems • ktola@bear.systems

ABSTRACT

Bear Systems provides a different type of cybersecurity—device-level ethernet communications control that stops hackers at the point of attack, eliminates zero-day concepts and secures devices and device communications.

The volume and velocity of complex attacks in Army systems span across more than just one device or even a single system, exceeding humans’ ability to effectively provide timely counter-measures. The complexity and depth of attacks also often precludes any realistic chance of proactive detection.

Bear Systems enables ubiquitous coverage across all devices (enterprise, connected sensors, IoT, IoBT, etc.) and unifies security across any type of network through a universal visual platform that empowers non-cybersecurity experts to both defend and counter-attack in cyberspace.

Bear’s solution has been built specifically to reduce attack detection complexity at the device level and to leverage this capability to detect patterns of activity that might indicate more widespread attacks before those attacks occur. It enables AI-driven automation to proactively adapt against attack vectors and transparently protect the massive growing number of connected devices against emergent threats, while empowering non-cybersecurity personnel to manage complex security environments.

Bear’s solution places full security on every device, fundamentally changing how cybersecurity is managed. The company’s solution enables distributed, lightweight, blockchain-protected, AI-driven device protection, advanced remediation capabilities and device management for powerful next-generation device and data communications protection and control, including seamless, real-time, counter-strike capabilities.

Utilizing lessons coming out of DARPA work to detect new patterns of activity, the system drives true end-to-end AI and machine learning that becomes increasingly efficient at scale. This multi-tiered machine learning normalizes data at the point of collection to eliminate noise and localize remediation responses for much more rapid responses. These higher-level functions interact with human operators through a series of intent-based rules to allow operators to control parameters of the AI system and determine when the AI should ask for help, or permission, while still allowing the distributed AI system to drive automated responses.

All actions occur through a series of policy-driven workflow controls to provide flexibility and control over every aspects of the Bear system—from individual operations on each device to local domain controller actions to multi-domain operations. Actions are not limited to defensive remediation because Bear’s solution operates at a sufficiently low level in device communications that Bear can redirect incoming attacks

without the attacker being aware of redirection. This ability supports real-time tracebacks, honey pots, dark webs and other counterstrike capabilities.

Going further, the company can capture malicious applications the instant unauthorized attempts to receive or send any packets of information are initiated. Unlike anything else available, Bear can instantly isolate and virtualize the environment of suspected malicious processes. Without taking down operations, Bear’s solution effectively removes the threat and enables subsequent cybersecurity analysis and remediation when Army operators are ready to do so.

And, unlike bolt-on predecessors, Bear’s innovative distributed true end-to-end AI system automates complex remediation and counterstrike capabilities throughout the Army’s enterprise systems and distributed environments like the IoBT.

BIO: Ken Tola started out in Washington, D.C. as a neuropsychologist prior to moving into IT in the late 1990s. Tola ran a division at Honeywell-TSI, modernized Cambridge Associates and then moved into government work under Tommy Thompson while helping to build out the HSS Command Center. He then went over to the Department of State where he re-architected the U.S. Visa and Passport Systems.

After leaving the State Department, Tola realized that cybersecurity was broken and, in 2008, he began a long journey to fixing this problem. During this journey, he accumulated numerous patents across the cybersecurity, privacy and AdTech markets.

Tola is an ardent supporter of veterans having experienced their sacrifice firsthand while a neuropsychologist at the Washington VA. As CEO of Bear Systems, he currently employs several veterans in prominent executive roles in his company.

Lessons in Advanced Analytics for Cyberspace at Scale

Baron Rawlins, Cybersecurity Specialist, Cisco Systems • barawlin@cisco.com

ABSTRACT

Over the past 12 years, Cisco has published more than 50 academic papers on the topic of cybersecurity analytics and a multitude of open source. The company has done this because it believes this area of study must remain transparent and open.

Having said that, getting a good grade on a paper and being effective on the battlefield of the Internet is very different. Taking concepts from academic research and then applying it in the world, at scale and against real nation-state threat actors in play, is something the company thinks it has done well.

Sharing this experience is important because if Cisco can save anyone time and resources, it has added value to the fight. The team that took the academic research of Encrypted Traffic Analytics to production would like to share the do’s and don’t’s of machine learning, point out unique requirements in cybersecurity analytics versus others and share a very pragmatic criteria for applying the most advanced analytics to cyberspace operations. This information would be appropriate for professionals with hands-on data science experience or those who are just interested in outcomes. The experts in the Advanced Threat Group at Cisco are working every day to bring machine-scale observations down to human-scale understanding.

BIO: Cisco’s Sunil Amin is the principal engineer and former chief scientist for Lancope/Stealthwatch, and TK Keanini is a distinguished engineer and former CTO for Lancope/Stealthwatch.

Sensitive Data Governance

Gina Myers, Commvault • gmyers@commvault.com

ABSTRACT

Managing confidential or sensitive data is a struggle for most organizations. Confidential and sensitive data includes personal data (PII), financial data and health and clinical information (HIPAA). No matter the type of data, it is important to have a data governance strategy. Data is an organization’s most strategic asset, but it also is the organization’s responsibility to manage and protect against as well as minimize threats to that data. Discover how Commvault’s customers are managing their confidential and sensitive data through a sensitive data governance strategy.

This session will cover the following topics:

- Protecting and managing sensitive data in any environment
- Minimizing data risks
- Providing Proof of Compliance
- Centralizing the search index

Artificial Intelligence Preparation of the Battlefield

Stephanie Chenault, Chief Technology Officer, Corvus Consulting LLC •

stephanie.chenault@corvusgroup.org

ABSTRACT

The U.S. Defense Department lags the hype cycle for artificial intelligence, machine/deep learning and implementations like natural language processing by years. It needs to uncover the root causes contributing to this delay and create winning strategies to overcome institutional obstacles to get ahead of industrial partners and adversaries who are further along the adoption curve.

Possessing technology is neither deterministic nor decisive when waging war. The effective employment and deliberate application of technologies to enhance warfighting capabilities implies advantage over an adversary when suitably coupled with offensive and defensive tactics.

With the big data bang of the 2000s, a global need arose to create sophisticated computational models and deploy new tools to better understand massive volumes of information. It is now a prevailing urgency to spin international data saturation into financial gold on an industrial scale. Having tremendous purchasing power, the military is in a position to shape new technologies to its needs.

One cause for the holdup is that the military services are unprepared to make the necessary policy shifts; their beleaguered acquisition process is another cause. Another reason for the delays is a lack in unity of effort; the services appear to be competitively racing against each other rather than working collaboratively to bring artificial intelligence (AI) to market.

Cyber and AI are tightly coupled focus areas for the Defense Department. In recent months the department has completed a comprehensive new strategy and conducted a cyber posture review. It is building a Joint Artificial Intelligence Center to guide the planning and execution of national priorities, including enterprise-worthy, high-budget efforts to apply AI to a cluster of joint challenges.

It is paramount the information technology workforce—from leaders to coders—be conversant about how AI works, as well as how it is evolving and can be employed effectively. Currently, the military runs a considerable risk of paradoxically squandering resources by pursuing activities it cannot do or cannot yet do while failing to prepare to exploit those capabilities at which it excels.

A thoughtful, studied process is required to conduct AI preparation of the battlefield. This entails rebooting the data discipline from source to sink, a task with little intrinsic appeal. Unfortunately, this requirement to reboot is occurring when the military has just begun to realize its return on investment in data management tools and outcome-driven business processes and has adopted an emphasis on portfolio performance goals. However, it is an approach that will train data to be ready to work for the military.

Any turnkey AI solutions would allow the military to fail fast, learn and adjust. However, data must be readied as even smart computational algorithms overwhelmingly fail to fire for effect because of missing or bad data.

This discussion will provide the audience tools they can use to set the data pre-conditions that will allow them to smartly apply AI again their problem spaces and capture machine-assisted opportunities.

BIO: Stephanie Chenault has more than 20 years as a defense civilian and executive, technical advisor. She is currently employed as the chief technology officer of Corvus. She began her career designing weapons systems at the former USAF Rocket Laboratory where as an intern she created the guidance navigation and control system for an exo-atmospheric kinetic kill vehicle.

Throughout her career, she continued to build C4ISR systems including two game-changing systems in Iraq–CIDNE and SIGACTs. As the chief system engineer at the Army’s CTSF, she became the Army’s Lead C4ISR Engineer during Operation Iraqi Freedom.

She has expert experience in technology procurement and development, cybersecurity and intelligence, new technology transition and system design. Her background is in aerospace engineering, quantum and astrophysics and she is currently enrolled in the MIT machine learning course.

Balancing Zero Trust and Operational Expediency

Kevin Jermyn, Federal Customer Success, CyberArk Software Inc. •
kevin.jermyn@cyberark.com

ABSTRACT

The insider threat has added to the Zero Trust requirement, challenging the enablement of operators to still complete their mission. Learn how to CaC-enable all—including legacy—systems, while still operating in a risk-appropriate manner.

Today’s cyber warfare and risk mitigation strategies require not only ensuring the identity of who is on the organization’s network and what they are doing but also making sure organizations take the next step in analytics. The challenge is to align with Defense Department CIO Lines of Effort and combine both behavioral analytics and correlation analysis to be truly able to give incident response teams and audit and information assurance operators the ability to know when suspicious activity is happening and react at a moment’s notice.

BIO: Kevin Jermyn, manager, federal engineering, CyberArk, has four years of experience with federal civilian and Defense Department customers. He works with clients as a trusted advisor to ensure customers are following best practices when deploying their privileged account security programs and to give advice on how the solutions the customer owns can help reduce the attack surface, close common attack vectors and be used as a tool. He has worked directly on DHS CDM PRIVMGT Continuous Diagnostics and Mitigation and has experience with DoD LoE, 800-53, 800-171, D(FAR)S, NIAP and RMF.

Transforming Cyber Operations and Decision-Making with Cloud Analytics and AI/ML

Daniel Prieto, Strategic Executive, Google Cloud Public Sector, Google •
prietod@google.com

ABSTRACT

Government and military organizations remain significantly challenged to improve their cybersecurity postures. At the same time, malicious cyber actors continue to improve their productivity, with an average “breakout time” of less than two hours to move laterally from the point of initial compromise to other systems and data in a victim’s network. In the face of ever-increasing threats and an explosion of devices and data, no organization will be able to spend or hire its way out of the problem. And, even if there were enough staff and money, between 70% and 90% of a security analyst’s average day is spent unproductively, manually integrating data from across myriad systems and running false alerts to ground. Only 10% to 30% of an analyst’s time is actually spent finding or countering intrusions.

Faced with an overwhelming deluge of cybersecurity data that provides incomplete situational awareness as well as time-consuming and overly manual analytic processes, how can the U.S. Army improve the effectiveness and efficiency of its cybersecurity efforts?

Cloud-based advanced analytics and AI/ML will be essential to the Army’s ability to achieve effective and agile cybersecurity capabilities. Cloud-based analytics have proven the ability to reduce the processing times of petabyte-scale workloads by upwards of 90%. Combined with the capability to increase the correlation speed of disparate heterogeneous data as well as powerful dashboards and visualization solutions can transform the Army’s cyber situational awareness and threat detection. Leveraging cloud-based auto-ML to speed the training of machine learning models can move cyber defenders from a largely reactive forensic posture to one of improved predictive foresight and increased automation and orchestration that can transform many time-consuming manual cyber-analytic processes.

As Army cyber warriors increasingly rely on cloud-based analytics and AI/ML, this session will address two critical questions. First what is best way to adopt cloud? Many cloud adopters spend far too much time managing cloud infrastructure, such as configuration, provisioning, maintenance, monitoring, scaling and tuning, and not enough time getting insights from their data. Second, what is the best way to integrate human and machine capabilities in both decision-making and operations?

BIO: Daniel B. Prieto is the head of strategy for Google Cloud, Public Sector. He brings more than 25 years of leadership and innovation experience in government, the private sector and academia, working at the crossroads of technology, national security and privacy. In government, he has served as the chief technology officer in the office of the Department of Defense CIO and as Director for Cybersecurity Policy in the White House on the staff of the National Security Council.

After 9/11, he helped stand up the Committee on Homeland Security in the U.S. House of Representatives. He has been a senior advisor to McKinsey and Company, an executive at IBM and America Online and an investment banker at JP Morgan. In these roles he acted as a strategist or advisor on more than \$150 billion in transactions in technology, defense and media, including the acquisition of Netscape, as well as the mergers of McDonnell Douglas and Boeing and America Online and Time Warner.

Prieto has held fellowship appointments at Harvard, Stanford and Columbia universities and at the Council on Foreign Relations. He has testified before the U.S. Senate and his writing and commentary have appeared widely. Prieto received his MA from the School of Advanced International Studies at Johns Hopkins University and his BA from Wesleyan University.

SIGINT at the Edge Using AI

Jeff Winterich, DoD Account CT, Hewlett Packard Enterprise •

jeff.winterich@hpe.com

ABSTRACT

Real-time analytics are a critical component for situational awareness at the tactical edge. In this talk, HPE will discuss how real-time signal identification using digital techniques and deep learning (6ms in 50 MHz spectrum) at the Edge is enabled – all in a powerful size, weight and power (SWaP) optimized HPE Edge-line EL8000 system. Additionally, HPE will show how organizations can deploy a new neural network with newly identified user-specific capabilities in the field within minutes. The HPE team will also explore how power-optimized GPUs are used in this solution for both inference and training—truly artificial intelligence at the Edge.

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—focused on the U.S. Army, U.S. Air Force and combatant commands. Winterich also serves as an AI ambassador for the HPE Public Sector team and customers.

Advanced Analytics Utilizing AI for Mission Analysis

Andrew Edmondson, Principal Architect, U.S. Army Account, IBM •

andrew.devin.edmondson@ibm.com

ABSTRACT

Commanders and staff integrate numerous processes and activities within their operation and across the force as they exercise mission command. This is manually intensive. The current suite of information systems are effective at collecting, storing and displaying operational information. This is foundational for automatically processing data into knowledge to generate shared understanding in an environment where the sensors and data inputs to these processes and activities continues to grow. An explosion of data and metadata expectedly increases the complexity in identifying key pieces of information or trends that are often not considered because staff and commanders are unaware of their existence.

Working with the Army Mission Command Battle Lab, IBM has developed a prototype application of artificial intelligence (AI) that supports the mission analysis steps of the military decision making process. Using IBM’s Watson technology, the AI employs natural language processing to aid the user in more quickly finding pertinent information within an OPORD, such as specified tasks and additional context from holdings such as lessons learned. This includes:

- Parsing of orders and other unstructured holdings.
- Consistency in process steps.
- Speed in finding, organizing and presenting information.
- Contextual surfacing of additional information.

This capability augments a commander’s staff leading to more timely and informed decision making. IBM believes this technology platform and solution baseline can reduce the cognitive workload and manpower intensiveness of analytic functions for defensive cyber operations.

BIO: Andrew Edmondson is a high energy executive technical architect and technical manager with diverse technical experience that for nearly 20 years has delivered purposeful, manufacturable and sustainable solutions in highly regulated and sensitive problem spaces. Undergraduate work in engineering manufacturing, graduate work in modeling dynamic systems and life experience in each section of the software development shop has provided a unique perspective in overcoming Army challenges.

Bayesian Learning for Robust and Resilient Multi-Agent Control

Lan Hoang, PhD, IBM Research • epyzerk3@uk.ibm.com

ABSTRACT

Determining optimal policies for complex networks of multiple actors is a challenging task. Reinforcement learning has shown itself to be able to build such policies, achieving strong performance over long time horizons with recent developments in deep reinforcement learning, allowing significantly complex reward and constraint functions to be routinely learned and understood.

In uncertain conditions and where a mistake can have significant consequences, such as those encountered commonly in the defense realm, it is necessary for these policies to be robust and resilient. One common cause for non-optimal behavior in such learned systems is policy drift, where a set of actors slowly moves from acting in an environment similar to that in which it was trained to increasingly foreign environments where their learned policies cease to execute the expected actions and thus deliver the expected rewards.

IBM Research suggests the coupling of two powerful techniques—a multi-agent setting of deep reinforcement learning known as multi-agent deep deterministic policy gradient (MADDPG) and a scalable Bayesian neural network trained using recent breakthroughs in probabilistic learning. The result of this coupling produces a probabilistic multi-agent reinforcement learning framework that is capable of understanding the uncertainty and thus the risk associated with taking actions in a given environment. This can lead to more conservative decisions when there has been significant policy drift without rendering the actor useless in uncertain environments. Additionally, within a live-learning setting, actors are able to efficiently determine which actions to take to speedily learn a model linking actions and rewards in a new environment, which results in a more agile team of agents when adapting to new conditions.

BIO: Dr. Lan Hoang is a research staff member of the Applications Team, IBM Research UK.

Using AI to Get Situational Awareness From Network Data

Seraphin Calo, Distinguished Research Staff Member, IBM Research •
scal@us.ibm.com

ABSTRACT

Gaining insights from the data flowing in a network requires discovering different entities in the network and understanding their behavior and how they interact with each other. This necessitates the accumulation of evidence bearing on alternative propositions and the execution of decision functions for each of the set of attributes that characterizes the elements of the system and their operation. In general, the outcome depends not only on the state of the accumulated evidence but also the accuracy of the decision functions and the process for combining their outputs.

IBM Research has developed a characterization system for identifying devices present in an IP environment based on interpretations of the network traffic that is being generated. A major factor in its effectiveness has been the generality and flexibility of the architecture that it follows. It was recognized that there was no single unique approach that could identify all the information of interest and accommodate all deployment models. It was thus imperative that the system be able to employ multiple types of analytics structured to the needs of particular environments. The ability to include both algorithmic and AI-based components gives it a wider scope and greater effectiveness. It acknowledges that communication protocols and signatures evolve in a deliberate fashion while AI/ML techniques are more generally adaptable to new areas of investigation and better at dealing with more opaque situations (e.g., encrypted data, anomalous behaviors). Combining the two makes the system more powerful.

BIO: Dr. Seraphin Calo is a distinguished research staff member at IBM Research and currently manages the Distributed AI Enablers group within that organization. He received MS, MA and PhD degrees in electrical engineering from Princeton University, Princeton, New Jersey. He has worked, published and managed research projects in a number of technical areas, including queueing theory, data communications networks, multi-access protocols, expert systems, policy-based computing, complex systems management, edge computing and distributed machine learning. Calo was a leading member of the IBM team that won and continues to work on government-sponsored research programs in information science. He has been very active in international conferences, particularly in the systems management and policy areas. Calo has authored more than 140 technical papers and has a number of United States patents (33 issued). He has received seven IBM Research Division awards and 13 IBM Invention Achievement awards.

AI for Modeling Cyber-Physical Object Movement at Scale

Mudhakar Srivatsa, Distinguished Research Staff Member, IBM T.J. Watson Research Center • msrivats@us.ibm.com

ABSTRACT

With the advent of the mobile, wireless and embedded devices, there is an abundance of location data available. Traditional spatial analysis techniques do not treat time as a first-class citizen. The IBM T.J. Watson Research Center introduces the idea of discretizing space-time as a first order primitive to significantly alter downstream algorithms ranging from simple spatial indexing to complex deep learning that operate on such space-time data. The company coins the term Space Time Box (STB) and proposes this as a fundamental primitive way of thinking about trajectories of moving objects. It substantiates and validates the concept of STB through various pieces of the organization’s past work ranging from tracking shipping trajectories to detecting human/drug trafficking and tracking human movement in dense environments such as at music festivals and game stadiums and tracking very fast-moving objects such as asteroids.

BIO: Mudhakar Srivatsa is a distinguished research staff member and manager at the Distributed AI department in IBM T.J. Watson Research Center. His work is at the intersection of AI and edge computing with focus on learning actionable insights over large-scale spatiotemporal data. He has authored more than 100 research papers, has been granted 50 U.S. patents and has received several outstanding technical achievement awards at IBM. He serves as the editor *IEEE Transactions on Emerging Topics in Computing and Springer Wireless Networks*.

Employing AI and Analytics to Solve Digital Forensics Problems Across Multiple Domains

Mary Anne (Harasim) DeHart, IntelliGenesis LLC • maryanne.harasim@igenmail.com

ABSTRACT

Haystack is a modular analytics platform used for network analysis and forensics. It was built on the foundational principle that the computer’s job is to reduce the user’s cognitive load by doing the hard work of sifting through high volumes and velocity data (the hay) to present the user with the most important and interesting data (the needles).

Haystack processes network traffic logs and performs built-in and user-developed analytics on them to detect trends and anomalies. It then generates a fully customizable report with this information.

Network Forensics

Haystack ingests and processes data from the commonly used free network analysis framework Bro Network Security Monitor. It models 20 different data objects into an analytic-ready overview of all activity on the target network. Haystack uses a flexible multi-layered modeling approach to rapidly integrate new data formats and add new data objects. It makes no assumptions about the format of the incoming data, rather bundling multiple formats into a single analytic-ready object model. New data can be ingested in a native fashion. This prevents loss of context and supports quick turn-around on data ingest and new analytic development.

Analytics Platform

Haystack’s analytic capabilities are both robust and highly extensible. IntelliGenesis has built several sophisticated analytics within Haystack that highlight anomalies and trends in the network traffic. For example, the organization’s analytics can detect bandwidth usage trends, usage of non-standard ports and packet size anomalies. All of these analytics are configurable. They can be narrowed to specific timeframes and applicable parameters and restrictions can be set to further specify data that is of interest or should be ignored. Haystack can perform this analysis in near-real time, processing days of data in minutes.

The ability to quickly and easily develop additional analytics is where Haystack’s extensibility shines. Users can develop simple analytics within the web-based interface using pseudo-code or more complex ones using Java, Python or R. The flexible data modeling supports rapid prototyping and development of these analytics. This allows IntelliGenesis to quickly react to a new user requirement or even an emerging threat to the network across multiple domains. It also allows users to develop their own analytics that specifically target their use cases.

Reporting

Haystack bundles rapid analytic development with the capability to generate a user-friendly report. Data presentation is an important part of network analysis, but oftentimes it is left to the analysts to re-process their findings into an official document. Haystack peels back these layers by providing a well-formed and customizable results view.

Results are presented to the user in a series of web-based charts and graphs. The user can choose what subset of the available analytics to execute. Only chosen analytics will display their results in the report. Each analytic has full control of the way it displays its results to the user. The report is fully customizable enabling the user to convey additional information with the ability to title and caption each graph.

BIO: Guy Howard currently serves as lead engineer for IntelliGenesis. He possesses more than 16 years of experience in full life-cycle software development and engineering across multiple contracts and projects within the federal Intelligence Community. On these projects he has integrated novel AI approaches to automate and optimize system performance, framed system infrastructure and developed and implemented various algorithms, rules and analytics. Howard also has management experience, leading development teams to design and build state-of-the-art data processing platforms. He holds a BS in computer engineering and an MS in technical innovation management.

Multidomain Cyber Analytics-Driven Defense (MCAD)

William Liu, Technical Director, LGS Innovations LLC, a wholly owned subsidiary of CACI Federal Inc. • william.liu@caci.com

ABSTRACT

CACI proposes Multidomain Cyber Analytics-Driven Defense (MCAD), a machine learning (ML)-enabled solution that automates defensive cyber operations against cyber threats across multiple domains. MCAD's concept of operations is as follows: 1) ingest and process raw data from multidomain (network, RF, logs, intel, etc.) sensors; 2) use domain-specific ML techniques to extract information needed to build situational understanding (SU) and detect threats in all sensed domains; 3) build and visualize SU incorporating detected threats.

For step 1, MCAD deploys hardware and software sensors as needed by mission requirements. For example, social media, threat intelligence and network sensors are activated in an enterprise setting while RF and network sensors are used in a tactical environment. A notable example of the organization's hardware sensor is CACI's small and medium form factor network sensors that support FPGA-based data analytics at the network edge and can be rapidly deployed by defenders such as Cyber Protection Teams (CPT) into diverse operating environments.

For step 2, MCAD utilizes a suite of machine learning techniques to extract SU elements and identify anomalous patterns in sensor data. The company provisions each technique as a software plug-in and route the appropriate domain sensor data to that plug-in. For example, it uses the natural language processing plugin to extract network topologies and the latest vulnerabilities, threat vectors and attackers' tactics, techniques and procedures from the human readable NetFlow reports and shared cyber threat intelligence, respectively. It passes packet capture to the recurrent neural network and k-means clustering plugins that best detect network intrusions and botnets. In the spectrum domain, CACI applies the organization's signal analytics capability developed for the Army Signal Classification Challenge. For optics, the organization's image analysis plugin can parse objects from static images and full-motion videos, attach contextual meaning to them and determine presence of threats. These plugins support composable ML workflows that implement ensemble and transfer learning techniques that achieve accurate results without requiring more training data. Finally, MCAD provides an Model-based Systems Engineering (MBSE)-driven development framework that continually retrains ML models, updates ML algorithms and refines the plugins by automating the end-to-end ML workflow.

For step 3, the team uses a knowledge graph to capture the overall cyber context and its corresponding threat conditions. For example, key enterprise or tactical network nodes are represented as vertices in the graph while malware detected on these nodes become neighboring vertices. It applies graph theory to support SU queries by human analysts in their military decision making process (MDMP). For visualization, it utilizes CACI's versatile Universal Composable Visualizer, which allows users to dynamically compose data fusion and visual building blocks into SU-specific views.

The company envisions linking MCAD to a course of action analysis platform linked to a cyber wargaming or modeling and simulation system to support defensive course of action formulation and adoption.

BIO: William Liu is a technical director at LGS Innovations, a wholly owned subsidiary of CACI Federal. He has deep experiences in leading and managing cyber and systems engineering R&D programs sponsored by SCO, DARPA (DMT-PAMS, National Cyber Range Phase 1, Active Cyber Defense), ONR and AFRL, as well as commercial entities such as Fujitsu of Japan.

Liu’s technical expertise lies in the areas of large-scale cybersecurity system integration, cyber threat intelligence sharing and response, ontology development, anomaly detection-based network security sensor, defensive cyber course of action modeling and simulation, software automation and adaptation and software-defined radio development. He also has deep solution architecting experiences where he developed large-scale managed IT service frameworks for Defense Department and IC customers using ITIL and Scaled Agile methodologies. Liu holds a BS in aerospace engineering from Georgia Tech and an MS in mechanical and aerospace engineering from Rutgers University.

Cybersecurity Common Operating Picture

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

ABSTRACT

Mission Innovate, a joint venture organization between All Points and Mission Multiplier, brings truly differentiated services in the area of cyber continuous monitoring and risk scoring/benchmarking. The team collaborated to develop an innovative solution called MI:COP that can present an accurate cyber common operating picture (COP) that it has recently successfully deployed at NASA Marshall Space Flight Center. Its MI:COP solution is unique in that it is focused on changing the behavior of cybersecurity practitioners by incentivizing them to pay attention to “key effectiveness measures” through risk scoring, implementation of a risk scoring dashboard and adoption of an overall “risk economy.”

The MI:COP solution is built on the philosophy that not all IT assets are created equal. Organizational leaders should be tracking key metrics related to those key IT assets (or key cyber terrain) and, through automated technology, using real-time data to inform more effective and efficient risk management decision making. The team achieves this goal by first working to identify the key IT assets within the organization and defining effectiveness measures that are quantifiable, actionable and meaningful to the client organization.

Simultaneously, Mission Innovate personnel work to ensure that each organization possesses the tools/technology to collect data that is needed to support the defined metrics. To normalize the data collected from the different automated tools, they leverage a common framework and nomenclature called secure content automated protocol (SCAP). Where SCAP does not currently support existing tools, they can develop the custom SCAP through the Open Checklist Interactive Language (OCIL). Using this protocol enables the team to more easily have an “apple-to-apples” comparison, which is not easily achieved when collecting data from different tools.

The data collected from the different sensors in the IT environment is then captured in a data warehouse where the Mission Innovate team runs tailored queries that help to generate the defined effectiveness measures. The information from the database is ultimately used to support the development of a dynamic risk scoring dashboard—the front-end of the organization’s MI:COP solution. The dashboard not only scores and tracks progress at the enterprise level but also enables the user to drill down to unique grades at the business unit level and even the specific IT system level. The dashboard results are updated in real-time based on the cadence of each scan that comes from the different sensors.

The end result of MI:COP implementation is a customized and automated risk scoring solution that ties together data feeds from automated IT security scanning technologies to drive changes in the behavior of IT security practitioners—tying known vulnerabilities to risk scores at both the organization and individual level—to focus on mitigating the highest risks first.

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

Miller possesses more than 19 years of experience and is a proven thought leader who 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. Miller's innovative cyber solutions—to include 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 was awarded the 2016 Emerging Entrepreneur of the Year by Innovate Huntsville and was nominated for the prestigious Russell G. Brown Award by the Huntsville Chamber in 2017, 2018 and 2019. He was a finalist as Entrepreneur of the Year as part of the 2018 Economic Development Partnership of Alabama (EDPA) imerge Innovation Awards. He is a regular speaker at information security industry leading conferences (e.g., FOSE, GFIRST) and has published several industry articles, most recently writing about shared risk for *Security* magazine. Miller holds an MBA in consulting from Thunderbird School of Global Management and a BA in international studies from American University.

AI/ML/DL and Advanced Analytics: Whoever Owns the Data Is King

Gregory Gardner, Chief Architect, Defense and Intelligence, NetApp •

greg.gardner@netapp.com

ABSTRACT

To understand where AI should be used and will be most successful in multidomain operations and military decision-making, users must understand what AI really is. AI in this context refers to a broad set of algorithms that can solve a specific set of problems, if trained properly. While integrating machine learning into a product is trivial, effectively training the algorithms to perform their task is not.

Data is the fuel for AI. AI works best when large amounts of rich, big data are available. As data collection, analysis and storage abilities dramatically improved over recent years, military organizations have found themselves with a huge potential resource yet under-equipped to wrestle with such high volumes of information.

The more facets the data uncovers, the faster the algorithms can learn and fine-tune their predictive analyses. According to industry predictions, AI's greatest limitation—high quality data—is becoming more and more evident. Similarly, successful machine learning also depends on large, broad data sets.

In the today's complex and rapidly evolving combat environment, whoever owns the data is king.

NetApp is the data authority for AI/ML. NetApp's constant innovation has made it the leading data management provider to the U.S. Army and the Department of Defense for the past 9 years. In June 2019, NetApp was named the global leader for corporate innovation in AI and received the Best AI Solution for Big Data Award in the 2019 AI Breakthrough awards program.

Here is what that means to the U.S. Army:

NetApp's all-flash arrays consistently deliver proven best performance with guaranteed low latency under the most stressful workloads. Additionally, NetApp delivers market-leading data reduction with features like deduplication, compression and compaction. Turn on snapshots and the storage savings increase 10 times. NetApp's solutions are secure. NetApp's all-flash arrays provide application-consistent data protection, synchronous replication, built-in encryption, WORM protection, multi-factor authentication, FIPS 140-2 Level 2 certification, crypto shredding and more. NetApp guarantees its products meet governance and compliance requirements.

Importantly, NetApp, NVIDIA and Cisco have partnered to deliver NetApp ONTAP AI, powered by NVIDIA DGX and NetApp all-flash storage. This integrated solution scales efficiently in response to business demand, offering enterprises the right balance of compute, storage and networking to deliver powerful AI services across a broad base of users. NVIDIA's DGX-2 server, certified only for use with NetApp, is an extremely powerful AI/ML/DL platform that benefits from equally powerful storage and network infrastruc-

ture to deliver maximum value. By combining NetApp AFF systems with Cisco Nexus switches, users can implement this verified architecture at almost any scale that they need, from a single DGX-2 paired to an AFF A220 system up to potentially 96 DGX-2 servers on a 12-node AFF A800 cluster. Combined with the superior cloud integration and software-defined capabilities of NetApp ONTAP, AFF enables a full range of data pipelines that spans the edge, the core and the cloud for all types of successful AI-related projects.

The quickest way for the Army to accelerate AI adoption is to leverage the innovation and tools in the hyperscale cloud. Those tools require rich datasets, which means a multi-cloud data strategy is required. The NetApp Data Fabric connects on-prem data center environments to the analytic capabilities of all major cloud providers. For example, Microsoft Azure can be used for text sentiment analysis, AWS for network packet analysis, Google for Image Recognition and on-prem training clusters can be built for classified applications. The Army can only leverage the best AI tools with a data strategy that allows for this flexibility. NetApp data mobility makes accessing these tools simple and straightforward.

NetApp provides the fundamental building blocks for hybrid cloud to ensure military users have the right data in the right place for the right cost. Whether it's tiering cold data to a DISA cloud, using a commercial cloud for backup of unclassified data or unifying management across flash and cloud, NetApp all-flash storage connects to more clouds in more ways than anyone else.

Finally, NetApp's technology advancements allow military users to stay relevant and drive ahead of their adversaries. NetApp leads the market shipping NVMe over Fabrics (NVMe-oF), the industry's first end-to-end NVMe system, support for 32 GB fiber-channel and 100 Gb Ethernet, data management software for server-side persistent memory and cloud data services.

In sum, NetApp's innovation focus and collaboration with the organization's partners allows the company to deliver an integrated data fabric, giving military users the freedom of choice, future-proof environments, simplicity and protection they require for successful digital transformation in AI/ML.

BIO: Dr. Greg Gardner coordinates NetApp's development activities in the defense and intelligence arenas. He is a retired infantry colonel with more than 30 years of commissioned service. After his retirement from the military, Gardner was vice president of the public sector strategy at Oracle then returned to government service as deputy CIO for the U.S. Intelligence Community. He has been at NetApp since 2011. Gardner holds a BS in electrical engineering from the United States Military Academy and a PhD in IT management from Capella University.

AI Development Principles for Army Missions

Michael O'Brien, Algorithmic Warfare Unit Lead, Northrop Grumman •

sean.obrien@ngc.com

ABSTRACT

The artificial intelligence (AI) revolution that has transformed the commercial marketplace is poised to transform the way warfare is conducted by the Department of Defense (DoD) and the Intelligence Community (IC). Analytics and AI are experiencing a sort of gold rush and there is much confusion—talk to 10 different people working in the field and you will get 10 different and often mutually exclusive descriptions of just what the basic terms even mean.

To understand the opportunities and challenges of this ongoing transformation, it is essential to establish a foundation and framework of discussion. Once that foundation has an initial form and there are multiple potentially useful taxonomies, the military and industry can begin to build the set of skills, infrastructure needs, development processes and system architectures required to missionize AI for the cyber analyst and warfighter.

The goal is to lay out a general set of definitions. These are not the only useful definitions, but they are proposed as a practical scaffold upon which the important discipline of what Northrop Grumman calls Algorithm Engineering (AE) can be built. Next, the industry team discusses the emerging field of Algorithm Engineering itself and how its practice and success are required to solve the unique challenges of the IC that won't necessarily come ready-made from the commercial marketplace. Finally, Northrop Grumman examines some critical enablers that are needed to close the gap between the current practice of AI and the successful missionization of AI to accomplish DoD and IC mission goals.

BIO: Dr. Sean O'Brien has been developing algorithms to exploit large data sets for more than 20 years. He currently runs Northrop Grumman's Algorithmic Warfare Unit and also acts as a Corporate AI Architect helping to lead AI efforts across the company. His team focuses on creating automated algorithm-defined systems and tools to aid analysts and operators in multiple Defense Department and IC organizations. He has a PhD in astrophysics and he and his business unit are based in Los Angeles, CA.

Advanced Identity Analytics to Integrate AI With Cyber Operations

Andrew Whelchel, Principal Solutions Engineer, Okta • andrew.whelchel@okta.com

ABSTRACT

Just as CEMA as a multidomain deployment doctrine is relatively new, so too are how advances in artificial intelligence, machine learning and threat identification integration can contribute to effectiveness of cyber offensive and defensive operations. Integration of these capabilities must be executed in way that is autonomous and accurate for threat identification to be effective. This presents an opportunity for CEMA planners to make use of AI/ML, threat identification and cyber defense response in way that is accurate to the data science but does not take a data scientist to execute and support.

This is the challenge: to leverage AI in particular for CEMA and be operationally effective so as to leverage the data for efficacy and be operationally useful so that its integration operation does not require AI expertise and/or a data scientist to retool for every operation. An even deeper challenge is to orchestrate the integration so that one can also achieve metrics in reducing the time between human reaction and dynamic threat response.

To achieve these metrics on a human-to-threat response and actual AI integration, the solution needs to be able to integrate the AI data, securely authorize that AI data, provide automated transactional responses and enable autonomous active cyber response operation. Meeting this challenge requires a focus on identity, specifically when using identity along with API authorization. Driving with identity transaction and the identity's API authorization enables the integration of out-of-box context data along with AI analytics for the identity transaction.

Solving this problem with an identity transaction that supports the AI data includes several functions/steps in the identity transaction that enable use and collection for an AI-based authorization request and response. The steps to ensure this include:

- Pre-authorization policy evaluation, including matching for machine learning threat context attributes.
- Authentication to multiple or single factor based on policy using AI in risk scoring.
- Authorization inclusive of OAuth2 bear token generation.
- Web hook integration for authorization of AI attributes.

When combined with AI sources and tied to defensive cyber response, this identity transaction is relevant as it provides the means to apply AI to any authorization request, including authorizing specific API data streams. Attendees of this session will learn:

- How to align the organization business value of artificial intelligence/machine learning goals to capabilities of cloud identity security.
- The operational use cases of an operational model for identity-as-a-service to support cloud applications and cloud artificial intelligence/machine learning data access.
- An understanding of the components and interfaces to deploy the operational model using identity-as-a-service, API gateways and machine learning APIs.

BIO: Andrew Whelchel, CISSP-ISSAP and CCSP, started in information security and IAM after graduating from the University of Memphis by supporting identity and access management by managing Microsoft Identity for U.S. federal customers. Later, he transitioned to network infrastructure security and consumer identity protection. Most recently, Whelchel has worked in the same role at RSA Security and Okta.

At RSA Security, Whelchel supported financial services, health care, U.S. federal and other customers with a focus on identity risk analytics and integration of identity fraud intelligence for cybercrime prevention. Now at Okta, his focus is on protecting employee and partner as well as citizen consumer identities for the public sector to reduce cyber risk as well as accelerate capabilities for cloud transformation. Contributions include work as a contributor on the NIST 1800-3 ABAC standard and speaking events about identity access management and security.

Asymmetric Advantage in Battlefield AI

Roger Morin, Solutions Architect and Inventor, Phacil LLC • rmorin@phacil.com

ABSTRACT

Corbomite delivers an asymmetric advantage to multidomain operations by integrating the strengths of both types of AI. These are data-based (e.g. machine or deep learning) and knowledge-based (e.g. expert system) types of AI. Once provisioned, it can be amassed and deployed to collaborate with the soldier, unit, system or large staff, requiring minimal training. It integrates these two types of AI to deliver analytical advantage greater than the sum of each AI types strengths. It is cloud or on-premise deployable or clusterable using low size, weight and power hardware to amass advantage in contested expeditionary environments.

Corbomite ensures cybersecurity and auditable attribution for each AI instance, for information technology (IT), as well as operational technology (OT, e.g. weapon systems) and Internet of Things (IoT) devices. And, it can rapidly validate and restore any IT, OT or IoT device's kernel level if one bit of security is in question. This allows rapid battlefield exploitation of cyber devices. It provides attributable and auditable, therefore accountable and trustworthy, end-to-end real-time warfighting HITL decision support and HOTL IT, OT or IoT system automation. This can never be accomplished by only data-based AI. Corbomite's AI assists even if information or network connectivity is limited, with information volume and velocity only improving performance. Corbomite is network capable but not network dependent, unlike most data-based AI.

Corbomite can enable HITL or HOTL planning, execution and training. Prototyping knowledge-based AI requires access by knowledge engineers to develop domain ontologies and to emulate a planner's, staff officer's, weapons technician's or trainer's expertise into playbooks that can be crossbred to other domains as U.S. Army property. Unlike data-based AI that requires exceptional coding expertise, knowledge-based playbook coding is very trainable, so the average service member can efficiently amass enough coding knowledge to maintain AI overmatch. The cost of knowledge engineering is won back in the widespread and exponential increase in automated HITL/HOTL assistance to less experienced operators or systems with trustworthy attribution.

Corbomite has already "rigged" foundational cybersecurity insider threat knowledge-baseline AI. This baseline enables any MDO domain to be further AI "rigged." Rigging includes both ontology and playbook development. Incorporating data-based AI requires continuous data access and continuous or periodic reachback to cloud or on-premise computing to retrain the AI per the dynamic environment. Given the expectation that reachback lines of communication will be contested, data-based AI alone is a sub-optimized solution. Regardless the condition, Corbomite's knowledge-based AI, which rules over all AI instances, is still in play supporting continuous HITL or HOTL advantage.

Corbomite's Problem Statement 1 Advantages

- Provides asymmetric AI advantage against high volume and evolving cyber threats.
- Is currently rigged with two layers of cyber threat identification and isolation capability.

- Can provide user-friendly MDO HITL overmatch for reduced time gap to threat response and autonomous HOTL AI assist, including cyber payload deployment, reducing cognitive workload and manpower intensity with full auditable authority attribution.
- Can efficiently evolve multidomain expert planner emulation AI integrated with continuous battlefield environment pattern analysis AI to speed and cognitively assist decision.

BIO: Lt. Col. Roger Morin, USMC (Ret.), is a senior IT/cyber solutions architect with Phacil LLC and inventor of the Co-symbolic Battlefield AI patent-pending Corbomite solution. In May 2019, he was one of six experts invited to mentor the Army Science Board on Battlefield AI. He was the Systems Engineering Technical Assistance program manager for the JIEDDO Attack the Network effort from 2010 through 2016. He is a former infantry commander, C4ISR planner, warfighting dean at Marine Corps University and School of Advanced Warfighting (SAW) graduate. He enlisted for active duty in 1981 and is a USNA Class of '86 graduate.

Inverse Properties to Create Cyber AI

Matthew Maher, Lead Data Scientist, Processus Group and Corvus Consulting •
maherm@processusgroup.org

ABSTRACT

Knowledge graphs built with process driven ontologies develop operational patterns in data to leverage inverse properties to identify patterns in offensive, defensive and cyber SU data. The group has developed models that leverage the inverse properties function along with graph data algorithms to identify patterns in data to identify and recommend a reaction to cyber threats.

For example, in the organization’s models, the team defined the cyber operational terms for an attack or defense. The models semantics contain the cyber term “ infiltrate,” define its meaning as “a form of maneuver in which an attacking force conducts undetected movement through or into a network, device service or platform in order to occupy a position of advantage on the enemy network, device, service or platform,” and provide data characteristics of a cyber infiltration and the data required to determine an infiltration. Then, in the modeling process, the team assigns an inverse property to the “infiltration,” in this case semantically defining a cyber “block,” “secure,” “isolate” or “exfiltrate” as the inverse response to an infiltration. In the model, the group again defined the definition for each as well as its data characteristics and properties. Assigning the inverse properties along with graph algorithms allows an intelligent system to establish patterns on cyber data and autonomously fix the issue or for a cyber SU system to provide a recommendation on how to assess the cyber terrain.

The team has developed these models for use in offensive cyber to help determine an enemy’s likely response, to recommend defensive tactics to the blue team, to provide defensive options within situational understanding and to aid leadership decentralize decisions. Tactical units are most effective when they can decentralize decision making through using effective intelligent systems and analysis. However, cyber defenders need to create the models to create the knowledge base that comprises a sequence of steps, soldier’s knowledge and equipment capabilities and data.

The explosion of IT and data has caused two problems for commanders and staffs: a degraded ability to tailor processes and procedures using current fielded systems and an increased cognitive burden related to processing and finding meaning in the vast amounts of data collected. Industry is using cognitive capabilities to address these problems and so can the Department of Defense. However, these capabilities require initial human intervention; and a knowledge base comprised of facts, beliefs, basic information and relationships. A knowledge base cognitive capability is applied to new data inputs and generate meaningful recommendations from patterns built using operationally accurate knowledge graphs and process driven ontologies (PDO).

BIO: The team has developed knowledge graphs for the offensive cyber, defensive cyber and cyber situational awareness that will augment machine learning and Artificial intelligence.

Cyber Data Hub for Analytics and AI

Zach Duncan, FlashBlade Specialist, DoD, Pure Storage •
zduncan@purestorage.com

ABSTRACT

Big data is no longer static, predictable data. In the modern era of analytics, infrastructure must be architected for the unknown, delivering real-time performance with cloud-like agility for any unstructured data. Modernize with Pure Storage FlashBlade is the industry’s first dynamic data hub purpose-built for today’s analytics workloads.

The industry is in a new era. While Hadoop was the only widely available analytics tool a decade ago, data scientists have a plethora of tools at their disposal today. Spark, Kafka and Elastic all push the limits of data in drastically different ways. And with the advent of machine learning and AI, truly unstructured, random data is enabling new insights, driving innovations once considered science fiction.

A new class of data platform is needed, one that is built for the needs of modern, dynamic data—and architected for the unknown. This is FlashBlade. FlashBlade is the industry’s first dynamic data hub purpose-built for modern analytics, offering real-time response for any unstructured data with cloud-like agility. FlashBlade is massively parallel at its core and delivers unprecedented performance and simplicity for data scientists and engineers. From small, metadata-heavy workloads to random, large file accesses, it is architected for the unknown—whatever the next big data initiative may be.

BIO: Pure Storage helps innovators build a better world with data. Pure’s data solutions enable SaaS companies, cloud service providers and enterprise and public sector customers to deliver real-time, secure data to power their mission-critical production, DevOps and modern analytics environments in a multi-cloud environment.

Autonomic Vulnerability and Compliance Suite Advanced Analytics Utilizing Artificial Intelligence

Margaret Margle, Senior Executive Director, Sabre Systems Inc. •

mmargle@sabresystems.com

ABSTRACT

Today’s networked battlefield has become increasingly vulnerable to all forms of cyberspace, electro-magnetic spectrum and directed energy attacks. The network has vulnerabilities when operating in a fully contested battlespace by adversaries (red) and equally congested by both neutral (gray) and friendly (blue) forces. Air gapped and connected (during maintenance or when uploading/downloading mission data) cyberspace attacks are increasing and countering these threats in multidomain operations requires a full understanding of the full spectrum of cyberspace operations and the military’s ability to exploit, deny and disrupt the adversary’s use of it.

The military also has to have a full understanding of the network and all of its cyber entry/access points and potential attack vectors that could be exploited to impede mission/safety critical functions. A typical cyber risk assessment that encompasses both mission and functional thread analyses can take up to six months to complete and is very labor intensive. Red team/blue team exercises can also take months to complete while the teams try to understand the full breadth of the attack surface.

To reduce the time to understand the vulnerability of any networked system, as well as help identify “work arounds” to ongoing attacks, Sabre Systems has developed the Autonomic Vulnerability and Compliance Suite (AVACS). AVACS utilizes both machine learning and artificial intelligence (ML/AI) to input/develop the systems architecture, threat model, access/entry points, subsystem capabilities, cyber requirements and controls (such as NIST), mission requirements and operational tasks topology structures and enables the user to identify exploitable cyber attack vectors; identify the weaknesses in the system architecture; propose mitigations to the risks; and support the development of tactics, techniques and procedures to counter any cyber-electromagnetic activity directed at the system. This includes assessments of supply chain and maintenance requirements to sustain cyber resiliency.

AVACS will reduce assessment time for both conventional cyber risk assessments, as well as war gaming exercises to a matter of days vice months and can be used to link network systems in the battle space to prepare for efforts such as “Cyber Blitz/Cyber Quest,” or to preview live, virtual and/or constructive environments. AVACS will also help develop a commander’s cyberspace situational understanding (Cyber SU), which is a critical enabler being developed along with defensive cyberspace operations/offensive cyberspace operations capabilities. AVACS is one of the most comprehensive cyber-assessment tool available today.

BIO: Robert Hanley is vice president cyber solutions architect responsible for developing and implementing cyber defense in-depth capabilities. Hanley was formerly the national director for the Department of the Navy responsible for certifying airworthiness and CYBERSAFE for all Navy and Marine Corps aircraft as well as for 18 international partners/customers, including the U.S. president’s helicopter, the Blue Angels and more than 4,000 operational and test aircraft, manned and unmanned. These airworthiness and cyber certifications ensured Navy and Marine Corps aircraft were safe for flight and could safely and effectively operate in any cyber contested environment. Former member of the DoN CYBERSAFE Advisory Board, Hanley also was the chairman of the National Airworthiness Council comprised of the senior airworthiness leaders from the U.S. Air Force, Army and Coast Guard, the FAA, NASA and DHS. Graduate of the U.S. Naval Test Pilot School, he is an internationally recognized expert on airworthiness and CYBERSAFE. Hanley has received more than 50 awards for accomplishments from the Defense Department, industry and academia, including the DoD Distinguished Civilian Service Award (highest award for a civilian in DoD) and most recently was inducted into the Virginia Tech Academy of Excellence after being named one of the top 35 aerospace and ocean engineering graduates of Virginia Tech since it was founded in 1872.

Digital Information Common Operating Picture (DICOP)

Mark Campbell, Chief Marketing Officer, Sc2 Corp • campbellm@sc2corp.com

ABSTRACT

Governments today face an uphill battle in the effort to sift through the growing volume of available data in order to stay abreast of constantly evolving threats. The Sc2 approach is to use human talent more efficiently, using machines to perform redundant and repetitive tasks through automation, thus making human talent scalable. Designed to support and enhance national security and intelligence missions, Equitus products are in use in several Middle East countries providing systems in support of military intelligence operations for the U.S. Central Command.

Sc2 Corp has developed a Digital Information Common Operating Picture (DICOP) with an integrated geospatial display and data-fusion capabilities for military intelligence operations. The DICOP solution includes visualization capabilities that are easy to use, allowing users to gain an understanding of the current situation for designated operations. DICOP is built from commercial off-the-shelf components consisting of Equitus Social Insight (ESI), Equitus Intelligence (EI), Equitus Text Analytics (ETA) and Equitus Visual Ops (EVO). The DICOP solution focuses heavily on putting relevant data into a single secure, non-public cloud analytic environment. Sc2 provides a dedicated client architecture that collects, transforms and combines social media data, structured files, unstructured text and client activities into a system where all reports generated can benefit from a greater collective data repository.

The four major components of the organization’s solution provide a robust capability that includes:

- The ability to crawl, scrape, ingest, analyze and store from more than 130 million global URLs (Equitus Social Insight).
- The capability to extract, transform, load and correlate a myriad of diversified data sources into a common intelligence database with robust tools (Equitus Intelligence).
- The ability to automatically ingest vast quantities of unstructured data (documents, PDFs and more than 100 document types) into an easily searchable datastore that creates automated link-chart and accurate entity networks (Equitus Text Analytics).
- An in-memory geospatial visualization platform that consolidates all Equitus-stored data into a single visualization platform (Equitus VisualOps).

Each component of the Equitus system is easily integrated with legacy and third-party systems to protect previous technology and data investments. The system is comprised of open API/SDK to support seamless integration with third-party applications. Equitus systems also contain and support various API standards to ingest or export data to client specifications to integrate and maintain exchange server compatibility.

Systems are designed to handle concurrent operational queries from multiple work groups across the organization, sharing a central system with continuous data ingestion.

At the heart of the organization’s system is Equitus Intelligence. EI uses advanced machine logic to find connections that humans otherwise could not find. The combination of machine-led analytics and human-led analysis capabilities helps users quickly find hidden connections and critical patterns buried in internal data and external/open-source data. From national security and defense to cyber and enterprisewide threats, EI helps develop a comprehensive understanding of the threat landscape to identify vulnerabilities and disrupt threats.

BIO: Mark Campbell joined the Sc2 team in the summer of 2018. With a master’s degree in international business from Pepperdine University, Campbell began his military career in 2005, rising to the rank of colonel in the U.S. Marine Corps in 2018. He has held positions in the U.S. Central Command, U.S. Special Operations Command and III Marine Expeditionary Force. His military experience also includes being a battalion commander for the 4th Amphibious Assault Battalion 4th Marine Division, planning and executing multiple Special Operations Forces exercises. Coupled with management experience in the corporate sector, Campbell brings more than 10 years of military and corporate experience to the team.

AI Tools Deliver Faster, Better Decisions for Defense and Offense

Ray Cruciata, Security Specialist, Splunk • rcruciata@splunk.com

ABSTRACT

As cyber missions evolve and intensify, the right artificial intelligence (AI) tool is a necessary precondition for success, enabling Army networks and network defenders to correlate established metrics with real-time activity data. Whether the immediate priority is defense or offense, an effective response to the modern landscape demands not only faster operational decisions but also the right decisions to counter an emerging threat or take advantage of a strategic opportunity—without requiring high-level data science skills to undertake a mission.

To defend against external threats, an AI system must offer increased speed and more effective response by enabling autonomous active cyber operations. That ability, in turn, depends on a sophisticated system of incident response, threat hunting, forensics, pen testing and event analytics that gives operators the ability to reduce event clutter, discard false positives and adhere to a complex set of operational rules. Smart, successful offensive operations depend on a mix of analysis and DevOps to support every step in the cyber kill chain—exploit, control, execute and maintain.

To deliver on those expectations, the Army requires a technology that optimizes people and process, creating an AI nerve center that gives security teams access to the statistical, visual, behavioral and exploratory analytics they require to drive deep insights, rapid decisions and successful action. Participants in this session will learn about a technology stack with the ability to detect and understand a threat, allowing the entire organization to respond in a manual, semi-automated or fully automated fashion.

Splunk personnel will introduce two essential resources that should be on every cyber warrior’s desktop: a Security Orchestration and Automation Response (SOAR) tool that reduces the time gap between human reaction and threat response and resources that help operators leverage machine learning to address evolving threats as they emerge. With the ability to identify anomalies that may be markers for malicious activity, the Enterprise Security Content Update (ESCU) application is a particularly powerful resource for anticipating and repelling cyber threats. Splunk’s computational capabilities give operators the ability to quickly spot and respond to values that significantly exceed the standard deviation for data points like:

- Baseline of DNS query length.
- Baseline of SMB traffic.
- Baseline of command line length.

- DNS query length outliers.
- SMB traffic spike.
- Unusually long command line.

BIO: Ray Cruciata is a security specialist in the DoD practice. He supports Defense Department customers in their use of Splunk for securing and ensuring operational health of mission-critical services. He brings to Splunk 20 years in enterprise software experience with roles in support, engineering and technical pre-sales. His background in software/hardware includes backup, storage, high availability and security. He has an undergraduate degree in computer information systems from Baker College. He currently lives in Orlando, Florida, with his wife and two daughters.

Accelerating Cybersecurity With AI-Based Advanced Analytics

Bradley Ward, Senior Director, U.S. Army Cybersecurity Solutions, Symantec •
bradley_ward@symantec.com

ABSTRACT

The combination of advanced analytics and artificial intelligence (AI) is poised to bring a significant shift in cybersecurity capabilities. Already, AI and machine learning (ML) are rapidly being incorporated into commercial solutions, augmenting existing data-driven security solutions. However, to fully leverage these new capabilities, Army organizations need to understand both the ways in which AI-based analytics can strengthen security and the challenges that need to be understood and addressed.

As the Army recognizes, one of the primary drivers for AI/ML is the increased volume and velocity of cyber threats. Over the years, automation has played a critical role in reducing the time required to identify and respond to threats. However, traditional automation can only go so far. AI and ML represent a leap in capabilities because they enable systems to evolve as time goes on and more data is ingested, increasing both the speed and effectiveness with which cyber systems can learn to identify threats—even threats that were previously unknown.

But threat response is just one dimension of cyberspace operations. Well ahead of any cyber incident, organizations can leverage data to assess and mitigate the risks present in their environment. A risk-based approach asks, “What behavior and sequence of conditions present the risk of a cyber breach? Where is there specific mission risk?” User and entity behavior analytics make it possible to develop models that identify the risk posed by every entity on a network (devices, users, applications, APIs, etc.)—and to re-evaluate that risk on an ongoing basis.

However, AI-based analytics are not foolproof. Even seemingly sound data models can produce unintended consequences or false positives, either because of bad data or poor data architectures. Also, it’s important to remember that adversaries also have AI/ML-based tools—and that an AI/ML-based system is another threat surface.

Symantec provides its clients with an understanding of the value and limitations of AI/ML-enabled analytics.

BIO: Subject matter expert briefer Dr. Andrew Gardner is the global head of AI/ML at Symantec. He created and leads Symantec’s Center for Advanced Machine Learning (CAML), which is a team of 12 to 20 applied researchers working on state-of-the-art AI/ML security innovation for cross-functional, multi-stakeholder projects. His leadership role includes operational, technical and strategic aspects.

Gardner’s career spans 25 years across enterprise, clinical and academic settings. Past roles range from software architect to machine learning consultant to chief data scientist. He is an active researcher with more than 20 peer-reviewed papers and a dozen filed patents. He teaches a graduate course in machine learning at the Georgia Institute of Technology and frequently presents technical topics around the world.

Gardner received degrees in electrical engineering from the University of Tennessee–Knoxville (BSEE) and the Georgia Institute of Technology (MSEE and PhD)

Vulnerability Analysis Using Machine Learning

Zach Bennefield, Senior Security Engineer, Tenable • zbennefield@tenable.com

ABSTRACT

Network defenders and offensive operators need a way to quickly assess a local or remote target and create a plan moving forward using actionable intelligence. The threat landscape is constantly changing as new exploits are being crafted and existing exploits are being chained together to create lethal cyber kill chains. This risk is multiplied by expanding asset types and the complexity of patch prioritization in an ever-changing threat landscape. The key to security is basic cyber hygiene, live discovery of assets on the network, continuous visibility into those assets and prioritization of remediation based on mission risk.

A new process known as predictive prioritization, which utilizes machine learning combined with threat-intelligence within the already heavily-employed ACAS suite of applications, enables network defenders and operators to key in on critical assets and their vulnerabilities. Security engineer Zach Bennefield will review the ways the Defense Department can manage, measure and reduce its cybersecurity risk in a focused manner using advanced analytics.

BIO: Zach Bennefield is a senior security engineer at Tenable focused primarily on Defense Department, IC and FSI relationships. Bennefield has 11 years of extensive security expertise starting in the U.S. Navy and continuing into the public sector. He received a BS degree from University of Maryland University College in networks and computer security and a MS from Utica College in cybersecurity with an emphasis on cyber operations.

Expediting Operational AI With Automated, Self-Service Data Prep

Brian Shealey, Director - DoD/IC, Trifacta • bshealey@trifacta.com

ABSTRACT

To effectively operationalize AI, it's critical to expedite the maturity cycles for building and improving models. This is a challenge due to the ever growing volume and complexity of data across the Army. Data science professionals spend upwards of 80% of their time cleaning and transforming data, writing lots of manual code (R, Python, etc.) that is error prone, ad hoc and non-collaborative before they can even test AI models. This is a critical bottleneck in the data ops workflow.

Enabling a democratized, self-service-driven and automated approach to data prep eliminates this bottleneck by empowering less technical data professionals such as analysts to transform and clean data to be used downstream in the process by those working to advance analytics and operationalize AI. The result is lower overhead, faster AI maturity cycles and improved insights through expedited operationalization of AI. This vastly improves the lethality of the organization's warfighters by bringing AI-based improvement to key support systems faster and more scalably.

BIO: Brian Shealey spent the past 15 years working with Defense Department organizations to adopt innovative emerging technologies to improve warfighter capabilities. He is responsible for Trifacta's Defense Department and IC business.

The Intelligent Edge with 4G/5G: Using MEC to Meet the Mission

Grant O'Brien, Manager, Federal Marketing, Verizon •

grant.obrien@verizonwireless.com

ABSTRACT

An effective concept of operations (CONOP) leverages a densified 4G LTE as well as future 5G connectivity to connect thousands of sensors (surveillance, anti-access/area denial, drones, UAS, CBRN, etc.) to provide:

- Operational visibility.
- Predictive posture for base resilience.
- Force protection.
- Command and control.
- Maintenance.
- Community.

Verizon will discuss how a multi-access edge compute (MEC) infrastructure can help to securely and with minimal latency compute data and make decisions at the edge of defense networks where events happen.

BIO: Steve LeFrancois, chief technology officer, Verizon Public Sector, is responsible for leading a team that supports Verizon's federal product/technology direction, services enablement and integrated enterprise solutions development for the customers.

LeFrancois joined the Verizon Business systems engineering team in February 1992 and has been actively involved in global, large-scale program management, systems integration and telecommunications practice areas along with the evolution of the international and managed services solutions within the federal government business sector. He brings more than 20 years of industry experience in support of IT and network solutions.

Prior to joining Verizon, LeFrancois held engineering positions at AT&T and Teledyne Brown Engineering where he developed a diverse background in advanced sensor platforms, systems analysis and back-office system development. He has played a key role in the design and deployment of IT and network solutions for the Department of Defense, Intelligence Community, Department of Homeland Security and federal research and engineering organizations.

LeFrancois graduated from the University of Virginia with a degree in electrical engineering.

Integrating the Analyst, the Logic and the Machine Into Defensive Cyberspace Operations

Philip Mar, Vice President/CTO Gouvernement Systems, Viasat Inc. •

phil.mar@viasat.com

ABSTRACT

Viasat is a global communications company that believes everyone and everything deserves and can be securely connected. It delivers secure connectivity with the capacity to change the world on the ground, in the air and at sea to diverse customers ranging from residential subscribers to the president of the United States and everything in between, including the Department of Defense (DoD) on the tactical battlefield. Its networks deliver more than 455 terabytes (TB) of data a day to users. The company ingests, processes and analyzes more than 30 TB a day to create and visualize network performance and cyber situational awareness (SA) using network, device and user behavioral analytics.

The company's Cybersecurity Operations Center (CSOC) is responsible for defending Viasat's and the organization's customers' owned and operated networks to make them cyber resilient even from advance persistent threats, including those from nation-states and those sponsored by or working directly for them. It uses a data and intelligence-driven, cognitive approach that continuously learns to augment and grow Viasat and the organization's customer's capabilities. This includes a 24/7/365 defensive cyberspace operations (DCO) capability that leverages Security Orchestration Automation and Response (SOAR) to create a force multiplier capable of analyzing and responding to more than 2.5 billion security events per day. The types of responses include but are not limited to cyber investigations, detections and real-time incident notifications to each of the individual customers that includes a recommended course of action (CoA).

One of the challenges of DCO is the sheer number of alerts generated by security tools. Cybersecurity teams today are already inundated with alerts, resulting in "alert fatigue." A survey conducted by the Cloud Security Alliance of cybersecurity professionals recently found 40.4% say the alerts they receive lack actionable intelligence to investigate and another 31.9% report that they ignore alerts because so many are false positives.

This problem is only getting worse with the number of connected Internet of Things (IoT) devices predicted to reach more than 20 billion by 2020. These are becoming more commonplace everywhere, including in government enterprises and Defense Department tactical networks. A recurring pattern in high-profile data breaches is that intrusion alerts and alarms do go off, but because of the sheer number of alerts being triggered, they simply get ignored. This is exactly what happened in the Target Breach of 2014, which cost the company \$252 million and led to the resignation of its CIO and CEO.

Many organizations feel like their cyber warriors are spending too much time clearing through meaningless alerts. Viasat did too, but today the organization’s security analysts are enjoying the CSOC life with all the details they could want right there on their dashboards, while the organization’s alerts fine-tune themselves with workflow action human input. With the help of SOAR and artificial intelligence that provides contextual information as to why the alert fired, the company has moved the security analyst from in-the-loop to on-the-loop. It can respond to attacks at network speeds (i.e., no analyst interaction required).

BIO: Phil Mar is vice president/chief technical officer for government systems at Viasat. Mar is responsible for managing the cybersecurity business division, cyber technology development and strategy for all of Viasat, as well as overseeing overall information assurance and cybersecurity for many of the company’s satellite systems.

He has been with Viasat for more than 29 years. As an expert on both systems architecture and security design, he has led the design of a variety of satellite and wireless communications systems and secure network systems. In the past eight years, he’s led the application of big data analytics in the cybersecurity.

Mar has a BSEE and MSEE specialized in secure communications.

The Modernization of Protection Beyond the Firewall With AI

Mike Price, Chief Technology Officer, ZeroFOX • mprice@zerofox.com

ABSTRACT

ZeroFOX provides visibility into and protection against rapidly emerging threats, malicious actors and TTPs that leverage social media and other digital communications platforms to influence political campaigns, execute phishing cyber attacks, steal PII, embarrass government leaders and departments, defraud citizens, hijack official account, spread malware, misinform the public and more.

ZeroFOX leverages at-scale data ingestion and artificial intelligence (AI)-based analysis to complement human intelligence curated from social and digital sources via highly contextualized alerts. The ZeroFOX platform provides comprehensive AI capabilities for efficient and effective risk identification via a combination of computer vision (CV) and natural language processing (NLP) tools. These capabilities allow agencies to take advantage of the opportunities digital engagement offers, particularly in multi-language text, image and video monitoring, while mitigating the risk that different digital platforms introduce. Through continuous investment in a sophisticated AI toolbox, ZeroFOX is always improving technical capabilities to ensure that intelligence teams can work smarter and faster.

Benefits offered by the ZeroFOX Platform AI capabilities include:

- **Extracting meaning from visual mediums:** With computer vision tools, security teams get clearer indications of threats that may have otherwise gone undetected through traditional analysis. Often an image itself is the only sign of a threat or issue within a post, either in the case of the text within that image or the suspicious use of an image altogether, such as an impersonation of personnel. To address these challenges, ZeroFOX offers optical character recognition (OCR), face and logo detection and comparison technologies. OCR extracts text from images while image comparison detects the similarities between images even if they are modified from their originals, ensuring security teams don’t miss these hidden risks. Additionally, threatening image detection, useful for early warning of potential violence, can discern objects such as weapons (guns, knives) within the context of pictures and posts.
- **Understanding and interpreting human language:** Language detection and NLP tools save security teams time by reducing false positives and providing deeper analysis than word matching alone. Key NLP capabilities now offered by ZeroFOX include sentiment analysis, which can detect the types and amount of negative sentiment present in text and scam and fraud detection, which assesses the presence of a digital fraud and malicious web links.
- **Using AI tools in conjunction to deliver highly customized and accurate threat detection:** Through FoxScript, users can take advantage of multiple AI capabilities (e.g. language detection and NLP classifiers on text extracted via OCR) and traditional techniques (e.g. wordmatch, regex) with out-of-the-box or customized rules to process large scale content with precise logic to identify and prioritize critical threats.

Essential to the government’s cyber posture is protecting official government-owned digital and social accounts critical to the nation’s communication infrastructure. With ZeroFOX, agencies can enable inline protection and continuous alerting for threats to government organizations and leaders. ZeroFOX also provides threat alerts on domain squatting, accounts attempting to impersonate legitimate government entities or employees across social and digital channels including the deep and dark web.

BIO: Mike Price is the CTO of ZeroFOX. He is responsible for leading and setting the vision for the organization’s technology. He oversees all aspects of engineering, research, development and all other technology operations. Before ZeroFOX, he founded the mobile security company Vulnr. Prior to Vulnr, Price was vice president of engineering at Appthority. In this role, Price collaborated with the engineering team to build industry-leading products with a focus on mobile operating system and application security. Previously, Price was senior operations manager for McAfee Labs.

CYBERSPACE MODELING AND SIMULATION

Cyberspace Modeling Using the Object Process Methodology

Ahmad Jbara, Assistant Professor, Augusta University • ahmadjbara@gmail.com

ABSTRACT

In recent years, the recognition of conceptual models as the underlying source of knowledge about systems has become a pillar of systems engineering, giving rise to model-based systems engineering (MBSE). In MBSE, the model of the system is the evolving authoritative resource for reference about the system.

Cyberspace is a system of systems in that many small and diverse systems comprise the structure as a whole. At its heart, CEMA are designed to posture the Army to address the increasing importance of cyberspace and the electromagnetic spectrum (EMS) and their role in unified land operations. CEMA are implemented via the integration and synchronization of cyberspace operations, electronic warfare (EW) and spectrum management operations (SMO). This dictates a complex system that is very dynamic and continually evolving. Conceptual modeling is the tool to put things in order and to provide an authoritative resource of knowledge.

The Object Process Methodology (OPM ISO 19450) is a conceptual modeling language and methodology for complex systems that integrates in a single view the functional, structural and behavioral aspects of the modeled system using formal yet intuitive graphics that is translated on the fly to a subset of natural language. OPM inventor makes a clear distinction between complexity, which is inherent to the underlying system, and complicatedness, which stems from the way a system model is built using a modeling language.

OPM stands in sharp contrast to other languages and methodologies in several aspects. First, it has a single kind of diagram that combines all the structural and procedural system aspects. This helps to avoid the need to tackle the model multiplicity problem. This problem is because of the cognitive load on the modeler, who is required to mentally fuse the multiple diagram kinds, each representing some aspect of the system using its own symbol set, syntax and semantics. Cyberspace is a domain that experts expect to have many different kinds of diagrams because of its diverse nature. Second, OPM is bimodal: it is both graphical and textual, catering to humans' dual-channel processing. Third, OPM is founded of a minimal universal ontology of objects as things that exist or might exist physically or informatically and processes as things that transform objects by creating or consuming them or by changing their states. Fourth, OPM has built-in complexity management refinement-abstraction mechanisms that include in-zooming, out-zooming, unfolding and folding.

The basic principle underlying OPM is that both objects and processes are first class things. These are complementary essential conceptual building blocks that are equally needed to model a system holistically, representing the two major system aspects: structure and behavior. Objects and processes express the system's structure and behavior in a single kind of diagram. For human-made systems, the third key aspect, the system's function is also represented by showing the main process and the value-delivering operand—the object that the main process transforms, thereby delivering value to the system beneficiaries.

Because of its intrinsic integration of structure and behavior, OPM provides a solid basis for modeling complex systems, and it has been applied to model real-time systems, ERP, multi-agent systems, data warehouses, biological system and Web applications. OPM is unique in that it inherently provides for modeling both physical and cyber informational system aspects and simulate them in the same model.

In particular, a recent work has used OPM as the basis to cope with the cyber-physical gap (CPG). The CPG is the difference between the real state of the world and the way the system perceives it. This discrepancy often stems from the limitations of sensing and data collection technologies and capabilities and is inevitable at some degree in any cyber-physical system (CPS). CPGAME is a conceptual model-based approach to capturing, explaining and mitigating CPG. CPGAME was applied for modeling and analysis of the 1979 Three Mile Island reactor number 2 nuclear accident. Further, I5 is an OPM-based framework for architecting systems of systems. It facilitates a smooth transition from a set of disparate system-centered views to a consolidated, integrated model, which accounts for integration aspects, interface and payload structure and behavior, interconnectivity processes and services and eventually emergent interoperability capabilities.

OPM modeling has been supported by OPCAT, a collaborative modeling CASE environment. OPCLoud is a new cloud-based collaborative OPM modeling environment. Both tools support simulation of the modeled system so that the modeler can better understand the requirements of the underlying system and detects logical errors among the user model.

OPCAT as well as OPCLoud assist to model the qualitative aspect of the system. However, sometimes there is a need to attach some computations to the modeled processes for the sake of better simulation. Recently, OPCLoud has been improved to let the modeler model the quantitative aspect by attaching computations to processes. These computations could be very simple arithmetic expressions, but they could also be code developed in a programming language and directly inserted to the model. This last improvement makes OPM and the supported tools a one-stop-shop where a modeler can model a system from end to end with all required aspects using the same language and methodology.

BIO: Ahmad Jbara received his PhD in computer science in 2016 from the Hebrew University, Jerusalem, Israel. For two years, he was a researcher and an adjunct lecturer at the Enterprise Systems Modeling Laboratory at the Faculty of Industrial Engineering and Management, Technion - Israel Institute of Technology. He was also a faculty member at the Computer Science School of the Netanya Academic College.

Since August 2018, he has been at the computer science department of the University of Connecticut. In August 2019, Jbara will join the School of Computer and Cyber Sciences of Augusta University.

His research interests are in the fields of program comprehension, code complexity metrics, code visualization and conceptual modeling using Object-Process Methodology (OPM). During the course of his PhD studies, he coined the term code regularity and modeled its effect on comprehension. Insights from his MS thesis were adopted in an early version of Internet Explorer. While at the ESML, Jbara was the architect of the OPCLoud, a web-based tool for conceptual modeling.

SMEIR

Ashley Furuta, Business Development Manager, IDS International •
afuruta@idsinternational.com

ABSTRACT

The Social Media Environment and Internet Replication (SMEIR) cyberspace training system offers customers a platform for full-spectrum cyber electromagnetic activities and information operations training within a secure, closed-loop environment. SMEIR replicates Internet architecture and content in a way that is fully customizable, scalable and adaptive to specific customer needs.

A holistic and dynamic training environment, SMEIR hosts realistic replications of major social media platforms (e.g. Twitter, Facebook, YouTube, Instagram), blogs, emails, instant messenger (with peer-to-peer encryption), online news media, government and NGO websites. SMEIR’s Exercise Development and Management Tool (EDMT) is synonymous to the control room of the exercise. Through the EDMT, a user can create virtual networks and generate traffic (both malicious and benign) across all of the networks in the exercise.

The SMEIR platform is built to run teams through full cyber attacks in a sandbox environment. Exercise managers can restrict or deny participant access to portions of the network within the training environment through real-world cyber attacks as opposed to simulated malicious behavior. Tools, tactics and procedures can be tested and reviewed in exercises requiring the identification and prevention of malicious threats. Exercise controllers can monitor and analyze exercise participant network activity through the EDMT to support lessons learned.

The system enables customers to train on the full gamut of cyberspace and information operations—from social media engagement and analysis to network mapping, as well as offensive and defensive cyber operations. SMEIR ensures compliance with intelligence oversight regulations by removing all real-world personally identifiable information and links to U.S. citizens from social media data.

SMEIR can be deployed in multiple ways depending on customer preference: on client hardware, on Gov-Cloud or on a portable IDS server. The portable IDS server utilizes a bare-metal hypervisor and is capable of running without any connection to the Internet, making it ideal for a SCIF or other sensitive facility. Amazon GovCloud offers a secure, elastic load balanced, cloud environment that is only accessible via a secure virtual private network. SMEIR maintains a multi-tenancy architecture and allows administrators to configure the software-defined infrastructure while maintaining control and isolating their environment. SMEIR is flexible in working with systems and requirements to develop the best implementation for each customer.

BIO: IDS International’s Social Media Environment and Internet Replication (SMEIR) began in 2013 on government-owned, closed-loop, wide area networks at the U.S. Army’s National Training Center and Joint Readiness and Training Center. SMEIR’s initial mission was enabling Army units at corps and below to research and assess social media content as well as enable psychological operations, civil affairs and public affairs digital population assessment and engagement. It has since grown to incorporate Special Operations Force’s training needs.

Modeling and Simulation of ICS Environments for Cyber Situational Understanding

Mary Anne (Harasim) DeHart, Director of Extended Enterprise, IntelliGenesis LLC • maryanne.harasim@igenmail.com

ABSTRACT

Simulation of industrial control systems (ICS) is a crucial step to improving cybersecurity, resiliency, cost effectiveness and user training. Unfortunately, the staggering complexity and variety of these systems often leads to partial simulations that mimic only one part of the entire system’s functionality. An all-inclusive SCADA simulation would require simulating the functions of a wide array of highly specialized devices that change rapidly and function at multiple layers: physical device, logic device, communications and human interface.

The company’s approach focuses on simulating high-level events that impact devices. By abstracting the system into objects with causal relationships, IntelliGenesis will develop a system that simulates the activity across a network of objects. It will automatically detect the objects in use on the network and their relationships based on a catalog of known devices. Then, it will construct a graph based on these relationships and simulate the network’s function. Users can edit this graph or create their own from scratch. Users can then interact with the simulation by disabling objects, forcing failures or injecting external events, showing the resulting impacts. External events can range from cyber threats to natural disasters.

This approach allows for creating what-if scenarios for evaluation, planning and training. Fictional scenarios based on the real-world architecture in the user’s environment enable the user to see how the simulation executes to spot places for improvement or potentially train operators on the correct actions to take to prevent a threat as it occurs. Simulations will have play/pause/rewind controls so that the outcomes can be examined and traced to causes. For this case, the simulation is given a set of starting conditions, then a series of forced actions are injected into the active simulation to create a real scenario.

For example, imagine a reservoir that pumps water to a water tower. There may be control devices that control the flow of water to the tower. IntelliGenesis can simulate what happens when a hurricane pours six, 12 or 18 inches of unexpected rain on the area. What are the effects on devices in the surrounding area because of the physical presence of extra rain? What are the domino effects on other devices that they are physically or logically connected to? If any of the control devices fail, will too much water be pumped into the tower? What happens if the tower bursts? The company’s simulation will enable users to visualize impacts and plan for these occurrences.

The company will support the ability to build more sophisticated and full-featured simulations for devices. There may be cases where a simulation requires a more detailed implementation of a device to glean the needed information. For this reason, the underlying simulation logic for all devices will be customizable to the extent necessary for a simulation. This will also support lower level analysis of impacts while preventing short-term obsolescence.

BIO: Guy Howard currently serves as lead engineer for IntelliGenesis. He possesses more than 16 years of experience in full life-cycle software development and engineering across multiple contracts and projects within the federal Intelligence Community. On these projects, he has integrated novel AI approaches to automate and optimize system performance, framed system infrastructure, and developed and implemented various algorithms, rules and analytics. Howard also has management experience leading such development teams to design and build state-of-the-art data processing platforms. He holds a BS in computer engineering and an MS in technical innovation management.

Deeper Analysis Capability at the Speed of Cyber

Jeremy Martin, Senior Solutions Architect, NexTech Solutions •

jeremy.martin@nextechsol.com

ABSTRACT

Enhanced Network Visualization Environment (ENVE) is a suite of cyber products that offers visualization and automated analysis of passive network data. This unique solution enables deeper and accurate insight of network data while having the capability to be delivered as a full stack or modularized set of products.

Key features:

- Reverse engineers a network and automatically generates a physical network topology.
- Provides real-time situational awareness of traffic on a network.
- Passively fingerprints devices on a network, characterizing nodes with detailed information.
- Includes intuitive interfaces that allow easy understanding of large, complex networks and fast search, retrieval of network artifacts.
- Automatically illuminates anomalies on a network, with machine-guided behavioral prediction of network activity.
- Aggregates outputs of network analysis into standardized and customizable reporting for dissemination.
- Extends capability through integration with other systems, both upstream and downstream.
- Delivers as a cloud-ready or deployable hardware solution.
- Supports all necessary infrastructure, platform and enterprise service needs to deliver an ATO-ready and hardened solution

ENVE Suite of Products:

FRONT END

- Catalog - Data management tool that enables searching, understanding and managing network artifacts.
- Curator - Reporting tool that aggregates work products in a user-editable form for PDF publishing.
- ThunderRidge - Network Visualization user interface (UI) that facilitates discovery and analysis through network graph topologies.

BACK END

- Cartographer - Processing engine that utilizes algorithms to translate network data into detailed representations of networks.
- JAM.L - Artificial intelligence (AI) built to answer questions about network endpoints.
- Librarian - Data catalog that indexes disparate network artifacts including network captures and configurations.
- Winnow - Processing engine that enables the construction of network artifacts, fingerprints and protocol reverse engineering.

SERVICES

- Enterprise Services - Full Stack of IT Services to satisfy operational needs in a secure environment.
- Platform Services - Application scaffolding to enable big data processing, orchestration and DevSecOps.

INFRASTRUCTURE

- Cloud Infrastructure - Secure, distributed infrastructure to support distributed operations.

HARDWARE

- Deployable Sensors - Hardware product to support cyber operations.

BIO: Jeremy Martin is a senior solutions architect at Nextech Solutions. He has more than 13 years of technical administration, engineering and architectural experience. His diverse background has included assignments with Marine Corps aviation units, U.S. embassies, Joint Special Operations Command and as a technical advisor to Defense Department/federal agencies. Currently, he is devoted to modernizing the tactical edge through automation, software-defined networking and virtualization/containerization.

Cyber Operational Risk Tool (CORT)

Geoffrey Embrey, Director of Army Programs, Noetic Strategies •

geoff.embrey@gmail.com

ABSTRACT

Commanders in the armed forces have enterprise and tactical assets located across the globe, the most critical of which must be monitored and protected efficiently and effectively to ensure mission assurance. This monitoring and protecting must be done with the limited cybersecurity resources that are available to each command. Through an automated capability, the Cyber Operational Risk Tool (CORT) provides commanders with situational awareness and understanding of mission based risk assessment of the cyberspace domain, informing intelligence driven decisions. CORT, a research and development (R&D) project, has the capability to ingest criticality, vulnerability and threat data (both automatically and manually), calculate risk to mission based on these attributes, and display all in views and a central risk dashboard. It provides a centralized capability to quickly identify critical systems and assets that must be protected to ensure mission assurance and enable prioritization of limited cyber resources.

CORT is a government off-the-shelf (GOTS) tool that uniquely fills a gap not filled by any current GOTS or commercial off-the-shelf (COTS) tool. The initiative started as a proof of principle cyber mission assurance visualization software tool for the Army Materiel Command (AMC). AMC provided the Space and Missile Defense Command (SMDC)/Army Strategic Command (ARSTRAT) an initial version of the tool and their technical center has further expanded it into a dynamic operational risk tool, providing the calculus to visualize and enable situational awareness (SA) and provide a “so what” impact assessment to a mission.

CORT models detailed critical mission decomposition and supporting Key Terrain–Cyber (KT-C) and Mission Relevant Terrain–Cyber characterization; highlights critical mission/cyber dependencies and relationships; and visualizes emerging vulnerabilities, threats, gaps and seams by cyber domain layer. It enables risk to mission analysis and supports mitigation strategies informed by dynamic, interactive, customizable detail of cyberspace information. It denotes the depiction, perception and understanding of cyberspace as it pertains to a commander’s operational environment and the correlating impact to critical missions, enabling mission assurance-based cyber threat analysis/intelligence and risk assessment.

CORT is a web application utilizing an information system agile development strategy with development stratified in four-week incremental sprints further broken into epics and user stories. It is based on performance parameters and attributes for criticality analysis, risk assessment and visualization and provides the flexibility to leverage and incorporate rapidly evolving technology to ensure cyber situational awareness, risk assessment and mitigation capabilities and remain viable through development, fielding and sustainment.

CORT utilizes many proven risk tools and models to provide situational awareness and risk assessment, including:

- CYBERCOM Risk Assessment Model (vulnerability, threat, impact) to provide the overall framework for combining risk factors into a single value; for deriving threat, vulnerability and impact from sub factors; and applies math behind subjective risk sub factors.

- National Institute of Standards and Technology Special Publication 800-30 Assessment Scale (vulnerability, threat, impact) to provide conversion factors for qualitative to quantitative assessment ratings.
- Army Research Laboratory Security Control Assessor-Validator Risk Assessment Process (vulnerability) to provide a mechanism for assessing vulnerability tied to existing severity valuations (e.g. Security Technical Implementation Guides) with correlating algorithms and formulas; and to provide a baseline for mitigations.
- ARCYBER Activity Capability Access Resources Expertise model (threat) to provide a mechanism for assessing threat tied to threat indicators with G2 community enhancements.
- SMDC KT-C Mapping Methodology Model Tactics Techniques and Procedures (impact/criticality) to provide criticality factors and mission impact metrics.

CORT is on target for accreditation under the Risk Management Framework and to become approved software as assess-only to meet the Army and other government agency's needs by the end of September 2019.

BIO: Geoff Embrey is the director of Army Programs for Noetic Strategies, a small business with a technical focus in cybersecurity and intelligence, software engineering, information technology and programmatic support. As such, he leads teams of system architects, software engineers, software developers and cybersecurity experts who develop and sustain software tools to model, simulate, calculate and visualize risk to both cyber capabilities and the mission sets they support.

Prior to his current position, he served for more than 30 years as a civil servant for the federal government, mostly within the Defense Department construct, all over the globe as an operations research and systems analyst (four years), program analyst (four years) and logistics operations analyst and executive (22 years).

Develop a Knowledge Graph of Spectral Data

Matthew Maher, Lead Data Scientist, Processus Group and Corvus Consulting •

maherm@processusgroup.org

ABSTRACT

Creation of a Spectrum Knowledge Graph provides a structure and common interface for all of users' data and enables the creation of smart multilateral relations throughout their databases. Structured as an additional virtual data layer, the Knowledge Graph lies on top of existing databases or data sets to link all data at scale, be it structured or unstructured. Knowledge Graphs are becoming central to machine learning these days, whether users like to understand the structure of a tactical network by predicting potential connections, detecting interference/use, understand users' behavior of a service or making real-time recommendations.

Four reasons a knowledge graph is beneficial:

- Combine disparate data silos: Knowledge Graphs help to combine disparate silos of data, giving users an overview of all of their knowledge not only departmentally but also across departments and global/international organizations.
- Bring together structured and unstructured data: Knowledge Graph technology means being able to connect different types of data in meaningful ways and supporting richer data services than most knowledge management systems. Organizations will then use this technology to extract and discover deeper and more subtle patterns with the help of AI and machine learning technology.
- Make better decisions by finding data faster: Using Knowledge Graph technology mitigates the inefficient query of disparate datasets by providing more enriched and in-depth search results, helping to provide relevant facts and contextualized answers to specific questions, rather than a broad search result with many often irrelevant documents and messages but no valuable input. Any graph can be linked to other graphs as well as relational databases. With all of these linkages in place, a fully fledged Knowledge Graph can provide enterprises with a solid infrastructure and foundation for any smart application.
- Future-proof your database with standards: Most enterprises working toward their AI strategy assume that external vendors are able to create a black box that funnels their data into an intelligent Knowledge Graph. This also means that these enterprises are highly dependent on external services and are unaware of how their machines are making decisions. Without quality data, it is impossible to get quality knowledge. With an Enterprise Knowledge Graph in place, organizations will benefit from higher reusability of their data when managing data models because their Knowledge Graphs are compliant with W3C standards.

GHOSTS, GreyBox and Other Tools to Enhance Exercise Realism

Tyler Brooks, Cyber Security Engineer: Exercise Developer, Software Engineering Institute • tdbrooks@cert.org

ABSTRACT

Over the past decade, the CERT Cyber Workforce Development (CWD) directorate at the Software Engineering Institute (SEI) has trained a significant number of U.S. government cyber professionals using on-demand and live-fire virtual exercises. Through planning, development and execution of hundreds of cyber training exercises, CWD engineers have identified realism as the core factor in determining the training value of an exercise.

The SEI provides training, education and open-source tools that enable other organizations and educators to improve. A subset of CWD’s tools and methodologies are used to maximize realism within cyber training exercises.

One focus is on quantifying how a sense of realism can be created within a virtual exercise. To accomplish this, SEI will explore the CWD’s R-EACTR framework, which guides exercise developers to ensure that critical factors are sufficiently addressed in order to develop the desired sense of realism.

Using R-EACTR, CWD has realized that an exercise’s virtual environment brings the most realism to an exercise. Because of security concerns, one key feature that is often missing in an exercise is the real Internet. Open-source tools developed by CWD called GreyBox and TopGen enable any virtual network topology enclave to gain quick access to a large-scale simulated Internet that delivers realistic routing infrastructure, web browsing, DNS, email, certificate authorities, a TOR network and more.

The next key factor to achieving maximum realism is creating realistic user activity on hosts and networks. To achieve this, CWD engineers created GHOSTS, a framework for orchestrating realistic non-player character activities. An in-depth examination of GHOSTS capabilities highlights how it can be leveraged by red, white and blue teams to support their objectives while economically creating a sense of realism.

BIO: Tyler Brooks is a cybersecurity engineer at the Software Engineering Institute, working as an exercise developer for the Cyber Workforce Development directorate. For the past few years, Brooks has been involved in creating and facilitating dozens of high-fidelity virtual cyber training exercises for Department of Defense customers. In this role, Brooks is responsible for designing and deploying virtual network topologies, researching and replicating modern adversarial techniques, facilitating live exercises and designing related assessments.

Brooks’ BS and MS in information science have also enabled him to act as a part-time instructor at the University of Pittsburgh. He continues to teach classes at the undergraduate, graduate and professional education levels.

State-of-the-Art Modeling and Simulation (M&S) Supports Mission Planning, Training

Melissa Andrews, Staff Engineer, Splunk • mandrews@splunk.com

ABSTRACT

To prepare personnel for the sophistication and complexity of cyber operations, the Army must depend on state-of-the-art cyberspace modeling and simulation (M&S) to support mission planning, proficiency development and maintenance, and situational understanding and decision-making.

One M&S platform that raises confidence in mission success is delivering an optimal exercise experience that ensures peak performance of applications and infrastructure through real-time monitoring and situational awareness. It features machine learning tools to predict and prevent potentially crippling degradations in service, effective use of data analytics to maximize user experience and consistent use of after-action reviews to drive continuous improvement and optimize user effectiveness and mission readiness.

By maximizing the availability of simulation and training systems, the platform helps operational units address problems faster, make better decisions more effectively and predict and prevent issues before they have an adverse impact on the mission or on user experience. It delivers on those needs by automating the correlation of heterogenous data to remove blind spots and place the performance of individual components in a wider, more holistic context. It also uses machine learning to monitor operations, report anomalies and recommend real-time course corrections.

The platform ultimately improves the operational efficiency and success of M&S exercises by delivering real-time situational awareness of system performance, usage and availability, anticipating asset needs and boosting supply chain efficiencies while reducing time and costs by automating error-prone and tedious manual processes.

BIO: Melissa Andrews has been working with the Department of Defense and technology since 1997. She is a skilled technical presenter and facilitator, adept at working with customers to discover their pain points and helping them use technology to address them, as well as keeping them informed and trained about new advances.

She joined Splunk in May 2015, where she supports Army customers, helping them understand how they can use Splunk to manage all of their machine data as they support the warfighter.

Andrews holds a BS in information systems from Columbia Union College, Takoma Park, Maryland.

Smart Base Network Interoperability with 5G

Grant O’Brien, Manager, Federal Marketing, Verizon •

grant.obrien@verizonwireless.com

ABSTRACT

For Defense Department facilities, future 5G wireless technology can provide a cost-effective platform to help improve network infrastructure and system interoperability. IT systems, networks, wireless/IoT devices and on-base first responders should seamlessly and securely work together to deliver data to the right person at the right place and at the right time.

Interoperability of 5G wireless devices and network can help defense agencies bring network entities together in the future to make faster, more informed decisions with the most current, secure IT modernization tools available and better concentrate on their core missions using virtualization, adaptive learning, automation and AI.

BIO: Steve LeFrancois, chief technology officer, Verizon Public Sector, is responsible for leading a team that supports Verizon’s federal product/technology direction, services enablement and integrated enterprise solutions development for the customers.

LeFrancois joined the Verizon Business systems engineering team in February 1992 and has been actively involved in global, large-scale program management, systems integration and telecommunications practice areas along with the evolution of the international and managed services solutions within the federal government business sector. He brings more than 20 years of industry experience in support of IT and network solutions.

Prior to joining Verizon, LeFrancois held engineering positions at AT&T and Teledyne Brown Engineering where he developed a diverse background in advanced sensor platforms, systems analysis and back-office system development. He has played a key role in the design and deployment of IT and network solutions for the Department of Defense, Intelligence Community, Department of Homeland Security and federal research and engineering organizations.

LeFrancois graduated from the University of Virginia with a degree in electrical engineering.

LOW PROBABILITY
OF DETECTION/LOW
PROBABILITY OF
ATTRIBUTION

Low Probability of Detection/Low Probability of Attribution Assurance

Ron Chang, Public Sector, DoD Account Executive, BluVector •

ron.chang@bluvector.io

ABSTRACT

Cyber Mission Forces (CMF) must make every effort that their activities are not detected, but if they are, attribution to their team or the nation must be minimized. Effective operations require the ability for the CMF to test tools prior to use and determine if the mission can be detected or attributed to a specific toolkit.

Low probability of detection (LPD) verification is achieved through exposing CMF tools to advance malware detection technologies that use a full spectrum of detection techniques including signature-based, dynamic analysis (sandboxing) and zero-day detection that leverages proven artificial intelligence. Through the use of multiple analytic engines, detection can be tested prior to tools being deployed, providing an advanced understanding of the possibility that the mission will be discovered.

In the event that the adversary is able to uncover the operation through the use of advanced detection capabilities, low probability of attribution (LPA) verification will be achieved using a malware family classification engine (MFCE) to test the tool prior to deployment. An advanced MFCE is trained on CMF-provided toolkits and will alert users if any new tooling can be associated to a known toolkit on which the engine had been trained. The analysis uses supervised machine learning and advanced fuzzy hashing techniques applied to the static representations of tool samples.

LPD and LPA verification solutions must support a wide class of tools including those targeting Windows, Linux, Mac and Android operating systems. Testing must be capable across multiple delivery formats including, but not limited to, PDF and Microsoft Office document types. The ability to perform testing and maximum assurance of LPD/LPA using a consolidated platform that completes analysis in as little time as possible will allow the CMF to achieve its mission with the highest degree of success.

BluVector creates solutions that will provide the CMF with the assurance of LPD/LPA through advanced testing. BluVector recently demonstrated its capabilities at a Dreamport RPE event with U.S. Cyber Command, winning the top spot through a test of malware detection systems that use machine learning to find malware obfuscated by red team participants and malware across multiple platforms. BluVector not only detects incoming malware with accuracy and specificity but also trains counter infiltration tools to be more effective, testing red team tactics and capabilities, assuring future mission success.

BIO: Ron Chang is the Defense Department account executive at BluVector and leads cybersecurity solutions for defense-related clients with a focus in Army, Air Force and defense-civilian areas. He has worked in the application of AI/ML, cloud and blockchain technologies to Air Force and other various Defense Department entities.

Chang enlisted in the U.S. Air Force and worked as a tactical aircraft maintenance technician on F-15C/D/E and A-10 aircraft and served in Operation New Dawn. He has a BA from Columbia University in political science, focused in national/international security and international affairs.

Conducting Secure Cyber Missions Using Network Obfuscation and Managed Attribution

Tom Badders, Senior Product Manager, Telos • tom.badders@telos.com

ABSTRACT

Like their counterparts in the physical warfighting domains, cyber operators need camouflage when they conduct their missions. Telos explores how a range of emerging technologies work together to disguise operators and eliminate cyber attack surfaces from the view of adversaries. Such techniques are already in use by the Defense Department, the Intelligence Community and commercial organizations to shield their cyber protection teams and to carry out cyber threat investigations, threat hunting operations and internet-based research.

These capabilities privatize the public Internet using high levels of network obfuscation, multiple layers of encryption and dynamic IP routing and how managed attribution masks the identity and location of personnel to ensure total protection as they conduct their operations. These same capabilities can also hide servers, applications and unified mobile communications to ensure completely private voice, text, video and chat over any device.

Telos offers a better understanding of these techniques and greater insights into how they protect people, assets and operations in the digital domain to minimize operational risk and to help achieve mission success.

BIO: Tom Badders has more than 40 years of experience developing and implementing secure network solutions for the federal government. He has significant experience in secure wireless networking with more than 200 deployments worldwide. His key professional capabilities include: requirements definition and analysis, turning customer requirements into technology solutions for mission success and business and capture management. For the past five years, Badders has been focused on product management, product development and product marketing to develop and deploy software-based cloud networking solutions for the cybersecurity market.

DEVELOPMENT OF ELASTIC COMPUTE, STORAGE AND SERVICES

Leveraging AWS' Hyperscale Cloud for On-Demand Scalability and Elasticity

Mike Colson, DoD Solutions Architect Manager, Amazon Web Services (AWS) •
mccolson@amazon.com

ABSTRACT

Using the AWS Cloud enables the Army to eliminate infrastructure capacity guesswork and leverage a secure cloud operating environment that delivers hyper-scale compute and storage. The AWS Cloud provides nearly infinite capacity to enable customers to scale through features like AWS Auto Scaling groups. The company's capacity enables customers to distribute IT needs across multiple nodes compared to a single large node. By designing applications for horizontal scaling instead of vertical scaling, which is used in traditional IT systems and has limits, the Army can benefit from AWS' massive scale and achieve faster time to value, often without significant cost impact. AWS provides two regions that meet Defense Department Cloud Computing Security Requirements Guide (CC SRG) Impact Levels (ILs) 2, 4 and 5; the AWS Secret Region with DoD CC SRG IL6 accreditation; and the AWS Top Secret Region for Director of National Intelligence (DNI) Intelligence Community Directive (ICD) 503-accredited Top Secret workloads.

AWS Regions and Availability Zones offer the Army the ability to operate production applications and databases that are more highly available, fault tolerant and scalable than would be possible with a single data center. Within the respective AWS Region, Availability Zones are interconnected with one another with fast, private fiber-optic networking, enabling the Army to architect applications that automatically fail over between zones without interruption. The AWS virtual infrastructure has been designed to provide optimum availability while ensuring complete customer privacy and segregation.

AWS On-Premises and Tactical Edge Solutions

AWS Outposts provides fully managed and configurable compute and storage racks built with AWS-designed hardware. When using AWS Outposts on premises, additional AWS Outposts racks can be requested through the AWS Management Console and added to the on-premises deployment, scaling the amount of compute and storage available and rebalancing the workload without a rebuild. The native AWS Outposts stack can enable AWS compute and storage to provide a scaled out architecture. The VMware build of AWS Outposts can enable the Army to connect using VMware NSX gateway connectors from existing infrastructure, expanding to the AWS Outposts in VMware deployment and creating the hybrid cloud environment.

Hybrid cloud offerings are built to use the value and elasticity of cloud with the low latency and connectivity loss resilience of on-premises capabilities. AWS will ensure that operational capability meets the Army's Service Level Objects as it designs and implements the hybrid cloud solutions for each location. AWS provides cloud solutions such as AWS Outposts and AWS Snowball Edge, which can operate in a disconnected state and remain operationally available. Existing resources provisioned on AWS Outposts are not affected by lapses in network connectivity. AWS Snowball Edge is a data migration and edge computing device that can be clustered to support mission requirements and operate with limited or no network connectivity.

AWS can also leverage AWS Snowball Edge devices to provide compute and storage in disconnected Army locations or in tactical field exercises.

BIO: Mike Colson is Defense Department solutions architect manager for AWS supporting its U.S. Army, U.S. Air Force and COCOM customers and resides in the Washington, D.C., metropolitan area.

Modular Enterprise-Grade Computing Power and Scale for the Tactical Edge

Duncan Stewart, Director of Strategic Development, Axellio Inc. •

duncan.stewart@axellio.com

ABSTRACT

The volume, velocity and complexity of data being ingested at the tactical edge on the modern battlefield presents both an opportunity and a challenge. Developing the ability to harness this information to enable real-time human-in-the-loop and automated decisions is quickly becoming the next great arms race. Near-peer adversaries, most notably Russia and China, continue to invest heavily in information warfare tools. For the U.S. and its allies to maintain their technological advantage, they must fundamentally change the way they compute, store and move data around the tactical and strategic theatres – and this starts at the infrastructure from which they manage and rely on for computing power and ultimately real-time decision making.

During a two-year Skunkworks effort with Intel, the world-class engineering team at Axellio Inc. created the revolutionary FabricXpress platform (FX), built with an architecture that takes hyper-convergence to a new level of performance and dramatically leap-frogs the normal industry product development cycle. The secret sauce of FabricXpress architecture is an innovative internal PCIe switching design to push and drive greater efficiency from commercial computing components and protocols. The architecture creates a super highway to internally connected devices that not only enables 10 to 30 times data transfer speeds but also allows 3 to 10 times greater density of processor and storage capacity. FX holds several records for IOPs, transfer rate and latency compared to traditional servers, storage area network devices – both bare metal and in hyper-converged cluster.

The system is designed with modularity and flexibility at the forefront to take on the most demanding of missions. The design includes swapping in the most advanced non-volatile memory express (NVMe) flash, graphical processing units (GPUs) and supports a variety of smart network interface cards, including but not limited to FPGAs and GPS timing cards. It also fully embraces an open architecture that enables swift assimilation of new customized or commercial components.

The Air Force recently awarded Axellio a rapid innovation contract to convert the organization’s traditional platform—a 2U or 3U chassis housing two Intel servers and up to 1 petabyte of NVMe storage deployed as a rack mounted hyper-converged cluster— into a carry-on suitcase fly-away kit for man-transportable mission efficiency in contested environments.

When employed in a tactical/hybrid cloud architecture, FabricXpress platforms significantly enhance the ability to adapt and scale to any mission, including operations in disconnected and contested environments. For the first time, warfighters can enjoy enterprise-grade data center performance and scale without the need to transport, install and maintain racks of gear at forward operating bases, tactical operations centers, or when on the move. To fully exploit this discovery, Axellio Inc. focuses on applications in advanced analytics appliances and edge computing, including the increasing demand for artificial intelligence and machine learning.

FabricXpress technology features various applications and uses to drive down SWaP, while increasing the computing power that can be brought to the field. Also, Axellio can describe ongoing high-profile projects related to multidomain targeting, missile defense, cybersecurity and satellite control.

BIO: Duncan Stewart is the director of strategic development at Axellio Inc. headquartered in Colorado Springs, Colorado. Stewart is a 24-year Air Force veteran with a wide range of experience developing advanced military avionics, managing fighter and airlift aircraft operations and leading global logistics efforts at the combatant command level. He is the former CEO of the Colorado Springs Technology Incubator and has been intimately involved in numerous high-tech startups in the medical, aerospace, software and telecommunications industry. He is currently the chairman of the board for ConcealFab (cellular equipment) and Maxletics (media analytics) and a board director for Lamina Systems (advanced sensors) and FalconWorks (biomedical devices). He has a BS in management from the U.S. Air Force Academy, an MS in aerospace management from Embry-Riddle and an MBA from Notre Dame.

High-Performance Edge Computing in a DIL and Contested Environment

Bill Burnham, Chief Technology Officer, Public Sector, Hewlett Packard Enterprise • bill.burnham@hpe.com

ABSTRACT

When the Army assesses deployed communications capabilities, size, weight and power (SWaP) have always been the three measures used to constrain deployable communications sets. A battalion on the move has been limited in the amount of compute capability it is able to carry, which therefore limits the level of automated decision support systems the commander closest to the threat can benefit from.

With the emergence of artificial intelligence and machine learning (AI/ML) as combat force multipliers, it would seem that the constraints of SWaP would forever limit how far forward the U.S. forces can deploy AI/ML tools, but those concerns are over. Hewlett Packard Enterprise has built four of the most powerful data center quality compute servers into the smallest form factor, able to operate in 135 degree heat and powered by a standard 110v power outlet, or 12v to 48v DC battery power. AI/ML can now be carried to the most forward edge of the battlefield and provide insights to commanders that will make the operational force more lethal and more survivable.

BIO: Bill Burnham is the chief technology officer for Hewlett Packard Enterprise’s U.S. Public Sector Business Unit. Burnham joined HPE in 2018 after seven years of federal service as the Chief Technology Officer for the United States Special Operations Command, responsible for the innovation/modernization of the global information and services networks supporting 70,000 special operations users. Prior to his service as a government civilian, Burnham was a career active duty Army officer with the majority of his assignments in tactical/operational special operations units and joint tactical communications units supporting deployed special operations forces.

Recognizing and Adjusting Data Services in a Contested Communications Environment

Brent White, Data Analytics Specialist, Iron Bow Technologies • brent.white@ironbow.com

ABSTRACT

Data Management:

Leverage holistic, integrated hardware/software data management platform to facilitate information sharing and management as well as enable a comprehensive management strategy for mission data.

A continuing Army challenge is management of the data it generates. Cyber is a particularly notorious offender when it comes to both data volume and velocity. Newer generation storage appliances are designed to handle the higher volumes and velocities (i.e. Flash storage); however, actual management of the data has lagged and is typically siloed into proprietary systems. Pure Storage’s unique business model and integrated data management platform has been disrupting the enterprise storage market with performant Flash storage and a holistic, hybrid cloud native data management platform that is driven by operational simplicity and effective use of both technology and robust APIs. The platform allows for data to be curated at an enterprise level and leveraged in any environment, including outside Pure Storage systems (Amazon EC2, for example) and align with Army strategic data management objectives.

Pure has validated designs to integrate with Cisco UCS (GEF) to maintain operational efficiencies and simplicity at the compute layer; has converged infrastructure offerings for this design called FlashStack; and has a complete product portfolio available as a service, including FlashStack.

Evaluating a standardized, multidomain platform would provide a set of baseline capability metrics and features for best-in-class infrastructure and data management from which to evaluate current and future capabilities and mission sets. Additional features of the Pure Storage business model provide additional value but are outside the scope of this paper. The company recommends requesting a full briefing.

Transforming Enterprise Ops to Multi-Domain Starts with Search:

Evaluate capabilities for enterprise distributed search, hybrid cloud and enterprise analytic platforms. The nature of the Army’s DCO mission can frequently make physically centralizing data in a timely fashion simply impractical if not impossible.

Data sharing between locations is a time-sensitive endeavor for mission effectiveness and program efficacy. Utilizing fully licensed implementation of Elastic will allow the Army to evaluate the effectiveness and mission impacts to clustering analytics, distributed search and unsupervised machine learning on data sets as a baseline of industry capability in this arena. This allows for metric development to assess current and future

platforms and capabilities to scale, tailor and stay ahead of adversaries. This also works in conjunction with and as a demonstration of enterprise data management.

Elastic can search across petabytes of cyber, geospatial, security, application and sensor data. It can reveal unknowns, patterns and threats with unsupervised machine learning and enable joint missions for tactical edge computing and aggregate intelligence. It is designed for continued effective communication defending against cyber in future large-scale multidomain combat operations with agility and capability for distributed search. Effectiveness for joint multi-domain operations also requires document-level (field/cell) security that restricts the information users can access. Combining role-based access control (RBAC) and attribute-based access control (ABAC) mechanisms enables use of data attributes to restrict access to documents in search queries and aggregations.

BIO: Brent White is Iron Bow Technologies’ specialist for data analytics. His background is in multiple analytics solutions and many storage technologies.

Advanced Multi-Domain Cyber-Comms for Contested Tactical Environments

Harris Nussbaum, Solutions Architect, Mission Solutions Group •

harris.nussbaum@missionsolutionsgroup.com

ABSTRACT

Although there is a predominant move to cloud, a hybrid approach will be the standard in the future because of the inherent issues with using the public or government clouds. Most importantly, this assertion has to do with when something goes wrong. In the larger cloud environment, individuals are simply a number. If a mission system has an issue, the organization’s ability to troubleshoot and repair is completely dependent on the cloud provider, as the organization’s access to systems and resources below the virtual machine are limited or nonexistent. Users are beholden to the speed at which that cloud provider moves through its support tickets and arrives at the organization’s problem.

The continued application of virtualization across each architectural level has enabled the abstraction of compute, storage and networking away from the hardware. Mission Solution Group’s solution involves the automation, integration and orchestration of virtualized compute, storage and networking in a method that allows a virtual infrastructure to adapt natively in support of system demand throughout any connected and authorized physical device.

Any hardware component connected to the company’s system is viewed simply as a resource supporting the virtualized infrastructure. The physical location of that hardware does not matter. It may live in a data center controlled by an AWS or Azure service provider; it may live in a co-located data center; or it may live on-premises at a base or on a ship. The physical location of equipment may be determined separately, and the allowance of utilization is governed by business rules vice technological limitations.

The second part of Mission Solution Group’s solution involves communicating differently. The company applies a virtualized network overlay solution that integrates agnostically to any device that is communicating using traditional TCPIP methods. In this description, TCPIP should be related to a single-path communications system, subject to man-in-the-middle attacks and the bottlenecks that occur within existing infrastructure(s).

To solve this problem, the company applies a product that captures the TCPIP traffic flow, then re-encrypts and converts the traffic into UDP. The data is then fragmented into smaller, non-descript data-elements and prepared for transport. A separate service determines which available path has the lowest latency at that time, regardless of the communication medium and independently sends each element down a randomly rotating pathway. There are several effects because of the speed and throughput is increased significantly, while improving the company’s cyber defense ability during transit. An additional method of threat detection is also enabled because Mission Solution Group can apply the following simple logic to any traffic ap-

proaching any part of the company’s system: If traffic is anything other than UDP, Then THREAT. Immediate action may then be taken in a fashion decided on by the business rules of the stakeholder organization.

Combining this type of communications with the further abstract of application functionality into products like Kubernetes and Docker allow control systems governed by business logic and rules to automatically protect, move and adapt the virtual infrastructure supporting the company’s applications.

BIO: Harris Nussbaum is a former signals and signals intelligence operator and analyst with experience in signal detection and exploitation, EW and EA, cryptography and communications systems while serving as a sergeant in the Marine Corps. After serving in the Corps, Nussbaum has been part of the design, build and integration teams building various tactical SIGINT and EA/EW products, including Communications, Collection and Electronic Defeat. More recently, his career has taken a systems architect path where he has designed and overseen the production of enterprise software/hardware products and systems for customers in both the commercial and federal spaces.

Building a Resilient, Unified and Scalable Data Platform

Ben Ogden, Architect, MongoDB • ben.ogden@mongodb.com

ABSTRACT

The modern Army is a data-driven organization. The effectiveness of critical decisions are directly impacted by the quality, accessibility and availability of the data on which those decisions depend. How quickly the warfighter can access and act upon information with confidence is a key competitive advantage against adversaries.

The Army has numerous data silos, each having varying representations of similar data, levels of governance and quality. Decision-making based on siloed data is time-consuming and difficult. Users are presented with conflicting information from various provenance and quality.

Existing Army systems face the challenge of managing evolving and unstructured data. They often lack in their ability to protect the data through modern security and audit controls. Inconsistent data management across the enterprise can adversely affect decision making and push the Army further from its goal to be a data-driven organization.

Army leaders must be able to see, share and act on unified, accurate and quality data from anywhere at anytime. A single view solution:

- Gathers and organizes data from multiple, disconnected sources.
- Aggregates information into a standardized format and joint information model.
- Provides holistic views for connected applications or services, across any digital channel.
- Serves as a foundation for decision making.

Organizations have long seen the value in aggregating data from multiple systems into a single, holistic, real-time representation of a business domain. For many organizations, successfully delivering a single view has been elusive. Technology has certainly been a limitation. For example, the rigid, tabular data model imposed by traditional relational databases inhibits the schema flexibility necessary to accommodate the diverse data sets contained in source systems.

MongoDB, the leading database platform for modern applications, is uniquely suited for this task because of its flexible data model that makes it easy to store and combine data of any structure within the database without giving up sophisticated validation rules to govern data quality. The schema can be dynamically modified without application or database downtime.

MongoDB provides horizontal scale-out for the single view database on low-cost commodity hardware. It also maintains multiple replicas of the data to maintain database availability. Replica failures are self-healing, and single-view applications remain unaffected by underlying system outages or planned maintenance. Replicas can be distributed across regions for disaster recovery and data locality to support global user bases.

MongoDB provides robust access controls via LDAP, Active Directory, Kerberos, x.509 PKI certificates and role-based access control. Data anonymization can be enforced by read-only views. Data in flight and at rest can be encrypted to FIPS 140-2 standards and an auditing framework for forensic analysis is provided. MongoDB also has an approved DISA STIG.

MongoDB has developed a reference architecture for implementing a scalable, efficient and secure single-view platform. The reference architecture, relevant to enterprise architects and engineers who are responsible for crafting solutions that gather data from various, disparate sources, outlines how MongoDB drives a single view and discusses common components, architecture patterns and key considerations required to build the single view.

BIO: Ben Ogden is an architect at MongoDB with more than 20 years of full stack software development experience and a key contributor to multiple DOD and IC programs. Ogden works with MongoDB's largest federal and commercial customers to turn complex data challenges into simple and performant solutions. He is also a technical advisor for the MongoDB Startup Accelerator.

Prior to MongoDB, he ran a software consultancy, was a technical editor for Manning Publishing and worked as a software engineer at Amazon Web Services.

Ogden studied computer science at the University of Maryland. He is an active speaker in the software and database community, most recently at MongoDB World 2019 in New York City, MongoDB.local events in Washington, D.C. and Atlanta, and MongoDB User Groups (MUGs) in Baltimore, Washington, D.C. and Virginia.

Multi-Domain Data Management in a Contested Communications Environment

Gregory Gardner, Chief Architect, Defense and Intelligence, NetApp •

greg.gardner@netapp.com

ABSTRACT

The beginnings of multidomain operations can be seen on today's battlefields. For example, air operations centers have made significant advancements to fuse space, air and some nascent cyber effects to support the joint fight.

There is similar progress in land and maritime operations centers. Yet all remain stovepiped to one degree or another. To compound this challenge, the continued growth in unmanned, sensor and networked devices—and the vast amounts of data they generate—drives the need for larger, more capable and more diverse communications systems. These systems must improve jam-resistance and low probability of detection to keep pace with adversaries' growing electronic sophistication and adapt to fast-changing operational environments. Yet, today's military communications architectures are static and inflexible with poorly managed data that rarely crosses the boundaries of operational domains.

Multidomain operations demand an adaptive data management architecture motivated by processes from the commercial world, which allow refined, cleansed data to be delivered where it is needed, when it is required regardless of domain boundaries. This vision embraces the diversity and multiplicity of network types across platforms in the multidomain battle space to provide highly reliable, networked and scalable data to every element of the fighting force.

Just like in the military, business leaders are under tremendous pressure to harness today's wealth of data and apply it intelligently to create new value across the entire organization—all with limited time, skills and budget. At the same time, their data is no longer locked away on devices hidden behind firewalls. Instead, it is becoming distributed, dynamic and diverse—and the resulting amount of data can be overwhelming and incredibly difficult to manage.

Thriving in this environment for both military and commercial entities requires creating a data-centric organization, which is no small undertaking. It also requires a holistic approach to managing data that is secure, efficient and future-proof and provides freedom of choice.

Put simply, the requirement is for a data fabric that delivers any data to any authorized user, anytime, anywhere securely limited by policy not technology.

NetApp delivers data in that manner today to diverse, global commercial customers, like DreamWorks, producer of sophisticated animated movies. The same capabilities are available to facilitate multidomain operations.

Here’s how:

NetApp ONTAP 9, the industry’s leading enterprise data management software, combines simplicity, flexibility and security with powerful data management capabilities, proven storage efficiencies and leading cloud integration. With ONTAP 9, organizations build intelligent hybrid clouds that span flash, disk and cloud. They flexibly deploy storage on their choice of architectures—hardware storage systems, software-defined storage (SDS) and the cloud—while unifying data management across all of them. Globally diverse organizations accelerate their enterprise applications with flash without compromising the essential data services that they need. And they seamlessly manage their data as it flows wherever it is needed to help leaders at all levels make the best possible decisions for their organizations.

With ONTAP, users get a comprehensive, industry-leading portfolio of storage efficiency capabilities that work together to minimize storage costs, reduce SWAP and maximize data storage. Built-in application workflows enable users to quickly and confidently provision storage for key workloads in less than 10 minutes. These workloads include Oracle, SAP, SQL Server and virtual desktops and servers. Rapid application deployment and data access speeds technology adoption and enhances superiority over adversaries.

NetApp simplifies data management processes to maximize the productivity and responsiveness of IT staffs. ONTAP provides a common set of features across deployment architectures that simplifies operations so that IT teams can focus on strategic and operational priorities. Users unify their data management across hybrid cloud infrastructures easily moving their data within or between storage clusters, or to the cloud—wherever it is most useful. This is the elasticity the Army needs. At the edge, NetApp provides industry-leading performance and the ability to grow and shrink resources on demand on the battlefield. NetApp also offers the ability to burst into larger on-prem data centers or to the cloud as missions dictate.

ONTAP is the foundation for a Data Fabric that gives users flexibility, choice and control across all storage environments. This includes integrating the innovations of today with legacy systems. Government users in particular appreciate that they can grow their systems with the latest hardware, continue to use their older hardware and connect all of it to the cloud. When it’s time to retire a storage system, they can simply upgrade the controllers and keep data in place on the existing disk shelves.

The leading portfolio of security capabilities in ONTAP helps users integrate data security across their hybrid cloud and avoid unauthorized data access. As one of the top providers of data storage and management to the U.S. federal government, NetApp understands the importance of security. NetApp was the first storage provider to achieve Common Criteria (ISO/IEC 15408) certification and be certified and listed on the Unified Capabilities (UC) Approved Products List (APL).

NetApp is ready now to serve as the data authority for multidomain operations. The company already provides the Department of Defense and the Intelligence Community with many data management services, but they are not being optimized. NetApp offers a full range of hybrid cloud data services that simplify management of applications and data across cloud and on-premises environments to accelerate digital transformation. Together with its partners, the company already empowers global organizations to unleash the full potential of their data to expand customer touchpoints, foster greater innovation and optimize their operations. We are ready to do the same to facilitate multidomain operations for the U.S. military.

BIO: Dr. Greg Gardner coordinates NetApp’s development activities in the defense and intelligence arenas. He is a retired infantry colonel with more than 30 years of commissioned service. After his retirement from the military, Gardner was vice president of the public sector strategy at Oracle then returned to government service as deputy CIO for the U.S. Intelligence Community. He has been at NetApp since 2011. Gardner holds a BS in electrical engineering from the United States Military Academy and a PhD in IT management from Capella University.

Advancing Cloud Services in Contested Environment Using Secure Cloud Identity

Andrew Whelchel, Principal Solutions Engineer, Okta • andrew.whelchel@okta.com

ABSTRACT

Multidomain formations are in a race of time to delivery capacity, capability and operational endurance in contested spaces with near-peer adversaries. Meeting this challenge, the cloud provides many unique opportunities to potentially accelerate speed and agility to win this race of time in the contested environment.

A central challenge at hand in the contested environment is to leverage cloud resources as fast and securely as possible to gain organizational speed and agility over adversaries in order to both deliver cyber assets for CEMA and support multidomain integration for combat operations support.

The key to meeting this challenge of effectively leveraging cloud resources to gain speed and agility against near-peer adversaries lies in the ability to take advantage of rapid technology developments in cloud identity, specifically Identity-as-a-Service or IDaaS. This specific development of cloud identity (IDaaS) has significant potential impact to reduce risk in multidomain operations and enhance success of combat operations with abilities to:

- Enable CAC to the cloud capability and CAC to any app access.
- Integrate identity access to AI/ML sources to create AI identity access to resources.
- Secure DevOps resources with secure identity both at time of development/test and delivery (i.e. - ATO on demand).
- Execute Zero Trust network policy protection against known and unknown threats.
- Implement automated cyber defense response based on identity threats to automatically reduce risk in near real-time.

Fundamental to the advancements listed is the ability to both modernize existing applications to enable CAC at the any-app and at-cloud service level. Prior to Cloud Identity, many if not most of these apps remained unavailable to CAC enablement because of significant customization efforts otherwise required. Not only does Cloud Identity enable this but also enables this at the same time as cyber risk is reduced with Zero Trust network policy implementation and cloud-based cyber defense response to identity threats.

Okta offers an operational model to use identity-as-a-service to secure and accelerate access to cloud applications. It also demonstrates how to integrate that operational model to win this race against time to provide speed and agility to multidomain operational task actions. Valuable information includes:

- Understanding the advances in development of cloud identity supporting cloud services and its operations in a contested environment.

- Learning how to apply operational use cases of cloud identity (i.e. IDaaS) to support cloud rapid deployment of cloud services in support of the race to deliver speed and agility to the multidomain formation.
- Learning the tools to develop demonstration capability of the components, interfaces and configurations to deploy cloud identity to enable SSO, MFA, CAC authentication to the cloud, Zero Trust and cyber defense response in the cloud to protect multidomain formations in contested environments.

BIO: Andrew Whelchel, CISSP-ISSAP and CCSP, started in information security and IAM after graduating from the University of Memphis by supporting identity and access management by managing Microsoft Identity for U.S. federal customers. Later, he transitioned to network infrastructure security and consumer identity protection. Most recently, Whelchel has worked in the same role at RSA Security and Okta.

At RSA Security, Whelchel supported financial services, health care, U.S. federal and other customers with a focus on identity risk analytics and integration of identity fraud intelligence for cybercrime prevention. Now at Okta, his focus is on protecting employee and partner as well as citizen consumer identities for the public sector to reduce cyber risk as well as accelerate capabilities for cloud transformation. Contributions include work as a contributor on the NIST 1800-3 ABAC standard and speaking events about identity access management and security.

PacStar Modular Data Center

Charlie Kawasaki, Chief Technical Officer, PacStar • ckawasaki@pacstar.com

ABSTRACT

PacStar has developed a COTS Modular Data Center (MDC) solution ideal for tactical, expeditionary and mobile applications that scales from very small teams at lower tiers to upper echelon workloads all based on a single family of hardware, network functions and software in a small form factor, rugged package. PacStar MDC enables organizations to aggregate data and conduct compute workloads at the edge of the network with the ability to deploy disconnected in FOBs, command posts, vehicles and other network echelons.

PacStar 400 Series MDC is the industry’s smallest, most versatile and most comprehensive modular COTS communication platform purposely designed for rugged use cases. The 400 Series consists of multipurpose server, storage and networking modules in a rugged small form factor (SFF) well suited for extending access to cloud data to the edge of the tactical network. Each module can operate stand-alone or be combined to form large enterprise grade systems with layers of redundancy. PacStar designs, engineers and manufactures the 400 Series platform to maximize capability with the smallest possible size, weight and power (SWaP). This family of products is TRL Level 9 of maturity and has been extensively MIL-STD tested (810G, 461F, 704D) with thousands of units produced and fielded annually.

PacStar is certifying multiple hyper-converged infrastructure, cluster and cloud providers on PacStar’s 400 Series MDC to offer deployment flexibility of software capable of aggregating storage and managing compute tasks. These innovations will provide an ideal platform for hosting myriad applications, containers and virtual environments for deployed warfighters. The solutions allow tactical networks to increase availability and performance of cloud services to the edge of the network.

The core PacStar 400 Series components of the PacStar MDC include PacStar 451 Xeon-D based servers with a single SSD; PacStar 455 Hyper Convergence Modules with up to 8 RAID-protected SSDs, providing up to 64 TB of raw storage; and PacStar 444 GigE switches. These components are typically mounted in a PacStar Smart Chassis with UPS, a PacStar Mini-Transit Case, or a Vehicle Rugged Rack. The modular design of this solution allows users to customize the CPU, RAM and storage capabilities depending on the specific use case.

PacStar also offers IQ-Core Network Communications Manager (NCM) software designed to overcome the complexity and training burden of managing diverse systems without highly skilled deployed administrators. IQ-Core NCM fills that gap by consolidating management under a single pane of glass for organizations attempting to deploy a collection of technologies, as opposed to administering through disparate user interfaces. IQ-Core NCM provides an intuitive interface making communications set-up and operation quick, easy to learn and repeatable, improving mobility and reducing training time. Additionally, IQ-Core NCM includes an extensive role-based access control (RBAC) system that mediates access to all underlying systems.

PacStar 400 Series MDC hardware with IQ-Core NCM is highly portable and highly scalable, providing high performance, high-availability and resiliency, large capacity distributed storage and supports clustering, and making it perfect for onsite tactical edge computing scenarios.

BIO: Charlie Kawasaki joined PacStar in early 2005 to lead the company’s technology strategy and future product roadmap for its proprietary product lines. Kawasaki currently leads PacStar strategic initiatives, investigating and developing new integrated solutions and technologies to meet customer needs, and particularly focusing on areas such as commercial solutions for classified (CSfC), cybersecurity and edge computing.

Mobile Cloud Storage and Compute Advantage

Nick Hopchak, Vice President, Phacil LLC • nhopchak@phacil.com

ABSTRACT

The constraints in physics, current electromagnetic and radiation network communications make rapid data transmission challenging. Shifting operational communications to dedicated transmission time for big data volumes sacrifices mission-first needs while increasing opportunity for peer competitor signal disruption or manipulation threats. To augment large data file transfers through satellite, line-of-sight or other communication means and increase tactical edge or mobile compute capabilities, Phacil LLC has partnered with Amazon Web Services (AWS) to produce an asymmetric solution for terabyte data mobility and compute.

The Snowball is a man-transportable, ruggedized, secure and MRE case-sized module able to meet the operational demands of tactical and mobile cloud storage and compute capabilities. A current model Snowball is 40 pounds and can be customized to offer 42 to 100 terabytes of storage and compute capabilities powered by 24 or 52 central processing units (CPUs). An optional graphics processing unit (GPU) is also available for greater compute needs. Snowballs extend some AWS basic data center functions to include EC2 instance and S3 bucket technologies easing data transfer to AWS environments. Data transfer to any cloud or on-prem environment and is also possible with a Snowball unit. Multiple-module clustering enables compounded capacity for data capture efforts and performance of in-parallel computing. Security controls include AWS’ multi-key authentication and module tamper resistance which renders the drives unreadable should it be physically tampered with or opened.

The Snowball comes with a command line interface to accommodate a broad user community and highly technical IT professionals. Phacil’s SB Manager software replaces the command line interface making it possible for trained warfighters or analysts to easily access, manage and extract the power of the Snowball at the tactical edge without advanced IT professionals. SB Manager is the only available user-friendly interface to automate many of the start-up, data replication, orchestration and synchronization capabilities between Snowball modules or via a connected network. Built as an open architecture management framework, the Dockers-based structure and mesh networking power the multi-module capabilities and ease of integration with applications deployed on the box.

Snowballs can function as part of a broader cloud network or as a local network of multiple interconnected modules. Synchronization and replication only require updating the deltas between modules regardless of network connectivity or direct connection between Snowballs speeding multi-module data capture and mobility between sites, units or commands at HQ or the edge. A strategy that deploys multiple Snowballs transiting across the battlespace brings scale, flexibility and speed with a data capture, muling and compute capability which counters peer competitor electromagnetic threats.

BIO: Rob Maupin has been providing advanced technology services for more than 20 years in areas to include data center, system, software and data science services. As the vice president for strategic initiatives, he currently provides leadership to product development and growth of the SB Manager, Snowball security suite of tools, artificial technologies and Corbomite solutions development for Phacil LLC. He brings his years of experience, AWS cloud business experience and technical professional accreditations to provide strategic and technical engineering consulting, systems architecture, software design and development services.

Defending Data in a Perimeter-less Domain

Rick Tyrell, Senior Systems Engineer, Thales eSecurity • rick.tyrell@thalesdsi.com

ABSTRACT

The warfighter gains a decisive advantage by rapidly analyzing data of many types and from many sources to provide situational awareness to increase operational efficiencies, decision-making and optimize execution of the mission. The data is also the target of near-peer adversaries in the cyber domain. Digital transformation has produced data at a massive scale, which demands elasticity of resources and changes how data is accessed and where it resides, often in elastic hybrid, virtualized multi-cloud environments that requires a nonlinear approach to security.

Just as the linear kinetic battlefield has changed, so has the concept of securing the perimeter in the cyber domain. Defending data affects all aspects of multidomain battle with Army, joint mission partners and coalition forces. It is imperative to the mission that the data being accessed has not been compromised or altered from its original state by utilizing policy-based access control that is enforced by transparent encryption.

The Thales Vormetric Data Security Platform effectively manages data-at-rest security by limiting the users, processes and resources that can access it while providing auditing and alerting to understand the who, what, when and where for real-time protection. The platform is composed of an integrated suite of products built on a common, extensible infrastructure with efficient, centralized key and policy management. It offers capabilities for protecting and controlling access to databases, files and containers and can secure assets while extending unified enterprise policy to data residing in cloud, virtual, big data and physical environments. The platform supports elastic multi-tenant environments and services such as bring your encryption and bring your own key. Secure multi-tenant domains enhance separation of duties, separation of the mission team and mitigates the risks with privileged user accounts.

This multi-layered security approach must expand and reposition to address evolving requirements. This is accomplished by first identifying the baseline traffic flows utilizing the data security manager (DSM), which is a root of trust, performing encryption management and access controls along with key management and key generation. Once these traffic flows are identified, policies lock down any deviations from baseline, providing unaltered, uncompromised data while providing protection from inside or outside threats. Traffic flows are allowed to traverse multiple methods of transport as they are tied to the user, processes and data not by unique host identifiers i.e. Internet protocol (IP) addresses.

More specific capabilities include: file-level transparent encryption for files, databases and containers; format preserving application encryption, key management, tokenization and data masking; and remote administration. The platform is highly scalable, capable of supporting more than 10,000 connections, which has been validated in Defense Department, federal civilian and IC environments. FIPS 140-2 Levels 1, 2, or 3 (Common Criteria certified) configurations are supported. In addition, the platform incorporates the use of AES-NI technology, which is a new encryption instruction set that improves on the Advanced Encryption Standard (AES) algorithm and accelerates the encryption of data in computer hardware to maximize overall performance and minimize any impact of the security overlay.

BIO: Rick Tyrell brings more than 20 years of IT experience applying best-practice principles for secure data transmission, high availability and virtualization for large-scale network architectures. He has expertise in electric and water utility telecommunications infrastructures, including Smart City technologies and IoT. He is part of a team that architect security strategies to protect sensitive data for both federal government and large commercial enterprises across the globe. In his current role as a senior sales engineer, he spends the majority of his time helping customers identify data flows and developing data-centric security approaches to protect the new perimeter.

Enabling Multi-Domain Dominance: Deploying the Next-Generation of Virtualization Capabilities

Matt Holt, Army Account Executive, Trace Systems Inc. • mholt@tracesystems.com

ABSTRACT

Achieving delivery of core services and mission command applications in a contested multidomain environment requires a revolutionary approach to achieve a cost-effective and sustainable solution that leverages emerging technologies for compute, storage and services. Operational requirements are driving Army units across echelons to host multiple mission partner environments (MPE) to support global combatant command (COCOM) requirements that complicate and increase complexity by echelon.

The company’s approach is to use emerging capability on a hyper-converged infrastructure and software-defined networking with unique internal encryption and key management to provide multi-tenant secret releasable (SEC//REL) environments with dynamic shared computing, storage and unique enclave services capabilities. The solution is currently undergoing NSA lab-based security assessment for a risk rating and certification as the Defense Department’s first tactical/deployable private cloud computing multitenant virtualized solution capable of hosting and delivering services and mission command applications for multiple SEC//REL enclaves on a single platform. The platform is the Modular, Dynamic Reconfigurable Integrated Virtual Environment (M-DRIVE) that provides a scalable and dynamic computing and storage across hosted SEC//REL enclaves.

Leveraging state-of-art processing and storage capabilities, this platform can deliver multiple MPE environments on a single platform with extensive reduction in size, weight and power (SWaP) and the number of server platforms relative to current and planned Army server single-enclave infrastructure. The unique system security design and out-of-band management builds in extensive cybersecurity defense in depth attributes. The applicability for the M-DRIVE throughout the Army MPE ecosystem could provide dramatic benefits in closing MPE gaps; collapsing legacy and current MPE infrastructure; and reducing sustainment and deployment requirements with reduced out-year life-cycle cost. Observed during the Army Warfighter Assessment (JWA 19) and in multiple Navy exercises (the technology and NSA sponsor), M-DRIVE demonstrated the ability to host multiple SEC//REL enclaves with dramatic compute and storage benefits in closing MPE gaps and collapsing legacy infrastructure.

This solution placed at echelon across the Army could provide a resilient and redundant capability to mission tailor and deliver MPE environments linked from the tactical to existing COCOM enterprise services level operating across domains in contested/DIL environments. M-DRIVE’s inherent dynamic compute and storage capabilities matched with its SWaP and scalability can increase warfighter agility and operational effectiveness for both deployed and home station environments.

BIO: Matt Holt is the Trace Systems army account executive working directly with the Army Futures Command Network-Cross Functional Team (N-CFT) and Joint Modernization Command (JMC) on this emerging capability and applicability to the Army MPE Ecosystem. Holt is a retired Army Signal Officer with more than 30 years experience operating in complex joint, coalition and multidomain environments from tactical to strategic levels. He has extensive experience in communication planning and leading operations required to deliver and enable mission command in these environments. He has deployed as a former 10th Mountain G6, III Corps G6, USAREUR G6, CTF-MTN CJ6, CJTF-76 J6, NATO IJC and USFOR-A J6 while his numerous operational assignments at the CCMD level exemplify his significant practical experience with the requirements and need to fight in multiple domains.

DEVELOPING TACTICAL TERMINALS UTILIZING DIGITAL RF

Understanding Electromagnetic Operations Framework to Address LPD/LPI

**Sgt. Maj. Raymond Reyes, USA (Ret.), Chief Information and Business
Development Officer, Corvus Consulting LLC • raymond.reyes@corvusgroup.org**

ABSTRACT

In the emergent era of great power competition, the nation's adversaries seek to achieve their strategic aims, short of traditional conflict by the use of a stand-off approach across the warfighting domains. Adversaries will leverage this "grey zone" conflict across political, military, economic, social, information, infrastructure, physical environment and time (PMESII-PT) in an attempt to defeat U.S. power. The importance of cross-functional integrated cyber, electronic warfare and signals intelligence has been recognized for the last decade not only the United States but across near-peer competitors and potential adversaries.

As the U.S. Army builds force structure, doctrine and material capability to meet the needs of cyber-electromagnetic activities (CEMA), one of the greatest challenges is understanding operational enablers/constraints and finding areas to conduct real-world test and evaluation to enable realistic individual and collective training. Communications and aviation infrastructures rely tremendously upon the carefully regimented and controlled use of the electromagnetic spectrum, but there are only a few areas in the United States suitable for conducting real-world electronic warfare and signals intelligence training, key to fighting and winning in multidomain operations. However, an in-depth and comprehensive understanding of the reasons behind these restrictions and of ways to work within them and mitigate them will lead to greater training and testing opportunities and a more powerful and lethal force.

Corvus Consulting can speak to the spectrum and cyber training constraints within the continental United States and across operations and methods to mitigate and work around them in order to achieve a well-trained and integrated CEMA force and in support low probability of detection/low probability of intercept (LPD/LPI).

BIO: Sgt. Maj. Raymond Reyes, USA (Ret.), recently retired as the Army's senior enlisted spectrum manager across the force with more than 30 years of service. Sgt. Maj. Reyes has combat and operational experience integrating electronic warfare and electromagnetic spectrum operations at the Army division, Army corps, service component command, joint task force, combatant command, Army Staff and Defense Agency echelons. Over the past 15 years of service, he engaged across every facet of the Army's force management model bridging tactical solutions with the institutional Army and enterprise-level solutions with the Defense Information Systems Agency. Sgt. Maj. Reyes currently serves as the chief information and business development officer for Corvus Consulting LLC.

Reduced Footprint Terminals

George Khoury, CTO, Government Services, Viasat Inc. •

george.khoury@viasat.com

ABSTRACT

Viasat has been a leader for more than 30 years in the technology innovation of multi-band, multi-network, multi-orbital regime, full-ITU compliant and ARSTRAT-certified terminal architectures and products for BLOS connectivity solutions. Hybrid Adaptive Network terminals maximize warfighter capabilities and resilience by providing simultaneous access to both commercial and Defense Department networks so that warfighters can seamlessly roam across this hybrid infrastructure. These terminals interoperate across multiple networks that span multiple waveforms and networking protocols, multiple orbital regimes—low earth orbit (LEO), medium earth orbit (MEO) and geosynchronous earth orbit (GEO)—and operate over multiple frequency bands, such as X, Ku, Mil-Ka and High Capacity Ka.

This technology innovation involves not only the physical antenna apertures but also the RF electronics components to implement waveform processing and modem functions in a small form-factor package that reduces the overall terminal footprint. First, the SATCOM waveform processing (modem) needs to be integrated into the RF electronics as much as possible: future Viasat terminals will have all the RF, modem and baseband data processing in the antenna assembly. Second, true performance comes from the satellite network: its 60 cm, battery-powered terminals can be set up and operated in minutes, delivering several times the capacity of 2.4m trailer-mounted, generator-powered terminals that require a team of soldiers hours to set up and operate. In the organization’s experience, small terminals provide better system gain (e.g. capacity) than large legacy terminals when they are members of a better SATCOM network.

At the same time, the warfighter requires resilience and choice: any terminal should be able to join multiple SATCOM networks (potentially multi-band, multi-waveform, multi-orbit) where the choice of which network to join is made by the warfighter command to optimize properties such as LPI/LPD/AJ, data capacity, cost, use of U.S. national assets, use of fielded terminals and cybersecurity. To this end, Viasat is working with industry partners and the Defense Department to create the appropriate terminal architecture(s) that meet these numerous and seemingly conflicting goals.

In addition to these innovations, Viasat recognizes that warfighters need to access innovation from across industry and programs of record. Therefore, the Viasat terminal architecture also supports standard intermediate frequency (IF) and M&C interfaces to allow operations with any third-party modems and networks. Through a standard L-band IF interface, any external modem can connect through the terminal and operate on the desired network. Viasat facilitates the terminal certification efforts required to allow the terminal to operate on the target network. The standard M&C interface is provided through OpenAMIP to allow the external modem to control the terminal, point the antenna and apply any configurations required to operate on the target network.

Significant efforts and advancements are being made in the development of terminal architectures that reduce the overall footprint of terminals. This innovative terminal architecture delivers easy operation and rapid maneuverability by minimizing setup time. It also effectively maintains optimized communications, command and control performance on-the-move, providing real-time connectivity, capacity, communications security and situational awareness to commanders anywhere on the battlefield.

BIO: George Khoury, chief technical officer for Viasat’s Government Services, has a background in satellite and wireless communications systems with a focus on market strategy, technology innovation, product roadmaps, systems engineering and data analytics. Khoury has more than 20 years experience in software and hardware development and test, building complex end-to-end communications systems for commercial and Defense Department markets.

ENHANCE SATCOM RESILIENCY

Moving From Purpose-Built Communications and Data Analytics Products to Virtualized Applications

**Michael Beeler, Vice President, Waveform and Analytics Virtualization,
Envistacom LLC • mbeeler@envistacom.com**

ABSTRACT

Envistacom is a world leader in communications waveform virtualization for cloud, public and private data centers, as well as tactical edge products using high-performance computing (HPC) architectures. Envistacom has invested in this transformative technology, enabling the abstraction of modem waveforms and other capabilities from purpose-built, real-time and continuous data processing physical devices to virtualized applications hosted on computing platforms.

As the cloud infrastructure continues to take the world by storm, the computing fabric revolution that is supporting the cloud is being supported by the HPC. The HPC is the combination of the central processing unit (traditional PC processor), combined with a hardware-assisted technology such as a field programmable gate array (FPGA). Tying this all together, advances in computing languages, such as Open Computing Language (OpenCL), have super charged the computing environment to allow extremely complex, logic intensive, waveforms for satellite, cellular, tactical radio and data analytics to now be completely virtualized and supported in the cloud or on stand-alone HPCs and tactical-edge devices.

Envistacom is building a communications and data analytics library for satellite and tactical radio waveforms, enabling next generation warfighters to carry a single hardware platform and allowing support for a multitude of satellite and tactical radio waveforms to be supported on a single hardware platform. To complement the virtualized waveform, distributed data analytics and other real-time and continuous processing capabilities may also be supported at the tactical edge, allowing a major improvement in reaction time being afforded to the warfighter. Envistacom is creating a new paradigm, enabling all waveform vendors to now participate in this new ecosystem. With its strong focus on research and development, Envistacom continues to provide support for emerging technologies to include, but not limited to communications waveforms and data analytics solutions.

As the U.S. government looks to improve its flexibility and reduce its dependence on purpose-built, single purpose solutions, Envistacom provides maximum flexibility and manageability while extending the life of existing deployed hardware solutions. The anticipated benefits of virtualization: The ability to adapt rapidly to meet new, changing and missing requirements and reconfiguration before, during and after a mission is a primary goal of this technology.

Building on the HPC technology, the virtualization solutions may exist as cloud-based or tactical edge-based solutions supported by a growing library of waveforms for satellite (e.g. DVB-S2, DVB-S2X, etc.) and Tactical Radio (e.g. SINCGARS) and data analytics (ground sensors, video surveillance and biometrics). Coupled with Envistacom’s hardware development skills small size, weight and power (SWaP) may be employed to provide extremely small footprint products with the power of full-size HPC processor solutions supporting all of Envistacom’s library of waveforms.

As the U.S. government’s branches and agencies continue to adapt and move to more cloud and flexible mission requirements, virtualization provides the technology that can scale and meet missions to enable the U.S. government to explore innovative ways to transform and deliver a flexible solution to the warfighter. This new paradigm will enable equipment that can provide cross branch and cross agency communications using a common ecosystem.

Virtualization is helping both commercial entities and the U.S. government reconsider their approach and look to a more flexible architecture that supports any and all waveforms on common computing and communications hardware.

BIO: Michael Beeler is vice president of waveform and analytics virtualization for Envistacom located in Frederick, Maryland. Beeler has more than 30 years experience in defense and commercial satellite communications. His career includes a concentration in virtualization of communications waveforms and data analytics, spread spectrum communications, hardware/software design, architecture and modeling and simulation tools for satellite and tactical radio communications networks.

Prior to joining Envistacom, Beeler was the founder/COO of Fast Fit Technologies (purchased by Envistacom May 2019), vice president of Engineering and Chief Engineer of Comtech EF Data. Beeler is founder/co-founder of numerous startup companies, including founder/CTO of Digicast Networks (purchased by Comtech EF Data); founder/CTO Trading Run Communications (purchased by Digicast Networks); founder/CTO GapView Communications (purchased by VSL Networks/Motorola); and co-founder/CTO ViaCast Networks. Early career work included numerous defense and commercial satellite companies such as Hughes, Contel ASC and Pulse Engineering.

Beeler holds 31 U.S. patents in the areas of satellite communications with concentrations in cloud-based and standalone waveform virtualization and spread-spectrum communication, optimization of satellite antenna pointing and bandwidth optimization techniques.

Beeler has an MSEE from Johns Hopkins University, Whiting School of Engineering.

Enhancing Resiliency via Enterprise Management and Control and DSSS Protected Waveforms (SATCOM Resiliency)

Mark Dale, Business Development Director, Kratos RT Logic • mdale@rtlogic.com

ABSTRACT

Satellite communications (SATCOM) are a critical element of the U.S. government Department of Defense communications infrastructure. Today, the vast majority of Defense Department SATCOM utilizes either the Wideband Global SATCOM (WGS) system or commercial transponded satellites that are susceptible to interference. Because of its importance supporting military operations, in the future adversaries may seek to deny, degrade or otherwise impair the department’s SATCOM capabilities.

Because of SATCOM’s importance and potential vulnerability, the Defense Department is actively seeking cost-effective means of increasing SATCOM resiliency. A potential solution that is a combination of two key enablers is available.

The first enabler is the Enterprise Management and Control (EM&C) SATCOM architecture. EM&C provides resiliency by enabling ground terminals with the capability to automatically and flexibly access multiple satellite networks and related ground infrastructure. This capability enhances resiliency by providing path diversity in the event that one or more networks are degraded or denied. EM&C is an end-to-end capability that involves adding key functionality to ground terminals and the LEO/MEO/GEO satellite networks they access.

EM&C functionality can be cost effectively integrated into existing terminals. Prototype EM&C capabilities have been recently delivered providing a proof-of-concept and contracts for follow-on work awarded. An overview of the EM&C architecture and prototype realization and a roadmap for future capabilities are provided.

In addition to the path diversity improvements provided by EM&C, protected waveforms enhance resiliency by enabling satellite communications terminals to continue to operate in contested (jamming) environments. The Direct Sequence Spread Spectrum (DSSS) class of protected waveform has advantages in performance and ease of integration into existing terminals. The proposed DSSS implementation is highly flexible to combat a wide range of interference levels and types. It nearly achieves the channel capacity, that is, the maximum amount of information throughput for a given level of interference, over a wide range of conditions. It is relatively simple to implement relative to other protected waveforms. Because of its simplicity and effectiveness, DSSS is being considered by several Defense Department programs as a protected waveform option.

DSSS technology supports the EM&C architecture and can be easily integrated into it to further enhance resiliency. DSSS technology and performance and specific options for combining this technology with EM&C and integrating the dual capability into current terminals are reviewed.

It is shown that the combination of EM&C and protected DSSS waveforms can cost effectively provide future warfighters with options for highly resilient SATCOM.

BIO: Mark Dale is a director of business development at Kratos-RT Logic, where he helps define next-generation satellite communications solutions in support of the U.S. government.

His recent activities have included support for the pilot phases 1 and 2 efforts sponsored by the Advanced Concepts Division of the Space and Missile Systems Center (SMC-MCX). Together with team members internal and external to Kratos, he has worked to define mechanisms to enable satellite terminals to flexibly access commercial and USG SATCOM capacity and roam between a diverse pool of satellites, teleports and managed systems.

Dale has been working in the satellite industry for more than 20 years, with responsibilities that have spanned systems engineering, product management and business development. Prior to working for Kratos-RT Logic, he worked at Comtech EF Data, Viasat and Broadcom. He holds a MSEE from the Georgia Institute of Technology and a PhD from the University of Southern California

Resilient Hybrid Adaptive Networking

Craig Miller, Vice President, Chief Technology Officer, Viasat •
craig.miller@viasat.com

ABSTRACT

Viasat’s Hybrid Adaptive Network (HAN) is an enterprise-level, flexible service delivery platform that provides unmatched resilience via a robust, scalable communications network that enables warfighters to seamlessly roam across multiple independent private sector and government communications networks spanning multiple satellite radio frequency bands, multiple orbital regimes and multiple independent ground networks.

The key components of Viasat’s HAN concept are multi-mode terminals, intelligent automated network selection, enterprise-level situational awareness and open-standards-based network layer interfaces to the component networks within the HAN. These building blocks allow the warfighter to seamlessly access multiple satellite networks in the same manner a commercial mobile device users can roam across varied cellular networks. Using multiple networks is a low cost, low risk approach that provides flexibility, freedom of movement and resilience that far surpasses what could be provided by any single network, no matter how exquisite. Operating on a HAN provides the warfighter assured communications in contested environments, creates deterrence and imposes significant additional costs on any adversary that would attempt to disrupt communications.

Most of the building blocks necessary to create Viasat’s vision of the Hybrid Adaptive Network already exist.

Flexible terminals that can operate over multiple networks are already in use today. For example, Viasat’s KuKarray multi-mode software defined airborne terminal can operate at both Ku- and Ka-band and is compatible with geostationary earth orbit (GEO), medium earth orbit (MEO) and low earth orbit (LEO) satellites. The KuKarray is capable of operating over Viasat’s networks, partner MEO and LEO networks, as well as government purpose-built networks, including WGS. Today, these terminals operate on Air Force One and numerous other government and commercial aircraft. Similarly, Viasat’s ground-based Multi-Mission Terminal (MMT) operates over multiple networks and frequency bands and is currently deployed with multiple Army Brigade Combat Teams (BCTs). Similar capabilities are available from other vendors, giving the government choice in the terminal solution that enables hybrid networking.

Viasat already provides enterprise-level situational awareness as a service for the Air Force One and the VIP/SAM fleet and has been selected by the Air Force to develop prototype multi-network situational awareness and common operational picture (SA/COP) capabilities for the government.

Viasat is also internally developing network management and selection tools that incorporate the multi-network situational awareness described above into an automated, artificial intelligence-based network selection capability. Furthermore, Viasat and other commercial partners are working together to develop and publish the Open Standard Interfaces that allow disparate networks to work together as a single network of networks: the Hybrid Adaptive Network.

Since the HAN is designed to easily add new networks via open standard management interfaces, it can leverage the exponential technology growth of the private sector to close capability gaps, deliver enhanced warfighter connectivity while simultaneously avoiding vendor lock by enabling ongoing, market-based competition for government communication services. Many of the key components of Hybrid Adaptive Networks already exist. This capability can be demonstrated now and, with modest investment, rapidly fielded into an operational capability.

BIO: Craig Miller is the chief technical officer for Viasat Government Systems. Miller is responsible for establishing and communicating the technical vision and roadmap for a diverse range of products and services, including its government satellite communications portfolio, tactical networks, encryption products, cyber/network security products, cybersecurity services, as well as its intelligence, surveillance and reconnaissance product portfolio.

Miller joined Viasat in 1995 and has more than 25 years experience in communications systems, including terrestrial wireless, satellite communications and terrestrial networking. Miller is an expert in multiple aspects of communications system security and design, including protocol/waveform design, terminal and space segment design, TCP/IP networking, network proxy design, cryptography, cryptosystems, network security, as well as offensive and defensive cyber techniques.

Miller holds a Bachelor of Science in electrical engineering with emphasis on communications and signal processing from the University of Arizona.

LOW PROBABILITY OF DETECTION/LOW PROBABILITY OF INTERCEPT

Information Theoretic Secure VPN

Daniel Kay, Senior Director, Cyber Reliant Corporation • dkay@trivalent.us.com

ABSTRACT

Cyber Reliant Corporation’s (CRC’s) approach to secure communications is focused on protecting data. It is currently approved to support NSA-certified secure data or voice communications up to top secret on Android devices.

CRC has adapted its proprietary data protection techniques to create an information theoretic secure virtual private network (VPN) capability to support highly specialized mission requirements. It believes this evolution in capability will enable the U.S. Army to customize a communication system with low probability of detection/low probability of intercept (LPD/LPI) capabilities to reduce platform and electromagnetic signature. CRC recognizes the importance of force protection of tactical Cyber Mission Forces (CMF) required in a peer/near-peer fight in a multidomain battle to ensure mission success. The company’s approach to an information theoretic secure virtual private network is a Technology Readiness Level (TRL)-4 proven capability readily adaptable to many conditions and operating environments including commercially available cloud architecture. CRC is prepared to rapidly move through technical maturity across U.S. Army program concepts, technology requirements and demonstrable technology capabilities.

CRC’s methodology leverages existing information technology infrastructure to provide data-centric protection to file, protocol (network, SATCOM), voice and video communications overcoming the main problem in secure communications: key management.

CRC’s data protection creates the opportunity to further obfuscate activities through proprietary deception techniques thereby reducing electromagnetic signature and concealing maneuver operations to provide operational advantage.

CRC welcomes the opportunity to conduct a classified information exchange and to arrange a demonstration of its Quantum-Resistant VPN technique over existing communications technologies.

BIO: D.C. “Danno” Kay, Cyber Reliant Corporation’s (CRC) senior director of federal programs, leverages decades of expertise in Department of Defense intelligence, surveillance, reconnaissance and cybersecurity to shape a presentation of Cyber Reliant’s capabilities to the federal sector.

Before joining CRC, he led execution of a large opportunity delivering capability to a major cybersecurity organization and grew the program across the U.S. departments of Defense and Justice. Kay holds a BA from American Military University.

Secure Comms in a Zero Trust Environment

Herm Hasken, Partner and Senior Strategy Officer,
MarkPoint Technologies LLC • hghasken3@gmail.com

ABSTRACT

U.S. intelligence experts have identified a number of nation-states and other actors conducting espionage and other tailored operations against key leaders and institutions across the U.S. government, defense contractors and allied nations. Foreign intelligence services continue to seek access to privileged U.S. government communications here and abroad.

At the tactical level, such exploitation has led to direct and fatal consequences. In multiple CONUS hostile areas and other deployment sites, U.S. forces continue to have their mobile devices (phones, tablets, laptops) probed, phished and hacked. The U.S. can also assume that rampant corruption in the government provides clear and unfettered access to cellphone company data, or the “back end” of the system. New vulnerabilities in legacy software and hardware continue to be discovered and exploited, making multiple mobile applications vulnerable to attack. This is a significant force protection and OPSEC consideration for commanders.

Over the past 24 months, it has become strikingly clear that foreign powers have been successful gathering data and leaking information gleaned from tactical mobile equipment for the purposes of gaining insight into tactical locations and maneuver operations. Despite organizational and operational security best efforts, U.S. government sensitive but unclassified communications networks continue to be probed, penetrated and exploited.

The Army requires communication systems with low probability of detection/low probability of intercept (LPD/LPI) capabilities to reduce platform and electromagnetic signature. Force protection of tactical Cyber Mission Forces (CMF) is required in a peer/near-peer fight in a multidomain battle to ensure mission success.

MarkPoint Technologies’ Cobra provides assured communication in all conditions and operating environments. Cobra does not rely on local cellular providers. Through proprietary wireless capability, Cobra significantly reduces and obfuscates a handset’s electromagnetic signature when conducting military operations. By staying off local cell structures, Cobra conceals the handset’s location when maneuvering to positions of advantage.

BIO: Herm Hasken has more than 30 years of combined military, federal and private industry experience in the special operations, intelligence and cyber communities of practice. He has served as the command representative to DIRNSA and U.S. Cyber Command for both Joint Special Operations Command (JSOC) and U.S. Special Operations Command. He served as special advisor to the director, DIA, and retired from the DIA while assigned to the U.S. Cyber Command J3. He provided staff support to the presidential transition team for national cybersecurity and policy and later went into private practice before joining MarkPoint Technologies as a partner and principal consultant for cyber operations. MarkPoint is the exclusive provider of Echo w/ Extras, a passive tactical cyber reconnaissance tool as well as a leader in cyber platforms.

Smartphones Could Compromise the Mission

Mike Fong, CEO and Founder, Privoro • mike.fong@privoro.com

ABSTRACT

The Army encounters high volumes of constantly evolving threats. Keeping Army communications safe from intercept and detection is more important than ever as cyber attacks evolve to exploit vulnerabilities in tools all soldiers and mission personnel carry: mobile devices. Mobile devices beacon more than just RF signals. They can expose the sensitive conversations and visual surroundings in their vicinity through compromised and unprotected microphones and cameras.

As cyberwar tools continue to grow in sophistication, so do the number of exploited vulnerabilities. Every layer of electronic devices have proven to be vulnerable, from the app and OS layers to the firmware and even the chips themselves. Any layer of breach allows an attacker to use microphones and cameras to gather information prior to encryption at rest or in motion. Unprotected microphones and cameras provide powerful vectors to intercept mission details and compromise operational security.

Learn the latest in how mobile devices are being compromised and how their vulnerabilities may impact mission success. Understand what is required to protect these systems and how to safeguard mobile device sensors from being used to capture or detect mission details.

Privoro, an emerging technology company based in Phoenix, Arizona, is the world leader in zero trust mobile hardware systems, microphone protection and passive RF attenuation. Privoro works with the Defense Department community to develop zero trust mobile solutions and has received contracts to enhance protection 24/7 for mobile users.

BIO: Mike Fong is the founder and CEO of Privoro, a startup company innovating a new class of hardware-based mobile security protections. Fong is an experienced technology entrepreneur, investor, board member and consultant. Before Privoro, he was the chairman and CEO of Calence, transforming it from a startup into the largest pure-play networking integrator in the U.S. at the time of its 2008 sale to Insight Enterprises. Privoro has attracted notable, high-profile tech investors such as John Chambers, former CEO and chairman, Cisco Systems; Jim Kavanaugh, CEO of World Wide Technology; and numerous others.

Fong is a proud recipient of the Arizona Technology Council's Ed Denison Business Leader of the Year Award. He received his BS in electrical engineering from Carnegie Mellon University.

A New Approach to LPD/LPI SATCOM

Lawrence Kingsley, SATCOM Systems Engineer, Viasat Inc. •

lawrence.kingsley@viasat.com

ABSTRACT

The warfighter demand for LPI/LPD/Anti-Jam (AJ) communications against increasingly sophisticated adversaries mimics the historical contest between armor and artillery. The traditional communications approach to counter the threat uses expensive, hard-to-use, nuclear-hardened communications systems or direct-sequence waveforms to protect low capacity datalinks by spending large amounts of bandwidth.

Viasat's approach is to arm warfighters with affordable, resilient, high-capacity, easy to use, rapid deploy SATCOM systems that have inherent LPI/LPD/AJ protection. This requires adversaries to bring their most exquisite and expensive systems to the field, to invest considerable resources and yet to fail against flexible, affordable systems. The company's approach is based on a whole-system perspective, and Viasat's High-Capacity Ka (HC-Ka) satellite communications solutions show that industry can provide high information rates while addressing the need for SATCOM systems to be LPD/LPI/AJ.

In addition to LPI/LPD/AJ attributes, warfighters also require LPA/LPG (attribution, geo-location) properties to provide essential communications with minimum emissions-based risk. A whole-system approach integrates all elements: orbit, frequency-band, satellite, waveform and terminal, optimizing end-to-end performance to achieve unprecedented capacity and resilience for millions of users. This approach stands in contrast to the traditional SATCOM design approach where operators piece together a system from a variety of components, including the modem and waveform, terminal and satellite. The traditional, lowest-common-denominator approach is suboptimal and the warfighter bears the brunt of the shortfall.

A SATCOM network that can support a million legitimate users can also tolerate high levels of interference (AJ), while the scale of the network improves LPD/LPA/LPG properties. SATCOM networks that support hundreds of gigabit per second of capacity are designed to work with small, low power, Ka-band user terminals that are more LPD than large, high-powered terminals. HC-Ka networks support more spreading and better automated network authentication than traditional Defense Department resilient waveforms with higher capacity and less detectability. With 250-500 MHz carriers and hundreds of gigabits of capacity, Viasat and other HC-Ka providers can support advanced LPD SATCOM waveforms. GEO and MEO HC-Ka systems force the adversary to use his most sensitive detectors at close range and bring his largest ECM assets to bear to jam the system, tipping the armor-artillery scale in U.S. favor.

Viasat has incorporated its HC-Ka technology in its currently fielded terminals, such as the AN/TSC-241 MMT. Small, light and battery-operated, MMT delivers 18/5 Mbps capacity (typical), which is much more than typically provisioned for traditional Ku-band trailer-mount terminals designed for operation in worst-case conditions on poor-performing satellites and constrained bandwidth. On Viasat and other HC-Ka satellites, there is no worst case; unprecedented performance is achieved anywhere within the HC-Ka footprint. Viasat's HC-Ka technology can be retrofitted to traditional military SATCOM terminals, increasing data rates while reducing electromagnetic footprint: when only 75 cm of 2.4m aperture is illuminated, the rest acts

as a shield to reduce sidelobes and detection. Demonstrations of the MMT on HC-Ka in northern Norway provided the same service capacity as demonstrations in Eastern Europe or in Germany.

BIO: Lawrence E. Kingsley is originally from New York State. He did his undergraduate work in physics at Clarkson College of Technology in Potsdam, New York. He then went on to the University of Rochester to pursue graduate studies in physics, earning first an MA and eventually a PhD in physics. His graduate research was partially funded by the Army Research Lab (then LABCOM).

Kingsley continued research at the University of Toronto as a post-doctoral fellow, living in Canada for a period before joining the Army Research Lab in 1991. After several years, Kingsley transferred to CECOM to work in satellite communications. He spent several years with the DSCS program office at Fort Monmouth, primarily investigating how various networking protocols (ATM, frame relay and IP) behaved over satellite links, monitoring research contracts, as well as working with terminal and modem certification.

Kingsley left CECOM and moved to Washington, D.C., to join COMSAT Laboratories in 1997, which was later acquired by Viasat. Kingsley was involved in the development and introduction of several of COMSAT Labs’ advanced satellite networking systems, such as the LinkWay mesh TDMA system and the LinkStar DVB-based VSAT system. For the past 20 years, Kingsley has been designing and implementing satellite networks using Viasat-based solutions for both commercial and government customers, being involved with customers from the proposal stage through implementation, training and sustaining support. He has been supporting the U.S. Army WIN-T Inc1 LinkWay-based network since its inception almost 10 years ago. He has also been working at Viasat to improve the state of the art of satellite networking. In particular, Kingsley has been involved with improving the LinkWay system, adding features such as COTM, ACSM, WGS Multi-SpotBeam support and enhanced resiliency.

MORE EFFICIENT ENCRYPTION MODULE

Enabling Efficient Communication Protection Across Multiple Types of Communication

Ken Tola, CEO, Bear Systems • ktola@bear.systems

ABSTRACT

Bear Systems provides a new type of cybersecurity that protects devices and device communications. Bear’s solution was originally designed for lightweight IoT devices to consume minimal power while providing maximum device and data communications security.

Bear’s Systems places full security on every device. The company’s solution enables lightweight device protection, data encryption and decryption, device authentication and authorization. The solution employs end-to-end AI for advanced remediation capabilities and device management.

Bear’s powerful next-generation device and data communications protection and control enables ubiquitous coverage across all IoT devices. Bear works across any type of existing network from Ethernet, WiFi and Bluetooth to RF, satellite, radio and OTA.

Bear was originally built to work over Bluetooth Low Energy (BLE) environments. A main aspect of this protection is a peer-to-peer multi-tiered approach wherein Bear continuously verifies the identity of each device, eliminating costly roundtrips to external sources for validation. Instead, Bear has a single packet solution for authorization and authentication that eliminates complex handshakes and message exchanges.

Bear works very low on a device, which makes Bear both more efficient and able to provide advanced protection. The lower down a device’s operations, the faster programs work, with decreasing amounts of overhead and power consumption for lower heat production and heat signatures. The optimal location for encryption is on microprocessors, and Bear can manage these chips. The next most efficient location for controlling processes, even those outside of an operating system, is in the BIOS. Bear works within this context and can move up a level into the very bottom of an operating system depending on the use case.

Bear encrypts Ethernet, the lowest level data packet found in devices and uses a group of security keys applied randomly. Bear can exceed the security of 256-bit encryption without ever having to generate such a large key. Bear has found that generating a number of small-size keys, from 50- to 100-bits in size, is much less costly in terms of resources and is much more secure. The power and flexibility of Bear’s solution also allows the military to implement preferred encryption algorithms independently.

Bear provides the advanced ability to protect communications without relying on any one type of communication. Combined, Bear secures new types of communications and transforms one type of packet into another. For example, a standard radio can employ encrypted communications to a satellite base station where the encrypted radio information is transformed into encrypted satellite streams. Those streams can in turn be converted to encrypted microwave transmissions to a remote WiFi network and decrypted at an authenticated, authorized location on the other side of the world.

These features are the true power of Bear—adaptive, low-level and highly efficient security operations, using less hardware and energy overhead.

BIO: Ken Tola started out in Washington, D.C. as a neuropsychologist prior to moving into IT in the late 1990s. Tola ran a division at Honeywell-TSI, modernized Cambridge Associates and then moved into government work under Tommy Thompson while helping to build out the HSS Command Center. He then went over to the Department of State where he re-architected the U.S. Visa and Passport Systems.

After leaving the State Department, Tola realized that cybersecurity was broken and, in 2008, he began a long journey to fixing this problem. During this journey, he accumulated numerous patents across the cybersecurity, privacy and AdTech markets.

Tola is an ardent supporter of veterans having experienced their sacrifice firsthand while a neuropsychologist at the Washington VA. As CEO of Bear Systems, he currently employs several veterans in prominent executive roles in his company.

Data-Protected Secure Communications

Daniel Kay, Senior Director, Cyber Reliant Corporation • dkay@trivalent.us.com

ABSTRACT

Cyber Reliant Corporation’s (CRC’s) approach to secure communications is focused on protecting data while recognizing the network is vulnerable to breach; it can support NSA-certified secure data or voice communications up to top secret.

The company’s Data-At-Rest (DAR) software is a full-featured mobile application currently supporting Android 6.0 and 7.0 on the DISA-mobility Samsung Galaxy S7 Custom Read-Only Memory (CROM) and Samsung Galaxy Tab S3 CROM devices and is integrated with NSA NIAP-approved and NSA-CSfC Components Listed method of DAR protection. The company’s DAR solution protects application file contents stored on a device and is designed to be custom integrated through minimal application coding to meet existing classified communications requirements.

CRC’s integrated application will provide an interface to support required application programming interfaces and processes. The company is committed to requirements of CSfC mobile access capability package (MACP) for providing the inner encrypted tunnel using transport layer security (TLS) 1.2 with National Security Systems (NSS) public key infrastructure (PKI) secret Internet protocol router network (SIPRnet) user certificates to connect and authenticate respectively to the Defense Department enterprise.

CRC has high confidence in its ability to enable mobility devices to store classified data in accordance with guidance provided by the NSA CSfC DAR Capability Package, as it relates to requirements and capabilities (e.g. storage locations and encrypted files) as applied to DAR applications on Android devices. It recognizes the security imperative in mobility device requirements including:

- Securely importing/exporting classified data via device storage media only to those file directories with DAR capability enabled.
- Supporting Android application secure usage and data processing at desired classification level contingent upon proper authentication.
- Only allowing DAR-enabled Android applications to securely import and export classified data via device storage media only to file directories with DAR capability enabled upon proper authentication.
- Integrating with an NSA NIAP approved and CSfC Components Listed method of DAR file encryption protecting contents stored on the device.
- Operating system file encryption components in accordance with and as identified by the NIAP validation report.
- Sending/Receiving files as attachments.
- Providing the ability to open and view attachments, including file types .doc, .docx, .xls, .xlsx, .ppt, .pptx, .jpg, .jpeg, .txt, .pdf, .avi, .mov, .mp4, .mp3, .wav, .bmp, .gif, .png and .webp.

- Creating new Microsoft and Open Office products and text files.
- Editing existing Office and text files.
- Deleting existing files off the device.
- Allowing storage of all files, including attachments, draft messages, configuration, databases, etc. to the device according to CSfC DAR Capability Package guidelines.

CRC’s secure solution will provide an automated classification marker:

- Providing a dropdown list of classification markers that will place selected classification markers in the body of communications.
- Providing a classification banner in a single line at top and bottom of the body of each message.
- Provide administrators the ability to update the classification dropdown list.

The secure solution will provide contacts management and allow users to:

- Create new contacts.
- Update previously-created contacts.
- Delete previously-created contacts.
- Search saved Contacts.
- View the Global Address List.

BIO: D.C. “Danno” Kay, Cyber Reliant Corporation’s (CRC) senior director of federal programs, leverages decades of expertise in Department of Defense intelligence, surveillance, reconnaissance and cybersecurity to shape a presentation of Cyber Reliant’s capabilities to the federal sector.

Before joining CRC, he led execution of a large opportunity delivering capability to a major cybersecurity organization and grew the program across the U.S. departments of Defense and Justice. Kay holds a BA from American Military University.

21st Century Cryptography

Dylan Hand, Senior Hardware Research Engineer, Galois Inc. • dhand@galois.com

ABSTRACT

Cryptographic modules deployed today in Defense Department and commercial systems have been primarily developed using outdated techniques and power inefficient implementations. The majority of cryptographic software comes from just a few software libraries written by applied cryptographers or programmers, generally not optimized for power efficiency.

To improve crypto performance, vendors use hardware acceleration of FPGAs and ASICs. However, most hardware cryptographic implementations are held back by legacy implementations, obsolete ASIC fabrication processes or integration in energy inefficient FPGAs. This is especially true for Defense Department certified, tactical crypto modules; they are expensive, heavy and power hungry. Many solutions have insufficient throughput for C2 communications, data feeds from unmanned systems and inter-soldier networks.

Recently, major corporations have spent millions of dollars on the development of technology that facilitates the creation of correct and secure cryptographic implementations. As new algorithm standardization in the U.S. focuses on lightweight block ciphers, new elliptic curves and post-quantum algorithms for Commercial National Security Algorithm suite, the cost to develop secure encryption continuously increases. Galois’ development approach at all levels—hardware, firmware and software—is tailored to produce correct-by-construction, low-energy, provably secure cryptographic cores. Two of its products, Cryptol and the Software Analysis Workbench (SAW), are the premier commercial technologies for cryptographic systems specification, verification and implementation synthesis. Development of both technologies has been funded for years by the NSA and other agencies for the Defense Department.

In addition to its secure, correct-by-construction synthesis tools, Galois has recently begun implementing encryption cores with Sharp, a state-of-the-art, asynchronous circuit technology. Recent improvements in semiconductor fabrication have not delivered the same gains in power efficiency seen a decade ago. Sharp unlocks the power efficiency potential of modern processes by enabling a wide range of operating voltages, reducing the power required to perform the same workload. Galois has utilized a version of this technology for an NSA-funded project to achieve fJ per encrypted bit energy consumption with the Simon and Speck block ciphers. The company is now applying Sharp technology for encryption cores, RISC-V CPUs and neural network accelerators in an USAF-funded program for low-power autonomous systems.

Chips with Sharp circuit technology consume less energy and generate less heat. The resulting impact to warfighters is multifold. A cooler chip no longer requires metal heatsinks or fans to dissipate heat, reducing weight and decreasing energy requirements even further. Eliminating cooling devices and reducing battery sizes enables lower SWaP systems that can operate in a wider range of mission environments.

The company’s active efforts for Defense Department’s cryptographic modernization is making dramatic improvements through lower cost, low energy, high performance correct-by-construction implementations. Called 21st Century Cryptography, its solutions use tooling developed for the NSA and Sharp circuit technology for world-class performant, energy efficient implementations to handle data up to top secret.

For dismounted soldiers, Galois proposes to extend its existing Defense Department crypto efforts for soldier-wearable applications suitable for tactical environments where energy efficiency, low thermal signature and performance are of key concern.

BIO: Dr. Dylan Hand, currently a hardware research engineer at Galois, was previously co-founder of Reduced Energy Microsystems (REM) and co-inventor of REM’s patented asynchronous circuit technology. Hand has spent more than a decade researching computer engineering and VLSI design as an undergraduate and graduate student at USC, receiving a BS, MS and PhD degrees in electrical engineering. He previously worked at Intel Labs’ Microprocessor Research Lab building CAD tools and optimization algorithms for asynchronous circuits. Hand has been at the forefront of research in asynchronous design, regularly publishing papers on increasing power-efficiency, performance and support for existing CAD tools.

SoCrypt: High Assurance Software Cryptography for SWaP-C Constrained Applications

Hal Aldridge, CEO, Secmation • hal@secmation.com

ABSTRACT

Modern military systems require secure communications between a rapidly expanding number of endpoints. These communications are essential between both warfighters and the Internet of Battlefield Things (IoBT) that supports them. Many of these communications are classified secret and below.

While traditional COMSEC solutions using purpose-built end cryptographic units (ECU) can fulfill the requirement for NSA-approved cryptography for many of these applications, a growing subset of applications do not have the size, weight, power and cost (SWaP-C) budgets necessary to support a dedicated ECU. For the warfighter, dedicated ECUs incorporated into one or more devices they carry can rapidly increase carried weight and total power consumption. It would be desirable to implement NSA-approved cryptography without a dedicated ECU.

This goal has proven challenging due to specific NSA requirements on how the cryptography must be implemented to protect classified information. To meet this challenge, Secmation is developing the SoCrypt solution for the Air Force Research Laboratory. SoCrypt incorporates an innovative combination of high assurance software design techniques with the hardware security features available in modern commercial off-the-shelf (COTS) processors. Leveraging security features in the ARMv8 processor architecture prevalent in many current and future COTS system on chips (SoC), SoCrypt’s verifiable, high-assurance software provides integrity and isolation of the cryptography adequate for SAB communications while enabling other real-time functions to share the same computing environment. With the correct selection of COTS components, this isolation enables SoCrypt to be a software embedment that adds SAB capability while not significantly affecting the SWaP-C of the device. The resulting highly efficient design utilizes the embedded computing capability that is already required to be in the device to perform voice communications or other functions. SoCrypt differentiates itself from other solutions by taking a ground-up approach, developing a robust, minimal set of software security features that directly tie to ARMv8/SoC provided security functionality. This deep integration combined with security architecture design provides both the assurance and fault tolerance needed for NSA-level cryptography. By providing an innovative solution for efficient, low SWaP-C, high-assurance cryptography, SoCrypt enables new security solutions for the warfighter, IoBT and critical infrastructure.

BIO: Dr. Hal Aldridge founded Secmation, a cybersecurity systems engineering and product development company specializing in applications including defense, Internet of Things and industrial control systems. At Secmation, Aldridge is leading R&D into wireless and embedded systems security solutions for customers, including the Air Force, Navy and Department of Energy.

Prior to founding Secmation, Aldridge served as CTO at Sypris Electronics, an information security company specializing in high assurance electronics and software used to protect sensitive communications and critical infrastructure. At Sypris, Aldridge led design and development for multiple NSA Type-1 certified products, including link encryptors and keyloaders.

Before entering the cybersecurity industry, Aldridge developed robotic systems for NASA and Northrop Grumman. He holds a PhD in electrical and computer engineering from Carnegie Mellon University specializing in fault-tolerant robotic control systems.

Data File-Centric Security

Richard Streeter, Senior Technology Consultant, Sertainty Inc. •

rich.streeter@sertainty.com

ABSTRACT

The most effective way to reduce encryption module power, heat and cost is by eliminating encryption modules.

Sertainty data protection technology encapsulates sensitive data inside self-protecting, self-authenticating and self-governing computer files. This is accomplished by combining encryption keys, authentication credentials and a configurable Sertainty Intelligence Module with the Army’s data, creating an impenetrable, reactive data-file—data:empowered. Protection is a zero-trust architecture, adjacent to, not in conjunction with, existing network security protocols. Multiple files or directories are embedded along with the Intel-ligence Module in a single data:empowered file making this technology perfect to protect not only bulk machine-to-machine data transfers but also individual files sent and saved. This process is equally effective in protecting data in flight and at rest.

Sertainty’s solution includes:

- **Intelligence Module:** An embedded, configurable executable-only accessible with an installed executable that works in conjunction with installed Sertainty libraries and logic. During file access attempts, the engine controls authorization, authentication and key management and auditing func-tions.
- **Self-Governing:** The data owner determines when, where, who, on what device(s) and what net-work location(s) the file is accessible. Those instructions are embedded in the file and enforced by the embedded Intelligence Module.
- **Self-Authenticating:** Each file contains identity information regarding each authorized process and/or device, enabling the Intelligence Module to confidently authenticate processes and devices.
- **Self-Protecting:** The Intelligence Module, among other functions, serves as an internal key man-agement system (KMS). The keys are both protected and transported within the file itself but also NEVER as clear text; this is NOT security by obscurity. Because the company embeds its own KMS, it produces multiple keys, allowing multiple independently protected internal structures.

The file components are broken into multiple separate secured parts, each part has independent gover-nance rules and encryption keys. Sertainty uses AES-256 encryption plus other obfuscating techniques. This ensures secured files are used by the right person, at the right time, in the right location and on the right device. Encryption is a means to a goal, not the ultimate outcome. The solution is the ultimate break-through, combining governance combined with the encryption.

The Sertainty technology is not a current standard; however, the benefits are many and profound.

The two most important benefits are:

- Once secured for storage, the files are prepared for transport. Sertainty data:empowered files that are sent over unsecured channels enjoy the same security level as while sitting at rest. When outside dedicated secure network enclaves, Sertainty data:empowered files are as secure as inside.
- Since the encryption keys are kept internal to the file, they are never exposed outside the data:em-powered ecosphere. Even if they were, the way the process works when internal file event logging is activated, each time the file is closed, it is re-encrypted with new keys.

The topic revolves around reducing the overhead burden of dedicated encryption devices. Sertainty tech-nology is software installed on computing devices, enabling a decentralized encryption environment. By not directly addressing the topic and its underlying assumptions, Sertainty does not *reduce* the current power, heat and weight thresholds, it **ELIMINATES** them.

BIO: Rich Streeter spent 28 years as a Navy cryptologic officer serving primarily as a reservist and was recalled to active duty three times after 9/11. While not in the Navy, he started as a programmer progressing to a CIO position for a medium-size defense contractor. The majority of his technical time revolves around creating database applications, administering databases or leading teams involved with databases or even multiple databases. While in the Navy, Streeter specialized in the convergence of cryptology and electronic warfare and cyber defense.

Efficient Encryption for the Tactical Edge

John Jaworski, Embedded Security Technical Lead, Viasat •

john.jaworski@viasat.com

ABSTRACT

Availability of military-grade cryptographic technology appropriate for protection of classified up to secret voice and data tactical communications is tremendously limiting the Army’s ability to leverage commercial wireless tactical communications, which is outpacing the military’s ability to develop and deploy wireless communications. Ubiquitous phones, tablets and other end user devices (EUD) and various sensors means there is not only an Internet of Things (IoT) in the home but also on today’s battlefield. Securing the data between all these devices, sensors, soldiers, commanders and intelligence analysts is critical to not only prevent data loss but also authenticate the data to prevent adversaries from injecting false data or commands. A solution that secures trusted information flow between all the elements but does not burden the soldier with a short battery life or a revealing heat signature is a force multiplier that not only increases squad and soldier effectiveness but also reduces collateral damage and friendly fire.

However, the development pace for an NSA-certified Type 1 encryptor that has CSWaP at the tactical edge similar to other mobile devices means the encryptor is not able to take advantage of these fast-moving commercial mobile electronics and is often a generation or two behind the EUD or sensor. A further complication is the technology of choice for most military encryption. ASICs or aging processors and FPGAs consumes many watts of power that limit the dismounted deployment time, increase the heat signature, require spare batteries to be carried and are not field updateable to support the latest efficient communications protocols. This dated technology also compounds the fielding delay because it forces a many years of long NSA certification processes just to update and years longer to develop and certify. These delays are orders of magnitude higher than the pace of change and often do not have the right interfaces or protocols to exploit the state of the art in wireless and network communications by the time they are fielded.

Recent advances in SWaP performance of microelectronics, driven by the explosive growth in commercial mobile electronics markets, have created the opportunity to change to this paradigm. However, to fully exploit this commercial innovation and avoid the already-obsolete-when-deployed issues, an encryption architecture is needed that is vendor and component agnostic, scalable to support multiple channels when needed, has minimal static power penalty or even zero standby power, but has fast enough startup to support push-to-talk audio or a data burst. Today’s power-efficient mobile electronic technology intersecting right architecture could deliver the Army a true plug-and-play encryptor that supports the full tactical edge mission of unmanned covert sensors, dismounted soldiers, video streaming data, and voice capabilities at the lowest power and heat.

BIO: Viasat is the leader in fully programmable security products for the Defense Department and other agencies that includes encryption of top secret/SCI data and voice levels with more than 50 NSA certifications during the past 15 years, supporting TS/SCI 100 + Gbps HAIPE to 20 Mbps, CHVP (Non-CCI) under 400 milliWatts.

CLASS III UAV ELECTRONIC ATTACK

Converged RF Solutions

Shane Clark, Scientist, BAE Systems • shane.m.clark@baesystems.com

ABSTRACT

Recent innovations in radar and EW technologies, adversary capabilities and techniques drive ECM systems toward converged and flexible systems, necessitating multifunction hardware capable of fielding a dynamic array of solutions—solutions that even evolve and react to changing mission and technique requirements through machine learning. The element-level digital phased array is uniquely suited for this role and is rapidly being matured to bring this capability to the warfighter.

BAE Systems is developing a next generation ECM system based on its software-defined digital array architecture. OASIS is an RF countermeasure-focused, multifunction RF system for protection of military rotorcraft and UAS. High technique flexibility, minimal SWaP, capability for arbitrary digital beamforming and simultaneous transmit and receive (STaR) enable the platform to fly in otherwise contested environments. A heterodyne RF front-end based on the MATRICs RF system-on-a-chip feeds element-level digitization, on-the-fly element/subarray allocation, enabling rapid resource redistribution and power savings. Scalable in frequency with common hardware, high-directivity beams provide high EIRP for jamming or high sensitivity while performing ISR or ES functions, all the while maintaining situational awareness through its simultaneous transmit and receive capability. Because the array is digitally addressable at each element, the company tunes a series of elements each to a different frequency band to provide a wideband staring capability for sensing, each covering a portion of the band with high sensitivity, while using an adjacent portion of the array for high EIRP jamming. Platforms using OASIS-like hardware for ECM receive the benefit of additional, reconfigurable capabilities as it supports multiple simultaneous military aviation functions beyond ECM including targeting support, DF/Geolocation, SIGINT/signals exploitation, GPS denial, cover jamming, communications jamming, MTI tracking radar and readily incorporates future sensing applications. The integrated, scalable and adaptive design of the system maximizes available SWaP for weapons systems while improving survivability and providing a host of electronic capabilities, serving as a force multiplier.

A sensor resource manager assigns and schedules the elements across the OASIS array in dynamically segmented subarrays according to RF tasking requests. Because the array is digitized at every element, it is possible to form any number of beams or functions by replicating received data and applying different amplitude and phase weights across the elements digitally within the constraints of the onboard FPGA or heterogeneous processing resources. The capability to form arbitrary numbers and shapes of subarrays dynamically as a mission evolves and, as RF task priorities change, enables an entirely new flexibility space not realizable using traditional phased array approaches.

Convergence of radio frequency functions into shared resources is a disruptive system design approach that drastically changes the way warfighter capabilities are developed, procured and utilized. Today's federated RF systems inefficiently utilize weight, power and cost resources, creating underutilized hardware that is effectively redundant at points during a mission. OASIS solves this problem with its RF converged aperture, reconfigurable transceiver and standardized interfaces using Vita 49.2, providing tactical functional performance for multiple functions from a single, scalable system, ready to adapt to the rapidly changing electromagnetic battlespace.

BIO: Shane Clark is a scientist at BAE Systems FAST Labs, working primarily on element-level digitized arrays and algorithm design. He holds a BS and MS in physics from the University of Washington and Mississippi State University, respectively.

SMALL FORM-FACTOR LONG RANGE SENSOR

Emergent Microelectronic Technologies Enable New Paradigms for Small Factor EW Payloads

Benjamin McMahon, Technology Development Manager, BAE Systems •

benjamin.mcmahon@baesystems.com

ABSTRACT

For future conflicts, the U.S. Army requires low SWaP-C solutions to successfully realize the CONOPs enabled by emerging microelectronics that bring unprecedented capabilities to low SWaP-C platforms. The extreme SWaP requirements to perform these functions from small platforms like a Group I-III UAS or projectiles require a new innovative approach, satisfying cost, weight, power, upgrade and sustainment factors while providing sufficient EIRP and sensitivity to achieve ranges more than 40 km for active and passive capabilities.

BAE Systems is nurturing an RF converged scalable payload called SCARAB that is capable of performing relevant RF tasks from SIGINT to COMMS, EW functions and radar inside a single, small low power system. When employed, this system will act as a primary payload for U.S. Army air-launched effects (ALE) platforms, eliminating the need for other systems to perform a single function, increasing effectiveness for all functions and reducing total SWaP-C of the mission equipment.

SCARAB is scalable with low NRE from less than 5 pounds to more than 30 pounds because of its leverage of COTs/GOTs ecosystem, providing enhanced performance for all functions as SWaP availability increases for larger ALE platforms. The system complements ALE platforms by providing a platform for a software-defined payload solution that can be upgraded with low NRE through its life cycle and scaled up or down to other platforms as needed.

The SCARAB payload consists of a standard 3U VPX ruggedized chassis and backplane with ABEAM transceivers. Each ABEAM card hosts eight half-duplex RF channels from 20 MHz to 40 GHz. ABEAM cards can be hosted with mission-specific embedded single board computers for functions requiring more processing capability than is resident on the Xilinx Ultrascale FPGA hosted on the ABEAM card, or other capability specific cards. The small size of the payload maximizes SWaP available for high power PAs, while the modular design permits easy reconfigurability for different functions by swapping aperture and amplifiers. Alternatively, high EIRP may be achieved by increasing the number of cards and channels and pairing the system with an antenna array, creating an active electronically scanned array.

ABEAM cards are based on the MATRICs chip, a field-reprogrammable array of RF subsystems tuneable from DC-40 GHz and contained on a single 8mm x 10mm SiGe-on-Insulator chip. The flexibility of the MATRICs chip allows the system to be adapted on-the-fly to meet even widely-disparate requirements of a range of missions.

The SCARAB payload combines unprecedented frequency agility with low NRE scalability across platforms and inclusion of open interfaces for third-party hardware, software and capability integration. The rapid in situ reconfigurability of this MATRICs-based approach provides an optimal transceiver for each mode of the ALE that is reconfigured throughout the mission for each function as required. Similarly, as new capabilities are integrated in software and firmware, the configuration of the transceiver is selected with no hardware changes.

BIO: Benjamin McMahon is a technology development manager at BAE Systems FAST Labs, where his team researches digital array EW and multifunction applications and enabling technology. Formerly an antenna engineer for EW systems, his efforts are now concentrated on digital RF system development, integration and fielding for U.S. Army rotary wing, UAV and active projectile applications. He holds a BSEE and MSEE from the University of New Hampshire.

CEMA Tactical Awareness Support Kit

Herm Hasken, Partner and Senior Strategy Officer,
MarkPoint Technologies LLC • hghasken3@gmail.com

ABSTRACT

To provide EW support and full spectrum cyber activities in support of multidomain operations at the operational and tactical levels, the U.S. Army will require advanced early warning capabilities, new tools to provide precision targeting and collection from increased stand off ranges and EW/cyber tools to defeat A2/AD efforts launched by adversaries. EW/cyber tools must be in place during the competition phase to provide enduring persistent access to adversary military communications and ISR infrastructure as well as insight to the neutral networks and infrastructure utilized by both adversary and U.S./Allied forces in foreign areas around the world. These EW/cyber tools must be small and ubiquitous, capable of being worn on a human body, mounted in a vehicle or placed on various sizes of drones or other platforms. These devices must be produced in several form factors to accommodate for local environment and mission profiles.

In response to such requirements, MarkPoint has created the CEMA Tactical Awareness Support Kit, or C-TASK. C-TASK's main engine is a software load that can passively record cellular, bluetooth and WiFi activity in its proximity. Proximity is a feature and function of the software load, antennas and low noise amplifiers being utilized. C-TASK also includes a software-defined radio (SDR) and hardware chassis, in specially configured variants, based on the mission at hand. As a ground sensor that is either body worn or vehicle mounted, the MarkPoint Echo Zero package, the main feature of C-TASK, is effective at longer ranges than current items in Army inventory. Once airborne on a tethered UAS, the stand off distance and effective detection range dramatically increases. This is achieved by utilizing a very small form factor (a Latte Panda), MarkPoint Echo Zero passive survey software load and some graphene antennae. With this very small package, MarkPoint has demonstrated the ability to conduct EW support at long ranges. The C-TASK was featured at the most recent Cyber Quest 2019 held at Fort Gordon, Georgia.

BIO: With more than 30 years experience in the SIGINT, cyber and special operations communities, Herm Hasken has been sought out by the U.S. Defense Department's most senior leaders to find and deliver advanced solutions for the Cyber Mission Force. Hasken serves as the principal operations consultant for MarkPoint Technologies, the nation's leading small business for passive cyber and EW support technologies.

Lighter Than Air, Small Form, Hyper Range

Jonathan J. Gollogly, Principal Consultant, Microsoft • jongo@microsoft.com

ABSTRACT

In future conflicts, communications will be jammed or denied by future aggressors or near-peer militaries. Satellite communications will be jammed or satellites shot down.

The drone will be created of exceptionally light foam for the body and the wings will be filled with helium. The drone itself will be air launched and fly remarkably high. AI will be embedded into the drone software. AI will be trained to utilize the jet stream to stay aloft. The drone will power its embedded hardware using exceptionally light solar cells attached to the outside of the drone. The communication equipment will be simple but encrypted cell phone transmitter technology or simple but light EW hardware. The U.S. military can launch these drones safely away from the war zone. Once in communication range, the military unit can utilize them for surveillance or as an EW platform or strike capability. These hyper range drones could loiter based on historical machine learning of weather patterns in a combat zone.

BIO: Jonathan J. Gollogly is the principal consultant and architect for Microsoft. He has 28 patent submissions, most in the ITAR, D-DIL or IC space.

Fleet Defense: Powered and Unpowered Submersible Drones

Jonathan J. Gollogly, Principal Consultant, Microsoft • jongo@microsoft.com

ABSTRACT

AI-trained drones will operate as schools in concentric rings around the fleet operating area and will require little or no power because they will be trained to use ocean currents; their motion through the currents will provide any power they need to operate. Much like a wind farm above sea level, this motion will recharge batteries, which in turn are used to store power for electronic warfare and electronics.

They will be able to conduct surveillance in hostile territory and a drone school will be able to detect ships, submarines and torpedos and react and defeat the enemy working in concert with fleet defense Aegis systems when activated. Drones will also exist as a pure electronic warfare/surveillance platform.

BIO: Jonathan J. Gollogly is the principal consultant and architect for Microsoft. He has 28 patent submissions, most in the ITAR, D-DIL or IC space.

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 more than 31,000 individual members, 139 chapters and 1,625 corporate members. For more information, visit www.afcea.org

