TechNet Augusta

2020 SOLUTIONS SHOWCASE

AFCEA TechNet Augusta Solutions Showcase

AFCEA International is pleased to host TechNet Augusta in an exciting and diverse format. The U.S. Army Cyber Center of Excellence and industry experts helped design a way to undertake this endeavor while addressing today's challenging circumstances.

TechNet Augusta's series of information sharing events began in May 2020 with the Army's request for industry solutions to some of its most difficult problems. These problem statements sought ways to use capabilities such as artificial intelligence and machine learning, data analytics and cross-domain technologies to address challenges with data management, cybersecurity and intelligence analysis.

AFCEA received more than 60 potential solutions that were reviewed by experts on the association's Technical Committee and are included in this compendium. The document is being presented and made available to the Army's leaders, program managers and technologists.

In concert with this call out to industry, AFCEA and *SIGNAL* Media introduced the TechNet Augusta Webinar Channel in October 2020. It features expertise in the areas of cyber, electromagnetic warfare and multidomain operations as well as descriptions of opportunities for industry to work with the Army.

And now, the association looks forward to the latest TechNet Augusta offerings, which include a series of virtual events that will take place from January through July 2021. These will focus on key Army actions necessary to successfully "Converge Information Capabilities in Support of Multi-Domain Operations."

More in-depth and extensive than webinars, this re-imagined TechNet Augusta will feature keynote speakers, Army Program Executive Officer/Program Manager sessions, continuing education, industry solution reviews, thought leadership presentations, direct industry engagements and virtual networking opportunities.

More information on the schedule and registration for the virtual series will be presented on the TechNet Augusta website.

The new format of this continuum of activities is keeping the lines of communication open among the Army, services, industry and government during what can only be characterized as a truly extraordinary time. While ensuring the health and safety of our military and civilian members, it is sustaining engagement to help solve unique as well as enduring problems.

AFCEA International deeply appreciates all the time, dedication and effort that has gone into supporting and producing TechNet Augusta. It is through this commitment that the military services and the companies that support them will succeed in providing global security.

Problem Statements

Army Use Case for the Internet of Things

Problem Statement 1: Future Joint All-Domain Operations (JADO) are becoming increasingly complex, multifaceted and unpredictable. As the technological capabilities of allies and adversaries advance, more pressure is put on commanders to anticipate, assess and take action in increasingly pressurized environments and constrained decision cycles.

Why is it important? The speed of decision-making will be paramount in the Army's ability to fight and win against peer adversaries in congested and contested environments. Its ability to leverage IoT technology and acclimate it into its integrated logistics systems (ILS), automated security screening systems and military platforms will play a major role in the success of future combat operations.

Army Migration of Data Analytics, Machine Learning and Artificial Intelligence Solutions in Army Enterprise Data Centers

Problem Statement 2: Today, the Army is unable to access, share and interpret the data across warfighting functions required to ensure commanders have the ability to exploit the power of current and emerging data analytics, cloud computing, artificial intelligence and machine learning capabilities.

Why is it important? The Army requires Integrated Enterprise Network/Integrated Tactical Network big data solutions that help achieve a global, standards-based environment with enduring goals of making data visible, accessible, understandable, trusted, interoperable and secure. The Army will continue to operate in increasingly complex, highly dynamic operating environments on the future multi-domain battlefield. The speed of decision-making will be critical to the service's ability to fight and win against peer adversaries in congested and contested environments. Information is an instrument of national power, and data is a strategic asset. Seamless access to Army data at echelon, when readily shared, increases readiness, enhances modernization efforts and ultimately impacts mission effectiveness across all warfighting functions.

Statistical Natural Language Processing to Support Mission Understanding

Problem Statement 3: Army systems must ingest unstructured, text-based data to extract the relevant information needed to enable automated processes such as mission mapping, dependency modeling or sentiment analysis.

Why is it important? The process by which the military issues orders is done via text-based communication. An Operations Order (OPORD), with applicable annexes, provides critical information such as task, units, timeline and PACE items for units to accomplish their assigned missions. The assimilation and understanding of this document take time and add a cognitive load to commanders and staff. However, natural language processing (NLP) applications could lower cognitive loads and hasten understanding by extracting key information from these written documents for further processing in other systems. For example, NLP could identify a defensive task and enumerate it for linkage with a dependency mapping algorithm that identifies mission-critical systems needed to support that task. Likewise, NLP could identify relationships, such as supported versus supporting, between tasked units so another algorithm could graphically depict such relationships. Furthermore, during mission execution, Mission Command Systems (MCS) frequently share information, such as significant activity (SIGACT) reports, via text. NLP could identify the nature of a SIGACT and develop courses of action with minimal human interaction to help address emerging information.

Mission Mapping and Dependency Modeling of Mission-Critical Systems

Problem Statement 4: The Army needs tools capable of determining how the failure or degradation of a mission system or systems impact their mission tasks and warfighting functions.

Why is it important? The Army relies on many systems to execute its warfighting functions. At any given time, the loss or compromise of one or more of these systems can impact the ability of commanders to execute their warfighting functions. For example, the loss of the Advanced Field Artillery Tactical Data System (AFATDS) or a compromise to the Blue Force Tracking network could compromise the ability of commanders to perform their fires warfighting function. Similarly, the loss of a radio frequency link could impact a commander's ability to execute command and control (C2). During operations, however, the loss of a mission-critical system and its impact may remain unknown until that system is required to execute the unit's mission objectives. To be more mobile, agile and lethal, commanders need tools that allow their staffs to identify mission tasks and associated warfighting functions, link them to mission-critical systems, identify other system dependencies and monitor these systems and dependencies for events in cyberspace and the electromagnetic operational environment (EMOE) that impact mission objectives. Doing so will help commanders and staff more quickly observe, orient, decide and act upon these events and mitigate or eliminate their impact to maintain advantage over adversaries during multi-domain operations.

Common Data Fabric with Cross-Domain Capability

Problem Statement 5: The Army requires a software-based system or architecture to serve as a common data fabric for parsing information into a common ontology, storing it and sharing it with mission systems across security enclaves.

Why is it important? The Army's convergence of mission systems into a common operating environment (COE) requires a common data fabric for sharing data between multiple systems. Too many military systems are "closed systems," receiving and hoarding data without providing an application programming interface (API) for other mission systems to access, query or acquire needed information from them. As a result, multiple mission systems must create their own links to multiple other systems and data sources using multiple APIs to acquire disparately formatted data in order to access needed information. In turn, these mission systems also store data and contribute yet another bloated silo of redundant data in an already constrained server infrastructure. These issues make it challenging to scale, innovate and create synergies between mission systems on tactical networks and across security enclaves. By integrating a common data fabric that also is capable of parsing multiple data formats into a common data ontology with a cross-domain solution, mission systems could access one data source for mission system data and no longer be forced to integrate directly with multiple other systems and data sources. Such an architecture would result in lower costs for compute, storage and networking, while improving synergies between mission systems.

Offensive Cyberspace Operations (OCO) Access Extension Capabilities

Problem Statement 6: What efforts are currently being made toward exploring tactics, techniques and procedures (TTPs) and vulnerability analysis (VA) against emergent technologies and protocols to navigate networks of connected devices? Describe what ongoing VA work you are currently focused on and what platforms you're conducting VA against with special emphasis on inter-platform pivoting. The Army is defining "emergent technologies and protocols" as any platforms and protocols that have yet to fully saturate their chosen markets worldwide. Specific details about particular platforms and protocols of interest can be provided in other venues. The Army requires VA against emergent platforms and protocols to navigate networks of connected devices.

Why is it important? In general, Offensive Cyberspace Operations are limited to what platforms and protocols are in use and vulnerable to exploitation. It will continue to be important for research and development efforts to pace technological advancement.

Security Orchestration, Automation and Response (SOAR)

Problem Statement 7: The Army requires a Security Orchestration, Automation and Response (SOAR) that enables it to respond quicker to Defensive Cyber Operations (DCO) events.

Why is it important? SOAR integrates disparate tools and technologies into a cohesive system capable of quick response. SOAR enables technicians with different levels of training to safely and quickly respond to events on the network. In addition, SOAR allows products never designed to integrate to be an integrated solution.

Countering Polymorphic Malware

Problem Statement 8: How does the Army counter polymorphic malware?

Why is it important? Adversaries are increasingly avoiding anti-virus detection tools by rapidly morphing their signatures. Small changes by adversaries create an asymmetric advantage by significantly increasing the work factor to defeat existing malware. The Army needs new techniques that would enable defenders to recognize polymorphic malware in real time at the perimeter. What are some innovative new ideas to enhance immediate malware recognition? How could they be implemented to defend U.S. networks and reduce the impact of their polymorphic nature? What applications are available to counter fuzzing and signature diversity in an automated fashion where traditional hashes or heuristics fail to detect malware?

Machine Learning

Problem Statement 9: The Army needs a machine learning system for identifying anomalous behavior in encrypted data streams.

Why is it important? With a significant portion of Internet traffic being encrypted, identifying anomalous activity in encrypted data streams proves challenging. SSL decryption can be slow and requires special setup and personnel authorized to inspect traffic. How does the Army use machine learning to profile encrypted tunnels for identification of malicious activity?

Resilient Network Transport Capabilities

Problem Statement 10: The Army requires access to reliable information in contested and congested environments. The Army requests a solution for improved network transport resiliency using intelligent software-defined radios to enable secure, multi-path diversity, while minimizing electromagnetic spectrum (EMS) detection.

Why is it important? In multi-domain operations (MDO), the Army requires resilient communications against peer or near-peer adversaries. Units must be able to maintain continuity of operations for each radio in the network. Units require software-defined radios that allow intelligent networking between multiple transport systems; automatically facilitate primary alternate contingency emergency (PACE) concept while utilizing antenna solutions that enhance low probability of interception (LPI)/low probability of detection (LPD).

High-Capacity Beyond Line of Sight Communications Including Low Earth Orbit/Medium Earth Orbit/Geostationary Earth Orbit

Problem Statement 11: To achieve multi-domain operations (MDO)-enabled capabilities, the Army desires high-capacity, low-latency and long-distance communications for expeditionary forces. The solution should provide approximately 1Gbps bandwidth and 50ms latency. The Army is primarily focused on a Low Earth Orbit (LEO)/Medium Earth Orbit (MEO) capability but would be interested in a Geostationary Earth Orbit (GEO) or beyond line of sight (BLOS) capability that meets the 1Gbps bandwidth/50ms latency requirement with a minimum range of 800Km.

Why is it important? This capability will provide expeditionary, mobile, beyond line of sight communications with increased bandwidth and low latency to provide the warfighter with enhanced transport for mission command systems, including sensor data.

Command, Control, Communications, Computers, Intelligence, Surveillance and Reconnaissance/Electronic Warfare Modular Open Suite of Standards Compliant Capability

Problem Statement 12: The Army is required to execute mission command (MC) and warfighter functions during multi-domain operations (MDO). As a result, Army vehicles and other platforms are laden with radios, video displays, sensors, electronic warfare tools, antennas and other vital communication technologies, each with its own power draw and platform footprint. At the core, these command, control, communications, computers, intelligence, surveillance and reconnaissance/electronic warfare (C4ISR/EW) systems use many of the same building blocks, but they are not shared or distributed between systems, for example amplifiers, filters and processors. The C4ISR/EW Modular Open Suite of Standards (CMOSS) was developed to facilitate consolidation of these disparate systems into a common ruggedized chassis, described as the CMOSS Mounted Form Factor (CMFF). The Army requires a materiel solution for the CMFF to facilitate convergence of warfighting capabilities. Solutions should be packaged as a CMOSS-compliant chassis system with physical specifications (standards) for capability cards. For capability cards, the service would like at a minimum to have a standard proposed for a communications card if the company is unable to capture the other capability functions. CMFF solutions should be available for various environments, for example chassis-concept integration solutions for use on a Stryker, Abrams or Bradley to provide commanders with the ability to use current warfighting capabilities. The solution should be adaptable for use in the Command Post environment.

Why is it important? CMOSS would improve the ease of operation, maintenance sustainment of current warfighting capabilities. The CMFF minimizes the need for platform-specific integration and allows the fielding of subsequent capabilities (i.e. circuit cards/modules) without the need of any additional cabling or mounts.

Real-Time Spectrum Awareness Visualization

Problem Statement 13: The Army requires a sensor or several small sensors that provide real-time electromagnetic operational environment (EMOE) input, is compatible with and displayable on the Electronic Warfare Planning and Management Tool (EWPMT), and is capable of monitoring friendly emissions and enabling emission control that supports operational planning and deconfliction.

Why is it important? The electromagnetic spectrum (EMS) is increasingly congested and changing at a pace with which databased information cannot keep up. The Army requires real-time means to sense the local environment that ensures spectrum dependent devices operate as intended, provide commanders EMS situational awareness of their own systems and help inform tactical decisions based on current EMS/EMOE.

Electromagnetic Spectrum (EMS) Deception and Masking

Problem Statement 14: The Army requires a capability to mask or hide its electromagnetic (EM) emissions at echelon to include assets. This includes, for example, combat vehicles, command posts and radars.

Why is it important? Army forces utilize a multitude of EM-enabled devices making their positions identifiable and targetable by adversary forces. Many of these EM-enabled devices are unique and/or high-powered, making them targetable at long ranges.

Small Form-Factor, Long-Range Sensor and/or Antenna

Problem Statement 15: The Army requires long-range electronic warfare (EW) sensors and/or antenna built in a small deployable form-factor that can achieve ranges greater than 40 kilometers.

Why is it important? All echelons need to be able to detect, identify and geolocate electromagnetic spectrum (EMS) signatures at significant distances to provide friendly and adversary situational awareness to enable lethal and non-lethal targeting capabilities in large areas of operations.

Cyber Domain Modeling and Simulation (M&S) Capabilities and Their Integration with Other Domain M&S

Problem Statement 16: The Army's current constructive maneuver models, both the entity resolution federation One Semi-Automated Forces (OneSAF), as well as the multi-resolution federation Joint Land Component Constructive Training Capability-Warfighter's Simulation (JLCCTC-WARSIM), do not adjudicate friendly or enemy actions within the cyber domain. Both the electromagnetic spectrum as well as cyberspace, including computers, routers, switches and associated networks, are not replicated in either model; therefore, friendly and enemy activities in the cyber domain have no bearing or impact on the success or failure of kinetic actions and battles. The Army requires an integrated force-on-force cyber domain modeling environment that replicates cyberspace, electronic warfare and networking across all strategic, operational and tactical echelons (theater to team), while incorporating all aspects of environmental impacts on the electromagnetic environment. This capability must also federate with the M&S capabilities for the other operational domains without the need for a high-performance computing environment.

Why is it important? The Army lacks a monolithic cyber domain M&S capability able to adjudicate both friendly and competitor actions within both cyberspace and the electromagnetic spectrum concurrently. This lack of capability in the cyber domain likewise translates into a lack of cyber M&S adjudication within M&S capabilities for other domains, including air, land, sea and space. Defense doctrine, including multi-domain operations, considers cyber as a distinct domain coequal with other operational domains. However, while Army training, experimentation, and testing and evaluation enterprises have verified, validated and accredited models for the other operational domains across the live, virtual and constructive simulation environments, no such capability exists for the cyber domain.

Table of Contents

Highlighted abstracts selected and presenting their solutions during TechNet Augusta as of December 18, 2020.

ARMY USE CASE FOR THE INTERNET OF THINGS

ARMY MIGRATION OF DATA ANALYTICS, MACHINE LEARNING AND ARTIFICIAL INTELLIGENCE SOLUTIONS IN ARMY ENTERPRISE DATA CENTERS

STATISTICAL NATURAL LANGUAGE PROCESSING TO SUPPORT MISSION UNDERSTANDING

MISSION MAPPING AND DEPENDENCY MODELING OF MISSION-CRITICAL SYSTEMS

COMMON DATA FABRIC WITH CROSS-DOMAIN CAPABILITY

OFFENSIVE CYBERSPACE OPERATIONS (OCO) ACCESS EXTENSION CAPABILITIES

SECURITY ORCHESTRATION, AUTOMATION AND RESPONSE (SOAR)

COUNTERING POLYMORPHIC MALWARE

MACHINE LEARNING

RESILIENT NETWORK TRANSPORT CAPABILITIES

HIGH CAPACITY BEYOND LINE OF SIGHT (BLOS) COMMUNICATIONS

COMMAND, CONTROL, COMMUNICATIONS, COMPUTERS, INTELLIGENCE, SURVEILLANCE AND RECONNAISSANCE/ ELECTRONIC WARFARE MODULAR OPEN SUITE OF STANDARDS (CMOSS) COMPLIANT CAPABILITY

REAL-TIME SPECTRUM AWARENESS VISUALIZATION

ELECTROMAGNETIC SPECTRUM (EMS) DECEPTION AND MASKING

SMALL FORM-FACTOR LONG-RANGE SENSOR AND/OR ANTENNA

CYBER DOMAIN MODELING AND SIMULATION (M&S) CAPABILITIES AND THEIR INTEGRATION WITH OTHER DOMAIN M&S

ARMY USE CASE FOR THE INTERNET OF THINGS

Adapting When Unpredictability Is the Standard

Jonathan Janos, Senior Solutions Architect, MongoDB • jonathan.janos@mongodb.com

ABSTRACT

As world events and mission operations accelerate toward the increasingly complex and unpredictable, there is a growing need for more capable decision-support systems to discern optimal courses of action within shorter timeframes based on more substantial amounts of data. Unfortunately, it's challenging—even impossible—to know in advance what will be the decisive insight. The real world is full of detail and nuance that can wreak havoc on any prefabricated system that has been tailored—no matter how elegantly—in an unrealistically controlled lab environment. If unpredictability is the standard, how can systems be architected to deliver more value in the most demanding situations?

First, it is important to acknowledge the critical constraint: Anything brittle is likely to break. Static reports, built from static data sets, integrated from predefined sources, will likely deliver value until they don't. Suddenly, the rigidity of these systems becomes a battlefield liability. Tailoring content has to be fast. As the situation on the ground changes, information systems have to adjust as close to real-time as possible. These adjustments include new information, aggregated in new ways, from the full range of available sources.

Relational database technology, now 50 years old since its inception, does not support this required agility. It asserts that the world can be predefined in very restrictive ways, with uniform sets of features and attributes. Anything anomalous, although frequently significant, has to be dropped as it doesn't fit into the data model. Or, the entire data model has to be refactored to accommodate it, a time-consuming process that introduces unacceptable levels of risk to ongoing operations.

Incorporating new data sources is subject to the same constraints. Standardizing across disparate data sources is prohibitively time-consuming, preventing new sources from being integrated within useful time windows. The result is a patchwork of disconnected information silos that cannot support self-service data requests or integrated analysis.

MongoDB introduces a new way to model data, facilitating the rapid ingest of new data sources, accommodating real-world variability and promoting the rapid development and rollout of new system features. Rather than forcibly separating related data across divided tables with predefined columns and relationships, MongoDB takes the straighter forward approach of storing data within JavaScript Object Notation (JSON) documents. JSON allows for hierarchical data and nested relationships and supports nonuniform data sets; individual documents may contain whatever required attributes. This flexibility promotes fast integration of new data sources and immediate access without requiring normalization.

Once ingested, data can quickly be analyzed and aggregated in new ways and developers can quickly roll out new features and capabilities. Analytical requirements can be done on rapidly changing, multistructured

data in real-time. User-facing enhancements do not require back-end schema changes. This dramatically accelerates the development process, resulting in faster iteration and deployment of new features with no risk to current operations. MongoDB customers frequently report improved innovation and three to five times developer productivity gains.

BIO: Jonathan Janos is a senior solutions architect at MongoDB helping executives and technologists better understand today's landscape of data platforms and their potential to fundamentally alter how organizations operate. He has been working in the information technology sector for more than 20 years, including at premier companies in the analytics and big data spaces.

Reducing the Warfighters Cognitive Burden

Matthew Maher, Chief Data Scientist, Processus Group •
maherm@processusgroup.org

ABSTRACT

The U.S. Defense Department is faced with high degrees of difficulty regarding the state of their data and the ability to turn this data into meaningful information on a timely basis. As technological capabilities advance around data acquisition, more data comes faster and more efficiently than ever before. As a result, the size and scope of the big data dilemma the whole world faces become especially problematic in the defense arena.

This is true at nearly every step in the data management process, including collecting, accessing, cleaning, transmitting, analyzing, securing and storing joint operational data. In addition, an even more critical task involves the effective leveraging of the information contained with the data to augment decision making. Consequently, multidomain operations are facing several significant data challenges, including but not limited to integrating disparate data sources, validating data and building responsive, actionable command and control support.

This dilemma is a roadblock for the Defense Department and military acquisitions to shifting the paradigm from antiquated software capabilities to artificial intelligence (AI) and machine learning (ML) capabilities and they need to ensure key infrastructure, including big data and knowledge artifacts, also mature enough to handle the transition.

Before any organizations or domains develop or adopt a strategy based on AI, ML or any other form of intelligent system, they need to do a self-assessment that answers three key questions: How well does the organization/domain share knowledge? What is the state of its data? Does it understand the cognitive requirements? Answering and understanding these questions is the key to knowing where the organization is now (point A) so it can take actionable and progressive steps toward where it wants to go (point B) to make the organization or domain AI-capable.

This paper will describe these challenges in more detail and offer solutions based on emerging technologies being brought into play by the Processus Group and its consortium of partners who have developed a number of unprecedented capabilities.

BIO: A former Army officer assigned between special operations and conventional forces and currently a data scientist, Matthew Maher is supporting AFCEA's technical pillar as the subject matter expert in data analytics. He has published several papers on the area of reducing the warfighters' cognitive burden, leveraging ontologies/knowledge graphs to combine qualitative and quantitative data for decision making and the creation of cognitive architectures, sematic data models and operational knowledge graphs for AI/ML training.

Data-Driven Decision Making of an Intelligent Defense Force

Matthias Ledwon, Industry Executive Advisor, SAP America •
matthias.ledwon@sap.com

ABSTRACT

The Intelligent Defense Force is SAP's vision for an integrated logistics system (ILS) that enables data-driven decision making at the tactical edge as well as in higher headquarters. In case of the U.S. Army, it would combine the Global Combat Support System–Army (GCSS-Army) weapon systems data through the Internet of Things (IoT) and artificial intelligence such as predictive analytics. An overview of the Intelligent Defense Force and its impact on the Army's tactical operations is this solution's goal.

GCSS-Army and the Logistics Modernization Program (LMP) are the backbone of the Army's supply chain. GCSS-Army also is the system of record for weapon system readiness. Both are based on a commercial off-the-shelf (COTS) enterprise resource planning (ERP) solution by SAP, like the business systems of more than 40 military organizations around the globe. Combining this expertise with IoT use cases of other large commercial SAP customers, uniquely positions SAP to develop the vision and realize it in an integrated intelligent solution that can also integrate with the same solution other allied forces use.

Sensor data onboard weapon systems as well as along the supply chain can provide equipment health data and supply status in accordance with the concept of operations. GCSS-Army as the tactical maintenance and unit supply system will automatically receive the data at the tactical edge as well as the central system. Leveraging a replatformed ERP called S/4HANA Defense and Security with in-memory technology and embedded artificial intelligence will provide predictive analytics to alert the maintainers and local commanders; provide status updates and predicted shortages or equipment failures; and ultimately enable better, data-driven decision making in real time or near real time. Leveraging state-of-the-art technology for disconnected operations, the solution also will support operations in communication challenged environments.

BIO: Matthias Ledwon is the industry executive advisor for the U.S. Defense Department at SAP America, serving as an intermediary between SAP's defense customers in the United States, SAP's partners and SAP. He is a thought leader and occasional blogger. Over the past 20 years, he has supported business transformations with SAP solutions in the defense and other industries. Ledwon is a former infantry officer, graduate of the University of the Federal Armed Forces in Hamburg (Germany) and lives with his family in Northern Virginia.

Novel Tactical-Edge Computing Architectures to Accelerate Mission-Critical Decision Making

Duncan Stewart, Director, Strategic Development, Axellio •
duncan.stewart@axellio.com

ABSTRACT

Tactical-edge demands, especially of all-domain operations, are becoming increasingly complex and multifaceted. The aircraft, satellites, ships and ground vehicles the forces operate today collect an abundance of information. Processing and analyzing that amount of data is a challenge, especially when an increasing number of sensors create large volumes of data that cannot be processed in a timely manner solely in the cloud or in data centers thousands of miles away from the front line through connections that are often insufficient to handle the demands, for example security compromised, lack of bandwidth or disrupted by enemies. Expeditionary military missions require enterprise data center capabilities at the edge in smaller size, weight and power (SWaP) form factors to meet the needs of today's operating conditions.

Today's choices for tactical-edge computing are characterized by two stark realities:

- Small, portable computing platforms in rugged cases are unable to keep up with the growing data processing and storage demands; and
- Large, high-performance data center computing platforms are too difficult and expensive to transport and operate in the field.

Fundamentally new design principles are necessary that make possible the development of data center quality systems with incredible power in small packages. These principles enable several integrated innovations, including:

- Highly expanded internal fabric interconnect architectures and more intelligent firmware to significantly increase the capacity and performance of commercial off-the-shelf components such as processing cores, memory, flash storage, GPUs and FPGAs;
- Greater modularity to allow for simple customization, scaling, operation and support; and
- Advanced thermal and power management to support dense packaging of more components in smaller configurations.

To maintain superiority over near-peer adversaries, the U.S. and its allies must dominate the information warfare battlespace and shorten the sensor-to-shooter cycle. As operations push forward in expeditionary missions, highly portable yet very powerful computing platforms enable the processing of a high volume,

velocity and variety of data at the point of ingest. With new architectures developed by Axellio, the warfighters are able to make better and faster decisions that cannot be matched by enemies. These systems have been rapidly adopted by the U.S. military to solve some of the most demanding challenges in sensor fusion, intelligence and cybersecurity.

BIO: Lt. Col. Duncan Stewart, USAF (Ret.), is the director of strategic development at Axellio Inc. He is responsible for exploring military and intelligence applications of the company's commercial innovations in edge computing. Col. Stewart served for 24 years in the active duty and reserve Air Force. During his career, he served as an acquisition program manager for advanced avionics, sortie generation officer for fighter and tactical aircraft and senior logistics officer at the COCOM level. He created the Strategic Innovation course at the U.S. Air Force Academy and supported several major science and technology initiatives. He is the former CEO of the Colorado Springs Technology Incubator and CEO of Quadric Biomedical. He currently serves as the chairman of the board of ConcealFab, the technological leader in telecommunication mounting infrastructure. Col. Stewart earned a Bachelor of Science in management from the U.S. Air Force Academy, a Master of Science in aerospace management from Embry-Riddle and an MBA from Notre Dame University. He is a patented inventor of several electromechanical and biomedical devices and maintains a TS clearance.

Joint All-Domain Operations Common Operating Picture (JADOCOP)

Steve Wagner, Enlighten IT Consulting LLC • swagner@eitccorp.com

ABSTRACT

Enlighten proposes utilizing the Big Data Platform (BDP) as the "data operating system" to aggregate, analyze and visualize data from IoT devices and correlate it with cyber, intel, surveillance and reconnaissance data to create a network common operating picture (NETCOP) that increases the speed of sensor-to-shooter (S2S) decision making. The BDP is an accredited government off-the-shelf capability that is currently operating in production on the NIPRNet, SIPRNet and Joint Worldwide Intelligence Communication System and storing and analyzing more than 30 petabytes of all-domain data across the U.S. Defense Department.

The BDP has been adopted by the joint community as the centerpiece of the Unified Platform and allows for the aggregation, correlation and analysis of data across the services providing the ability to create a truly Joint NETCOP, leveraging data from Army, Air Force, Marines, CYBERCOM, Navy, Coast Guard, DISA and others. The proposed NETCOP dashboard will ride on the BDP and connect to the Unified Platform to incorporate data from all domains and services. The capability will leverage the integrated, accredited bi-directional cross domain service at CYBERCOM to provide a real-time S2S kill-chain decision making capability.

Internet of Things (IoT) integration with supply chain logistics has created a network of sensors that should be leveraged to speed up S2S decision making by providing real-time insight into location, availability and readiness of weapons and ammunition. GPS devices track assets in transit that can inform route planning, identify when assets are delayed and assist with contingency planning for alternate routes. IoT devices also can monitor environmental factors that could impact the readiness of assets upon arrival, such as temperature and humidity. IoT devices are generating this useful information, but it is not currently being aggregated with other all-domain data sets to inform decision making in the S2S kill chain. The BDP is positioned to be this aggregation point. The data-agnostic capability is already collecting petabytes of all domain data; integrating IoT information would be an important step forward in operationalizing this data to increase the speed of decision making.

Joint All-Domain Operations require large-scale data aggregation and integration across hundreds of data sources and data types to provide a high-confidence NETCOP that increases speed in making end-to-end S2S decisions. IoT devices are rapidly advancing situational awareness of all domain operations by adding sensors and the potential for data integration for every step in the S2S kill chain.

Supply chain situational awareness is a key component of S2S, as commanders need to understand the status and location of forces, weapons and ammunition to make an informed shoot decision to shoot. S2S decisions are only effective if warfighters can rapidly react to sensor information, so maximum integration of

data into one NETCOP is key to enabling S2S Joint All-Domain Operations. The NETCOP should integrate IoT sensor data with Key Terrain Cyber (KT-C), targeting, intelligence, surveillance and reconnaissance data from across the joint community in the BDP to increase the speed of decision making.

BIO: Over the past four years, Enlighten IT Consulting LLC, a nontraditional defense contractor, has been providing the U.S. Defense Department with advanced situational awareness leveraging an all-domain ready data platform with cross-domain capabilities in support of U.S Army Program Executive Office for Enterprise Information Systems, Army Cyber Command, Air Force Cyber, Marine Corps Cyber and U.S. Cyber Command networks.

Integration of IoT Data Into JADO

Jason Crabtree, CEO, QOMPLX Inc. • jason@qomplx.com

ABSTRACT

The Army's use case for Internet of Things (IoT) interoperability can be addressed by using an intermediary system with a dedicated reconfigurable instance that operates between each pair of the existing systems that share actionable information. Each instance operates one way, serving as an orchestrator of reporting, visualization, messaging or a domain-specific action from a source to a target system. It also serves to transform data from source format to target format, ensuring that authentication requirements are met. Eliminating transforming data manually and the need to re-authenticate manually alone can be a timesaver.

The company illustrates how its data fabric, Q:OS, can be configured to accomplish the objectives of integrating IoT data into Joint All-Domain Operations (JADO). Q:OS includes configurable components that can be templates for rules-based orchestration, streaming data message queuing and load balancing and data transformation for this purpose. Several such configurations can be operational in parallel, serving as one of the many one-way instances mentioned above and can relay, suitably transformed, streaming or batch data or action-request between two systems.

BIO: Jason Crabtree is a cofounder and serves as the chief executive officer and board member at QOMPLX. He is an expert on cybersecurity, operational risk management, decision support/automation technology and simulation/predictive modeling of complex-adaptive systems. As a Rhodes scholar, Crabtree researched artificial intelligence-based optimization of engineering design processes at Oxford University. First Captain of his class at West Point, he is a licensed professional engineer who served as a Ranger/Sapper-qualified infantry leader in Afghanistan before completing military service as a special assistant to senior U.S. Defense Department cyber leadership with emphasis on the development and operational integration of advanced technology initiatives including work with DARPA. Crabtree also was a 2014 Cyber Policy Fellow with the Madison Policy Forum in New York City and a 2016 Cyber Fellow for the New America Foundation. He has been an invited participant, panelist and speaker on energy, risk management, finance and security for organizations, including the Casualty Actuarial Society, Financial Services Roundtable, the Center for New American Security, the Markle Foundation, the Ditchley Foundation, the Gridwise Architecture Council and RAND in both the United States and United Kingdom.

ARMY MIGRATION OF DATA ANALYTICS, MACHINE LEARNING AND ARTIFICIAL INTELLIGENCE SOLUTIONS IN ARMY ENTERPRISE DATA CENTERS

Big Data Platform

Steve Wagner, Vice President, Enlighten IT Consulting LLC •
swagner@eitccorp.com

ABSTRACT

At the foundation of all successful migrations of data analytics, machine learning and artificial intelligence lies a mature infrastructure that enables computing, data storage and analytics for effective modeling. Enlighten led the development of the government off-the-shelf Big Data Platform (BDP), a robust and scalable architecture capable of ingesting, storing and visualizing multiple petabytes of data. Its distributed data structures and streaming ingest capabilities provide storage and retrieval rates in the millions of records per second. Enlighten also developed and deployed a suite of situational awareness analytics to the BDP, giving analysts tools for accelerated threat detection, diagnosis and mitigation.

Initially developed in 2012, the DISA government off-the-shelf BDP, a Risk Management Framework (RMF) accredited with authority to operate (ATO), delivered streaming and batch data processing, storage, visualization and analysis system at Technology Readiness Level (TRL) 9.

Enlighten's BDP approach will enable users, managers and stakeholders to access, share and interpret the data across warfighting functions required to ensure commanders have the ability to exploit the power of current and emerging data analytics, cloud computing, artificial intelligence and machine learning capabilities. Furthermore, Enlighten is meeting the challenges of the volume and complexity of big data by applying artificial intelligence and machine learning capabilities. These solutions include the Cyber Learning Engine (CLE); RAPID, a comprehensive analytic solution; and the Rapid Analytic Deployment Management Framework (RADMF).

This BDP solution provides an accredited and secure environment in which new analytical tools that support predictive analysis can be quickly built to support U.S. Defense Department efforts and easily shared across a common platform between analysts both within the Army, USCC, DISA and other agencies. It also provides a platform that facilitates the rapid integration of new or existing data into the analysis process, allowing for more rapid analysis and fusion of multiple threat vectors. The BDP will accelerate the integration of new analytical tools into the predictive analysis the Army conducts and leverage the experience to address and support all cyber threat needs.

BIO: Over the past three years, Enlighten IT Consulting LLC, a nontraditional defense contractor, has been providing the Defense Department with migration of data analytics, machine learning and artificial intelligence solutions in support of U.S Army Program Executive Office for Enterprise Information Systems, Army Cyber Command, Air Force Cyber, Marine Corps Cyber and U.S. Cyber Command networks.

Data in Extreme Environments

Herman Leybovich, Vice President of Engineering, Klas Telecom Government •
herman.leybovich@klastelecomgov.com

ABSTRACT

Data at the extreme network edge is growing at rapid rates. The ability to collect, process and distribute information in near real time has taken on new importance for decision making. The computing and storage resources traditionally used to do this are located in temperature-controlled data centers not tactical settings. Sensors are becoming more diverse with mission partners using different technology to perform the same functions. These factors make interoperability and the sharing of critical information in harsh environments unreliable and expensive.

By making the collection, processing and distribution functions modular, the company can rapidly innovate on the extreme network edge on the bedrock of reliability. The modularity of the Voyager ecosystem allows us to rapidly test, evaluate and field new capabilities without ripping out an entire system. Reliability of Voyager allows the company to put technology into spaces and places where other technology doesn't work. With the latest innovations in its product offering, Voyager is bringing true data center performance to new frontiers.

BIO: Herman Leybovich started his career in technology in 2007 as a satellite operator in the U.S. Marine Corps. Since 2011, he has held engineering roles in the private sector supporting both SLED and the federal government. In his current role as Klas Telecom Government's vice president of engineering, Leybovich leads a team of engineers that aligns the needs of their mission partners in defense, intelligence and public safety with Klas Telecom's technology strategy. He is married to Mikayla Leybovich, and they live in Northern Virginia.

DevSecOps Driven Big Data Platform

John Eubank, Technical Director, Alion • john.eubank@alionscience.com

ABSTRACT

The U.S. Defense Department's development and implementation of an open-source approach to massive scale data management has been accomplished through a joint collaboration between the services, multiple combatant commands and the 4th Estate. Under the Unified Platform efforts, the Big Data Platform (BDP) has been implemented at multipetabyte scale in the NIPRNet, SIPRNet and Joint Worldwide Intelligence Communication System AWS cloud environments. The success of the BDP implementation for the cyber-space operations community sets an impressive foundation for transformation of the platform's capabilities for the use in Joint All-Domain Operations (JADO).

The presentation would provide an overview of utilizing the existing BDP and implementing a DevSecOps Software Factory focusing on enhancing the baseline platform, ingesting new data sets, developing data analytics to include machine learning and deep learning, and building visualizations and applications to meet and exceed user needs. BDP comes with a parallel project for the tactical edge known as the Lower Echelon Analytics Platform (LEAP).

A unique aspect of the BDP and LEAP architecture is distributed sharing of queries and analytics both horizontally across the network and vertically across classifications. The distributed sharing approach moves result sets versus moving the entire data set, reducing the volumes across the network infrastructure. BDP and LEAP can be deployed to cloud architectures from the edge to enterprise along with traditional physical infrastructure.

BDP facilitates bringing the data together into a unified architecture across the U.S. Defense Department and IC. This facilitates the transfer of capabilities across organizations, reduction in service-specific customized training, cost avoidance from building and managing new data platforms, and the ability to share data in near real time for JADO.

The BDP's approach has been proven in the past eight years and is currently running at nearly 30 petabytes of data across all production deployments. The open architecture model of BDP has resulted in data being visible, accessible, understandable, trusted, interoperable and secure. Basing the software development in an Agile DevSecOps approach provides a highly dynamic development ecosystem to maintain software delivery at the speed of the fight.

The BDP brings a compilation of more than 40 industry leading open-source projects for big data use cases that have been hardened and accredited using the Risk Management Framework (RMF) for use across the NIPRNet, SIPRNet, Joint Worldwide Intelligence Communication System and SAP/SAR network classifications. The BDP for the cyber community provides a massive scale data hub making data readily shareable

and usable for the mission. It recently competed in and won the AFWERX Joint All-Domain Command and Control (JADC2) Challenge and, in GFY 21, the BDP is ready to become the JADO Data Hub. Alion is asking for additional partners to join the DevSecOps ecosystem in collaboration and development around the open-source architecture.

BIO: John Eubank has spent the past eight years tackling the U.S. Defense Department's massive scale data challenges from the tactical edge to the joint enterprise. Most recently, Eubank has taken on leading the Alion Information Warfare transformation for Joint All-Domain Operations. His day-to-day role is Alion's cyber technical director, providing solution design on full-spectrum cyberspace operations.

Eubank has a master's degree from the University of Maryland in information management and a bachelor's degree from Towson University in computer information systems and business administration (dual degree). His extensive background prior to entering the big data space included cellular telecommunications, accounting, oversight of NSA's East Campus build out and software engineering.

Army Migration of Data Analytics, Machine Learning and Artificial Intelligence Solutions in Army Enterprise Data Centers (AEDCs)

Scott Phillips, HPE Enterprise Software, Federal, HPE • scott.phillips@hpe.com

ABSTRACT

The technology realm is in the midst of a significant IT paradigm shift. The traditional approach of having applications dictate how data is organized and stored is going through a major transformation driven by increasing data volumes and the advent of more complex applications, particularly new AI/ML workloads that require large data volumes.

The classic IT landscape consists of three different foundational layers. Even today, these fundamental concepts haven't changed, but the construct of these functional layers has advanced.

Applications have evolved from being monolithic to multitier to today's connected network of distributed services weaved together through microservices. Middleware has evolved from being purely a runtime layer for applications to a layer for computational frameworks, orchestration engines and modern database technologies. Hardware has shifted from being physical to virtual to delivered as a resource through a cloud-consumption model.

However, none of those evolutionary steps considered data as a first-class enterprise citizen. As a result, the Army is faced with the challenge of data being stored across all layers without a universal way to manage and access it. Every step of abstraction in each of these foundational layers significantly increased data silos and complexity. Consequently, data management is difficult because data is not explicitly decoupled from its dependencies.

HPE has introduced a new plane in the stack called the Data Fabric. It disaggregates data from the modern constructs of applications, middleware and hardware. As a result, the Army will gain end-to-end control over data visibility, accessibility, pedigree and provenance, interoperability and security independent from any other layer in the IT stack.

The Data Fabric solves the challenges of managing the complexity of the modern data environment by managing data and its ecosystem from edge to core to cloud. As a result, the Army can focus more on how to leverage the data instead of being distracted by the management of multiple data technologies needed to support applications and analytics across the enterprise.

The Data Fabric is a critical layer within the enterprise IT stack because it:

- Provides a consistent data abstraction layer for enterprises to manage, secure, govern and protect data;
- Consists of standard APIs to simplify consumption and interoperability of any data by a broad set of applications and tools; and
- Seamlessly handles the complexity of data across locations, hardware infrastructures from on-premises to the cloud to the edge and containers.

The Data Fabric optimizes the entire data life cycle—from ingestion to multi-echelon and domain processing—to enable applications that simultaneously require real-time analytics, machine learning and AI. It gives complete flexibility in leveraging the underlying infrastructure on-premise, cloud or containerized infrastructure.

Mission benefits realized by utilizing the HPE Data Fabric include:

- Reducing TCO by sharing a common data infrastructure across echelon, teams and workloads;
- Providing consistent data governance and security enterprisewide;
- Delivering business-critical SLAs on open-source standards while leveraging modern tooling;
- Maximizing value from data with end-to-end controls on your most important digital asset: data; and
- Enabling MDO from core to edge, providing the ability to share data required to C2 decision making for mission requirements and increasing lethality.

BIO: Scott Phillips is an enterprise account executive for Hewlett Packard Enterprise Software Sales supporting the U.S. Federal Sector Business Unit. In this role, Phillips is responsible for driving software revenue across the unit. He joined HPE in 2020 after working multiple years with technology companies specializing in the big data AI/ML ecosystem where he was responsible for selling solutions to the Defense Department and civilian agencies. Phillips attended the State University of New York Polytechnic Institute, where he received a Bachelor of Science in telecommunications.

ML Training Data Ops: Best Practices

David Cook, Senior Director, AI and Machine Learning, Figure Eight Federal •
dave.cook@figure-eight.com

ABSTRACT

When faced with the overwhelming challenge of congested and contested environments in the multidomain battlefield, artificial intelligence and machine learning can prove invaluable to exploiting data as a strategic asset and achieving full operations/intelligence convergence. Foundational to that convergence, though, is imbuing content and context of the deployed environment into ML training data. Nothing moves in AI and ML without high-quality training data at scale. Only by labeling and reviewing ML training data with local context and pairing it with data from a central repository can analysts and field users gain the full situational and operational awareness that AI/ML in human-machine teaming provides.

A scalable ML DataOps solution—one that combines both open source and best-in-class COTs capabilities and is inherently flexible and easily deployable across enterprise and tactical edge networks—can assist the Army in meeting its goals of readiness and AI/ML dominance. Through an enterprise-grade ML DataOps pipeline, data can move easily from acquisition to enrichment, impacting the capabilities of the warfighter in near real-time.

Figure Eight Federal will discuss defining and designing an ML DataOps solution that works across multiple security classifications and clarify high-level best practices in ML data engineering and data enhancement that meet Army mission needs. The discussion will be informed by lessons learned on Project Maven, where Figure Eight Federal has been the authoritative ML training data platform since May 2017, working with the Joint Artificial Intelligence Center (JAIC) on multiple lines of effort and through its commercial SaaS experience creating more than 1B annotations each year for the last 14 years. On Project Maven, the Figure Eight Platform has been used to create over 350 million data labels since June 2020 using secure and unclassified networks. Hundreds of labelers have supported 25-plus lines of effort and a wide variety of unstructured data types. The JAIC and its commercial work provide an equally firm grounding in use cases and data types that be applied to Army mission challenges and dynamics.

Figure Eight Federal will bring its subject matter expertise to discuss the necessary infrastructure and compute for ML Data Ops, satisfying requirements for information assurance and security in an ML training data program and a Data Labeling and Annotation Pipeline design leveraging metadata lakes already deployed that provide consistent, iterative improvement across ML projects and programs. From data curation to model testing, evaluation and deployment—the end goal is to outline and support a foundational path forward to extensible, accessible high-impact Army AI/ML solutions.

BIO: Dave Cook is the senior director for AI and Machine Learning for Figure Eight Federal. He is a data science and geospatial practitioner based in Washington, D.C. Over his more than 25-year career, Cook has focused on solving complex challenges in law enforcement, intelli-

gence, defense, civilian government and across leading corporations worldwide. Believing that data science and analytics is more a marathon than a sprint, he holds firmly to the power of properly curated and managed data and the power of new applications in artificial intelligence and machine learning. Cook has a Master of Science in policy analysis and management information systems from Carnegie Mellon University and a Bachelor of Arts in American history and political science (information science) from Northwestern University. He has worked in data science and geospatial machine learning, both as an entrepreneur with his own company and with Figure Eight Federal since 2012.

Operation Decision Making Model With Qualitative and Quantitative Data

Matthew Maher, Data Scientist, Processus Group •
maherm@processusgroup.org

ABSTRACT

Processus Group explains the importance of combining quantitative and qualitative data in the learning process for artificial intelligence/machine learning. The company provides some examples of how it has used the sematic power of ontologies/knowledge graphs. The examples it offers capture warfighter knowledge, training and intelligence as qualitative data in the semantics of the modeling process. Its examples show how the company created qualitative semantics in the data and object properties in an ontology to provide the warfighter knowledge in the military decision-making process (MDMP).

One of the goals of artificial intelligence is to have a machine aid in the decision-making process by determining patterns and potential outcomes that mimics human intelligence. However, for artificial intelligence to make decisions like a human, it would have to have a way to replicate the concept of knowledge, experience and training. Put another way, it would have to replicate qualitative data in the decision-making process.

In a human, qualitative data provides context to the quantitative data that is processed to make these decisions. To use data for decision making, the analysis of data must support both quantitative and qualitative data.

Quantitative data analysis is objective because it is based on mathematical and statistical research methods. The number of soldiers and weapons, the geometry of the battlefield and the range of weapons are all examples of quantitative data. Qualitative data is generally more subjective and is dependent on people's experience, knowledge, training and biases.

Processus Group's process creates dynamic situational understanding by combining data with knowledge. Put another way, Data + Knowledge = Understanding. Understanding leads to faster, more accurate and better coordinated decision making, especially in a system-of-systems and/or multidomain environment.

BIO: A former Army Officer assigned between special operations and conventional forces and a current data scientist, Matthew Maher is supporting AFCEA's technical pillar as the subject matter expert in data analytics. He has published several papers on the area of reducing the warfighters cognitive burden, leveraging ontologies/knowledge graphs to combine qualitative and quantitative data for decision making and the creation of cognitive architectures, sematic data models and operational knowledge graphs for AI/ML training.

Attending to the Unattended: RPA Crytographic Authentication

Brent Hansen, Chief Technology Officer, Thales Trusted Cyber Technologies • mary.shiflett@thalestct.com

ABSTRACT

U.S. federal agencies often require PKI certificate-based authentication to perform Windows logon and to access public-key-enabled systems. This requires use of a multifactor authentication token that performs a cryptographic operation using the certificate and keys residing within the token.

Traditional multifactor authentication introduces roadblocks to technologies like robotic process automation (RPA). OMB Memo M-19-17 outlines a policy that requires management of digital identities of nonperson entities such as software robots. This means that all software robots are required to have individual digital identities and credentials that are managed in the same fashion as traditional user identities. Although software robots cannot be issued a physical token, they can utilize multifactor login capabilities through the use of a centralized, hardware security module-based authentication system.

Thales Trusted Cyber Technologies will discuss RPA cryptographic authentication best practices including:

- Generating and protecting PKI credentials for software robots;
- OMB Memo M-19-17 compliance for RPA; and
- An RPA federal implementation overview.

BIO: Brent Hansen is Thales TCT's chief technology officer. He leads Thales TCT's sales engineering organization and spends the majority of his time evangelizing and strategizing on data-centric approaches for federal agencies looking to avert being the next victim of a data breach.

Hansen brings more than 19 years of IT experience in data and enterprise architecture, data warehousing, big data and business intelligence. He is an industry expert in data encryption and tokenization. He leads teams that architect security strategies to secure and protect sensitive data for both federal government and large commercial enterprises across the globe.

Data Security for the Perimeterless Hybrid Cloud Environment

Brent Hansen, Chief Technology Officer, Thales Trusted Cyber Technologies •
mary.shiflett@thalestct.com

ABSTRACT

The Army Network cannot rely on network and endpoint security alone but rather must depend on the defense in depth necessary with controls closer to the data to ensure security in a perimeterless environment. Encrypting sensitive data is a fundamental part of any cybersecurity strategy. However, the cryptographic keys used to encrypt and decrypt data are often overlooked.

Cryptographic keys are the keys to the kingdom. Large volumes of encrypted data yield copious amounts of cryptographic keys that need to be managed, stored and secured. If these keys are compromised, attackers can gain access to encrypted information.

Many infrastructure, platform and software-as-a-service providers offer data-at-rest encryption capabilities with encryption keys managed by the service provider. Many industry or internal data protection mandates, as well as industry best practices as defined by the Cloud Security Alliance, require that keys be stored and managed remotely from the cloud service provider and the associated encryption operations. Providers can fulfill these requirements by offering bring-your-own-key (BYOK) services to enable customer control of the keys used to encrypt their data. Customer key control allows for the separation, creation, ownership and control, including revocation of encryption keys or tenant secrets used to create them.

Thales Trusted Cyber Technologies addresses how to effectively implement BYOK services to secure the modern hybrid, multicloud architecture, including:

- The challenges of securing and managing hundreds of master keys per subscription across multiple clouds;
- Understanding how, when and by whom encryption keys are used;
- Reducing enterprise complexity via secure key management utilizing a FIPS (140-2 L3) boundary to support data on premise and in a multicloud enterprise, rather than relying on disparate point solutions; and
- How to make data accessible, trusted and secure to meet compliance with the Army Data Strategy, map to recommendations in the Defense Information Board (DIB) Zero Trust Architecture and NIST SP 800-53 security and privacy controls.

BIO: Brent Hansen is Thales TCT's chief technology officer. He leads Thales TCT's sales engineering organization and spends the majority of his time evangelizing and strategizing on data-centric approaches for federal agencies looking to avert being the next victim of a data breach.

Hansen brings more than 19 years of IT experience in data and enterprise architecture, data warehousing, big data and business intelligence. He is an industry expert in data encryption and tokenization. He leads teams that architect security strategies to secure and protect sensitive data for both federal government and large commercial enterprises across the globe.

Accelerating Cybersecurity Through AI/ML Automated Prioritization and Root Cause Analysis

Duncan Stewart, Director, Strategic Development, Axellio •
duncan.stewart@axellio.com

ABSTRACT

Modern cyber adversaries use sophisticated multistage and multihost attack techniques. Because of current limitations of intrusion detection and forensic analysis tools, reconstructing attack scenarios is extremely challenging and results in delayed anomaly detection, threat identification and resolutions. The volume, velocity and variety of attacks create thousands of SIEM or SOAR events that leave frontline defensive cyber operators overwhelmed and unable to effectively and efficiently triage priorities among major threats, minor threats and false alarms. To combat complex cyber attacks, a new approach is needed that combines event data with detailed attack data then employs AI/ML algorithms to improve threat analysis and prioritization.

There is a solution that uses an intelligent threat analysis framework that prioritizes the most severe threats while streamlining root cause analysis. Combining SIEM and SOAR event data with detailed attack data derived from actual network packets will increase available threat information and situational awareness while improving productivity of the limited analyst resources. It combines expert insight with AI/ML guidance to automate the manual task of alarm prioritization and response. This simplifies and accelerates access to the incident data by pre-selecting packets relevant to the reported alarm. It also automates the initial packet analysis rather than leaving this entirely to the analyst expertise—weeding out false positives and annotating the presented packet data, highlighting anomalies and identifying additional threats. This approach requires powerful hardware platforms that can ingest, store and process vast amounts of network data in near real time.

Axellio is employing its revolutionary edge-computing systems to drive advanced AI/ML cybersecurity solutions. Given the vast amount of data and constantly shifting threat vectors, AI and ML models are perfect to accelerate the learning process, avoiding lengthy manual reprogramming of the analysis logic as typical in today's applications. This results in reduced time-to-threat mitigation by increasing the available attack information and situational awareness while reducing the time spent on false positive alerts. This improves the team's productivity, allowing it to focus on higher priorities and reduce case backlog.

BIO: Lt. Col. Duncan Stewart, USAF (Ret.), is the director of strategic development at Axellio Inc. He is responsible for exploring military and intelligence applications of the company's commercial innovations in edge computing. Col. Stewart served for 24 years in the active duty and reserve Air Force. During his career, he served as an acquisition program manager for advanced

avionics, sortie generation officer for fighter and tactical aircraft and senior logistics officer at the COCOM level. He created the Strategic Innovation course at the U.S. Air Force Academy and supported several major science and technology initiatives. He is the former CEO of the Colorado Springs Technology Incubator and CEO of Quadric Biomedical. He currently serves as the chairman of the board of ConcealFab, the technological leader in telecommunication mounting infrastructure. Col. Stewart earned a Bachelor of Science in management from the U.S. Air Force Academy, a Master of Science in aerospace management from Embry-Riddle and an MBA from Notre Dame University. He is a patented inventor of several electromechanical and biomedical devices and maintains a TS clearance.

Enterprise and Warfighting Systems 'And Never the Twain Shall Meet' or Do They Meet at the AEDC?

Gina Myers, Public Sector, Commvault • gmyers@commvault.com

ABSTRACT

Is integrating more data analytics, machine learning and AI—or more precisely expert systems—the Holy Grail of bridging information sharing and distribution between the enterprise and tactical edge?

Army Enterprise Data Centers (AEDCs) developed not as much to fill an operational gap but more as a natural part of life-cycle refresh leveraging modernization to deliver ever more compute and store in ever smaller footprints. When coupled with cheap fiber transport capable of moving vast amounts of data with performance reaching that of having on-prem infrastructure, regional consolidation along enterprise mission areas made sense.

Add a major BRAC effort from 2010 to 2012 for good measure and AEDCs became part of the information technology fabric providing both effective and efficient operational enterprise solutions as the Army continued its path toward consolidated information technology architectures.

Returning forces leveraged these consolidated data centers as an installation as a docking station to better integrate their tactical G1, G2, G3, G4 and G8 systems with the enterprise business equivalents. These units also leveraged the centers to host training modules to maintain skills and certification. That creativity quickly created dependencies to the point that when Army units deploy back into real world undeveloped areas, the constrained transport bandwidth at the tactical edge becomes a limiting factor in maintaining combat readiness. This gap at the tactical edge is not new but now more than ever has to be addressed by more than increasing the bandwidth with compression technology or WAN equalizers that have only generated marginal improvements. The gap remains and is increasing under the crush of an ever-increasing volume, velocity and variety of data from myriad IoT devices being fielded.

Commvault will explain how holistic data management systems that integrate data analytics, machine learning and expert systems are offering alternative solutions to ensuring a distribution scheme where the right data if provided just in time in the right data package to allow the tactical edge to leverage the compute and store capability of the AEDC. The AEDC can leverage new technology that extends cloud-like compute and store to the edge in highly resilient software defined solutions. In addition, holistic data management systems can provide multitenancy RBAC-controlled single set of code and intuitive dashboard interfaces to managed data readiness from the rear and enterprise locations to the tactical edge.

BIO: Richard Breakiron is Commvault's senior director, strategic initiatives, Americas public sector, focused on the federal community. He gained his extensive experience in developing, deploying and operating critical network information technology and large data management systems while serving as an officer the Army, senior government civilian with the Army and DISA and U.S. security agencies.

STATISTICAL NATURAL LANGUAGE PROCESSING TO SUPPORT MISSION UNDERSTANDING

Reducing the Warfighters Cognitive Burden

Matthew Maher, Chief Data Scientist, Processus Group •
maherm@processusgroup.org

ABSTRACT

One of the goals of intelligence systems is to have a machine aid in the decision-making process that mimics human intelligence by determining patterns and potential outcomes. However, for artificial intelligence to make decisions like a human, it would have to have a way to replicate the concept of knowledge, experience and training. Put another way, it would have to replicate qualitative data in the decision-making process.

In humans, qualitative data provides context to the quantitative data that we process to make these decisions. Humans can combine quantitative and qualitative data to combine mathematical measures with creativity and emotional intelligence to make decisions better and faster than their competition. Now, if a machine could understand the same context through knowledge, experience and training then create relationships with quantitative data, we could increase the ability to use artificial cognitive capabilities to aid in the decision-making process.

The Processus Group has shown how this can be accomplished though the combination of natural language processing and the creation of knowledge graphs that capture the relationship of operational processes to generate an OPROD. The organization has developed each section of the OPORD as "object properties" in the knowledge graph and then defined the relationship of quantitative data (AOR, friendly forces, timeframe, etc.) with qualitative data (commander's intent, goals, situation, etc.) to show a mapping of information that exists, or is created, in products that are yielded throughout the military decision-making process. This mapping allows users to leverage natural language processing to fill in much of the data in the OPORD and provide a process for combining qualitative and quantitative data so commanders can make faster and better decisions.

By providing both data capabilities in a model, Processus Group allows non-experts to make expert decisions. Put another way, the organization helps the combatant commander understand how cyber, EW and other nonkinetic capabilities can fulfill the command guidance. To provide the answers and/or a path to solving the operational contextual intelligence in a system, Processus executes a mission engineering (ME) process that analyzes the organization's or domain's state of readiness. The process is a detailed analysis that provides an assessment of how the people, systems, knowledge, data and processes are aligned to the operational outcomes. It adds a layer of operational viability to existing engineering processes with the goal of ensuring the program enhances knowledge sharing, reduces cognitive burdens and increases semantic understanding.

Processus' paper, "Reducing the Warfighters Cognitive Burden," was awarded the paper of the year at the ICCC. Beating out papers from Google, IBM, Amazon, Stanford, Cornell and other large tech companies and top universities because the organization proved how qualitative data can be captured in the semantics of a knowledge graph and used in the training of an intelligent system.

BIO: A former Army officer assigned between special operations and conventional forces and currently a data scientist, Matthew Maher is supporting AFCEA's technical pillar as the subject matter expert in data analytics. He has published several papers in the area of reducing the warfighters' cognitive burden by leveraging ontologies/knowledge graphs to combine qualitative and quantitative data for decision making and the creation of cognitive architectures, sematic data models and operational knowledge graphs for AI/ML training.

Using NLP to Automate Some Mission Analysis, Planning and C2 Functions

Jason Crabtree, CEO, QOMPLX Inc • jason@qomplx.com

ABSTRACT

Q:OS, QOMPLX's data fabric, allows the continuous, concurrent evaluation of streaming data (e.g., from network logs) based on configurable rulesets. Ruleset evaluations can trigger real-time alerts and/or trigger pre-configured workflows. The triggered alerts and workflows act to draw attention to and/or resolve the anomalies that were detected by the rulebooks, ensuring that human reviewers' attention is reserved for only true and/or severe emergencies. Q:OS also contains the company's Model Management and Data Management products. Model Management includes NLP routines and structured-data transformation and schematization routines.

Q:OS thus comprises components that can robustly be configured for the parallelly similar Mission Understanding scenario. Using Q:OS, a rule-based workflow can be configured to parse and analyze OPORDs to identify key tasks and potential automated or semi-automated course of action development. This further analysis would be an NLP routine with its own configured workflow that would annotate the OPORD, tagging critical requirements and identifying supported and supporting relationships among units.

Concurrently, staff can configure Q:OS's rules-management and orchestration components on their own to map out the dependent systems that need to be conditionally incorporated into the workflow. Upon operation of this configuration of Q:OS, it will be possible to recommend or automatically execute the course(s) of action previously mapped using the rules-management and orchestration components. During execution, the NLP routine will be able to analyze SIGACT messages of various formats, automatically update the common operating picture and cross check the messages against key information requirements such as commander's critical information requirements to update commanders and key staff elements rapidly.

BIO: Jason Crabtree is a cofounder and serves as the chief executive officer and board member at QOMPLX. He is an expert on cybersecurity, operational risk management, decision support/automation technology and simulation/predictive modeling of complex-adaptive systems. As a Rhodes scholar, Crabtree researched artificial intelligence-based optimization of engineering design processes at Oxford University. First Captain of his class at West Point, he is a licensed professional engineer who served as a Ranger/Sapper-qualified infantry leader in Afghanistan before completing military service as a special assistant to senior U.S. Defense Department cyber leadership with emphasis on the development and operational integration of advanced technology initiatives including work with DARPA. Crabtree also was a 2014 Cyber Policy Fellow with the Madison Policy Forum in New York City and a 2016 Cyber Fellow for the New

America Foundation. He has been an invited participant, panelist and speaker on energy, risk management, finance and security for organizations, including the Casualty Actuarial Society, Financial Services Roundtable, the Center for New American Security, the Markle Foundation, the Ditchley Foundation, the Gridwise Architecture Council and RAND in both the United States and United Kingdom.

Big Data Platform/Threat Hub

Steve Wagner, Vice President, Enlighten IT Consulting, LLC •
swagner@eitccorp.com

ABSTRACT

Enlighten proposes utilizing the existing implementation of the Big Data Platform (BDP) Threat Hub application to provide natural language processing (NLP) capabilities for processing structured and unstructured text, establishing automated workflows and initiating courses of action (COAs) to reduce human interaction and maximize understanding of issued military orders.

The BDP is a government off-the-shelf technology originally developed by Enlighten under contract with the Defense Information Systems Agency (DISA) and has evolved through joint collaboration, research and development with U.S. Cyber Command, U.S. Army Cyber, U.S. Air Force Cyber and U.S. Marine Corps Cyber. These military organizations have production implementations of the BDP that process and store live and historical network, mission and threat data, ranging from multi-terabyte to multi-petabyte implementations.

One of the augmenting technologies is the Threat Hub application, which serves as a singular repository of cyber threat indicators for the U.S. Defense Department. By processing structured feeds of cyber threat intelligence reporting and parsing unstructured text using regular expression algorithms, Threat Hub provides a distributed network of shared indicators of compromise to intelligence analysts and on-net cyber operators that are supported by contextual source reporting. Threat Hub also includes customizable workflows that guide analysts through defensive processes to mitigate threats to Defense Department networks.

Integrating natural language processing algorithms—such as terminology extraction, relationship extraction and sentiment analysis—into Threat Hub can be used to identify key cyber terrain referenced in written orders and/or relationships between entities in the corpus of data stored in the BDP, resolve mission dependencies, graphically represent those relationships and recommend COAs based on automated playbooks. As the NLP capability, playbooks and APIs are refined, the need for human interaction in exercising some defensive actions could be eliminated completely.

Because the BDP is already deployed to NIPRNet, SIPRNet and Joint Worldwide Intelligence Communication System, integration with the Unified Platform's WOLFDOOR program can allow NLP-informed workflows to cross security domains, allowing critical mission, threat and network data to be utilized to more effectively address emerging information, reducing the amount of time to respond and reducing cognitive loads across the cyber operations workforce.

BIO: Over the past four years, Enlighten IT Consulting LLC, a nontraditional defense contractor, has been providing the Defense Department with similar metadata extraction capabilities in support of U.S. Army Program Executive Office for Enterprise Information Systems, Army Cyber Command, Air Force Cyber, Marine Corps Cyber and U.S. Cyber Command networks.

MISSION MAPPING AND DEPENDENCY MODELING OF MISSION-CRITICAL SYSTEMS

Mission Mapping and Dependency Modeling of Mission-Critical Systems

Jason Crabtree, CEO, QOMPLX Inc. • jason@qomplx.com

ABSTRACT

Integrating disparate, interdependent and mission-critical data systems is a multi-layered challenge. It starts with ingesting and processing raw data at high volumes and low latencies followed by establishing analytics and monitoring processes for each data source. Finally, each system needs to be represented in an ontology designed to assess the interconnected resilience and vulnerabilities at each node. For forward-looking analytics, there's the additional task of leveraging historical datasets to implement forecasting methodologies.

The Q:OS platform provides a data fabric with pre-integrated products that tackle each of these steps. It is built on top of a component registry that includes datasets, models and workflow automation tools. Data sources are registered with appropriate data transformation and schematization processes, allowing for health monitoring and advanced analytics on different systems.

All registered datasets can be tagged and contextualized with dependency information that capture the relationships between different data sources. As different anomaly detection and alert systems monitor individual datasets, a graph-based data model ensures potentially cascading failures, are identified and addressed expeditiously. This ontology serves to mitigate the potential impact of critical failures including data integrity issues, network congestion and communication loss. Historical anomaly detection datasets also are stored in the registry and leveraged to build time-series forecasting models that anticipate and flag system-wide stability risks. The results of this dependency modeling and the identification of potentially critical failures will help in the prioritization of assets for cyber and EM protective measures.

BIO: Jason Crabtree is a cofounder and serves as the chief executive officer and board member at QOMPLX. He is an expert on cybersecurity, operational risk management, decision support/automation technology and simulation/predictive modeling of complex-adaptive systems. As a Rhodes scholar, Crabtree researched artificial intelligence-based optimization of engineering design processes at Oxford University. First Captain of his class at West Point, he is a licensed professional engineer who served as a Ranger/Sapper-qualified infantry leader in Afghanistan before completing military service as a special assistant to senior U.S. Defense Department cyber leadership with emphasis on the development and operational integration of advanced technology initiatives including work with DARPA. Crabtree also was a 2014 Cyber Policy Fellow with the Madison Policy Forum in New York City and a 2016 Cyber Fellow for the New America Foundation. He has been an invited participant, panelist and speaker on energy, risk management, finance and security for organizations, including the Casualty Actuarial Society, Financial Services Roundtable, the Center for New American Security, the Markle Foundation, the Ditchley Foundation, the Gridwise Architecture Council and RAND in both the United States and United Kingdom.

Big Data Platform/REDMAP

Steve Wagner, Vice President, Enlighten IT Consulting LLC •
swagner@eitccorp.com

ABSTRACT

Enlighten proposes enhancing the existing implementation of the Big Data Platform (BDP) REDMAP application to provide mission mapping and dependency modeling of mission critical systems.

The BDP is a government off-the-shelf technology originally developed by Enlighten under contract with the Defense Information Systems Agency (DISA) and has evolved through joint collaboration, research and development with U.S. Cyber Command, U.S. Army Cyber, U.S. Air Force Cyber and U.S. Marine Corps Cyber that have production implementations of the BDP that process and store live and historical network, mission and threat data, ranging from multi-terabyte to multi-petabyte implementations.

One integrated dashboard providing situational awareness of mission relevant assets on the BDP is the REDMAP capability. REDMAP visualizes a geographic representation of mission-relevant terrain: cyber. The capability allows for configurable grouping of critical assets and facilitates situational awareness by providing automated alerting to inform users of vulnerabilities associated with the cyber terrain. Alerting is triggered by a series of analytics that ensure only relevant alerts are pushed to users. Alerting is configurable and can be tailored to any data set with any parameters. REDMAP provides near real-time situational awareness by monitoring relevant data sets as they are ingested into the BDP and alerting users as soon as relevant data is seen.

By incorporating additional data sets and developing enhancements to the dashboard, REDMAP's mission mapping capabilities can be extended, providing additional context to decision makers. Incorporation of MADSS data can provide REDMAP with authoritative task critical asset mappings from the operational community, allowing REDMAP to present mission mappings of key cyber assets in a user-friendly and intuitive user interface. With further incorporation of data sets, such as eMASS, SolarWinds, VMWare and vROPs, REDMAP can provide insight into system health and status. Correlating system health information with mission mapping and cyber key terrain will show the linkages between system health and mission readiness.

The intuitive and configurable nature of REDMAP provides an ideal integration point for aggregating disparate data sets to provide mission mapping and dependency modeling. Mission relevant data is segregated and siloed in disconnected tools and systems. REDMAP and the BDP can bring these various data sources together to provide a real-time dashboard that allows commanders and staff to observe, orient, decide and act quickly upon mission relevant information.

BIO: Over the past four years, Enlighten IT Consulting LLC, a nontraditional defense contractor, has been providing the Defense Department with similar metadata extraction capabilities in support of U.S. Army Program Executive Office for Enterprise Information Systems, Army Cyber Command, Air Force Cyber, Marine Corps Cyber and U.S. Cyber Command networks.

Intelligent Management of Mission-Critical Information Pathways

Hunter Moore, Principal Researcher, Rotunda Solutions Inc. •
hmoore@rotundasolutions.com

ABSTRACT

Today's modern battlefield is a dynamic conglomeration of ground, air and satellite surveillance tightly intertwined with critically timed communications, sequential tasks and complex interdependencies between dispersed warfighters, command elements and multiple tiers of mission systems. The continuity of these entities is essential for providing key information necessary for timely and strategic decision-making. Data proceeding from these collective resources must be gathered and organized in a manner conducive to efficient, secure and reliable analysis and dissemination, whether at the strategic apex, the tactical edge or some node in between.

Accordingly, failure along this network can have compounding effects, negatively impacting the execution of warfighting functions, disrupting the timely flow of crucial information and potentially endangering lives, assets and mission success. It is essential that operational elements not only understand the cross-domain functions, relationships and impacts of key systems but also are armed with real-time data to predict and preempt the risks of compromised systems, prepare responses to potential resulting states and to navigate the decision space that emerges to mitigate damage and ensure the best ensuing course of action.

This talk proposes a system that monitors the current state of each of these individual battlefield subsystems to monitor mission-critical dependencies, actively assess and profile a stance of risk and proactively determine alternate pathways to avoid emerging obstructions in information delivery.

Through the utilization of sensor fusion and reinforcement learning techniques, the presentation will generate three main deliverables. First, it will provide an assessment of the current state of the battlefield agents as discussed above. Second, it will provide a decision-support tool for dispensing resources in an efficient manner to fix and/or maintain mission-critical components such as communication hubs and power stations. Third, the proposed system will provide a real-time analysis of the most efficient and secure alternate pathway for information transfer along a possibly compromised battlefield network, taking into account key features of the data being relayed. By continuously monitoring the pathways and analyzing the potential for nodal compromise, the system will be able to route information along the most secure, expedient and appropriate path available. Furthermore, it will alleviate the need for costly traditional methods of determination of secure pathways of communication, permitting for those cognitive resources to be applied in more mission-intensive decisions.

BIO: Hunter Moore is the principal researcher of Rotunda Solutions Inc. and oversees analytics strategies and the launching of new analytics lines of effort at the U.S. Defense Department Joint Artificial Intelligence Center (JAIC). In addition to his work at the JAIC, he has served as a researcher for projects for the Defense Innovation Board, NASA, the Department of Defense Chief Information Officer and commercial corporations. His project experience spans fleet management efforts, human systems, effort estimation and relevant to this effort, projects concerning smart battlefield/sensors research for deployed missions' systems. His professional experience includes experience as a professor, engineer, scientist and consultant.

DevSecOps Architecture for Mission Mapping

John Eubank, Technical Director, Alion • john.eubank@alionscience.com

ABSTRACT

For the Army challenge of mission mapping and dependency modeling of mission critical systems, an existing capability is in place that was built out under the Joint Cyber Command and Control (JCC2) program known as Big Data Platform (BDP). BDP as a software solution is paired with an Agile DevSecOps delivery approach to provide rapidly scalable and adaptable planning and analysis utilizing modeling and simulation (M&S), artificial intelligence (AI), massive scale data collection and storage and cutting-edge user-driven visualizations.

BDP provides the joint warfighting community an open architecture with documented APIs and web services for connecting to and integrating the disparate sensor data feeds in a machine-to-machine model and pairing that with natural language processing to extract value from human-generated reports, tickets and other content in a human-to-machine model. Within the platform, machine-generated and human-generated data can be correlated and analyzed using a variety of analytics, machine learning (ML) and deep learning capabilities.

The platform is differentiated in that it provides a data science ecosystem for analytics and AI to be applied to the corpus of data that is collected and stored inside the system. To determine impacts of failures and degradation across thousands of data types an architecture needs to allow AutoML to plug in various models depending on user criteria and mission tasks. Often, the infrastructure is a constraint, limiting the number of models that can be applied at one time. AutoML combined with a data science enables the DevSecOps environment be live in production, which facilitates implementation of notebook capabilities to obtain the necessary outputs from the data.

Critical to the architecture is understanding the data integrity, reliability and trustworthiness of data. Drawing from the platform's use across the U.S. Defense Department for the past eight years, capabilities like Feed Health, a BDP app, can be used to provide near real-time understanding of the data quality and its impact the analytic accuracy to inform warfighting functions.

The BDP apps for JCC2 were developed to support cyber mission planning, battlespace management, mission assurance and decision support. The platform recently won the AFWERX Joint All-Domain Command and Control (JADC2) Challenge. This competition highlights the value in transforming BDP from a cyber warfighting platform to be a mission agnostic warfighting system.

The platform is primarily utilized as an enterprise cloud massive scale data processing system. The Army has been investing in a complementary project known as the Lower Echelon Analytics Platform (LEAP) for use at the Edge and Fog. BDP and LEAP are distributed architectures facilitating queries, analytics, deep learning and machine learning models running across multiple implementations of the platform and then aggregating result sets back to a single operators or decision maker.

A core of the BDP's approach is Agile DevSecOps whereby new applications can be built and fielded in hours or days to keep pace with the changing operational environment. Deployed DevSecOps engineers can facilitate tailoring and updating capabilities based on the availability of data, processing infrastructure and other constraints at the edge. In parallel centralized DevSecOps engineering teams at the enterprise

can be working to build large-scale capabilities. Getting a rapid capability development enables accurate mission mapping with direct correlation to available data with highlighting of the gaps and reliability issues in the data informing decisions.

BIO: John Eubank has spent the past eight years tackling the U.S. Defense Department's massive scale data challenges from the tactical edge to the joint enterprise. Most recently, Eubank has taken on leading the Alion Information Warfare transformation for Joint All-Domain Operations. His day-to-day role is Alion's cyber technical director, providing solution design on full-spectrum cyberspace operations.

Eubank has a master's degree from the University of Maryland in information management and a bachelor's degree from Towson University in computer information systems and business administration (dual degree). His extensive background prior to entering the big data space included cellular telecommunications, accounting, oversight of NSA's East Campus build out and software engineering.

COMMON DATA FABRIC WITH CROSS-DOMAIN CAPABILITY

Common Data Fabric With Cross-Domain Capability

Jason Crabtree, Chief Executive Officer, QOMPLX Inc • jason@qomplx.com

ABSTRACT

QOMPLX has built an enterprise data fabric, Q:OS, that can integrate domain-specific applications for multiple distinct domains. Each application can acquire data from multiple, internal and external, streaming and batch sources and can organize it into its own common domain-specific knowledge base. Each application also can periodically share data, at the requisite level of granularity and transformed into the appropriate format and schema, with each other. The underlying data fabric, Q:OS, enables this concert to operate alongside the core functionality of each application. It provides storage, orchestration and transformation services for data that is common to, external to or internal to both applications.

The company presents Q:OS's role in this hybrid application scenario as a limited example of the capabilities required for and challenges inherent in developing the data fabric the Army needs. Such capabilities include granular access-control, down to a single row or a small subprocess, configuring its storage components to design and scale a multiformat (suited to a particular set of use-cases/models), common knowledge-base and building an extensible roster of models and data transformations that operate atop this base. Q:OS also allows the configuration of workflows and APIs to share data between the knowledge-base and models/transformations. Configurable APIs also are useful when exposing analytics results to an end-user through screens.

BIO: Jason Crabtree is a cofounder and serves as the chief executive officer and board member at QOMPLX. He is an expert on cybersecurity, operational risk management, decision-support/automation technology and simulation/predictive modeling of complex-adaptive systems. As a Rhodes scholar, Crabtree researched artificial intelligence-based optimization of engineering design processes at Oxford University. First Captain of his class at West Point, he is a licensed professional engineer who served as a Ranger/Sapper-qualified infantry leader in Afghanistan before completing military service as a special assistant to senior U.S. Defense Department cyber leadership with emphasis on the development and operational integration of advanced technology initiatives including work with DARPA. Crabtree also was a 2014 Cyber Policy Fellow with the Madison Policy Forum in New York City and a 2016 Cyber Fellow for the New America Foundation. He has been an invited participant, panelist and speaker on energy, risk management, finance and security for organizations, including the Casualty Actuarial Society, Financial Services Roundtable, the Center for New American Security, the Markle Foundation, the Ditchley Foundation, the Gridwise Architecture Council and RAND in both the United States and United Kingdom.

Normalizing Data for the Common Data Fabric

Shawn Campbell, Product Manager for Government Solutions, Owl Cyber Defense LLC • scampbell@owlcyberdefense.com

ABSTRACT

As the Army and other organizations evolve their data infrastructure for on-premise to a hybrid integration of public cloud, private cloud and on-premise implementations, the data and the way it is transformed also needs to evolve. Data transformation requires establishing consistent, complete and correct structures for definition, access, processing and transfer of the data. Innovations can be used in cross-domain solutions for data description and transformation both for cross-domain solution (CDS) domain crossings and pervasively throughout the rest of the common data fabric.

To transfer data between and among security domain-based data infrastructure silos requires the use of CDS technology. CDSs provide both flow and content controls for the transfer of the data. In the past two years, they have been transforming in similar fashion to data infrastructures. There is now a common CDS fabric being established under the auspices of the National Cross Domain Strategy and Management Office (NCDSMO) and its Raise The Bar (RTB) mandate. The mandate prescribes continuing innovative rigor and robustness for both the system assurance as well as the content assurance of data being transferred.

That content assurance is being driven by improvements in content filtering technologies, processes and practices. A nexus for those improvements with the transition to a common data fabric is using the data format description language (DFDL) to establish common data models, called DFDL schema, that describe diverse native text and binary data formats. CDSs are using DFDL to normalize those diverse formats into XML so they can consistently, completely and correctly inspect/validate and sanitize that content through filtering pipelines to ensure the transferred data is clean in accordance with organizational and data owner policies.

A critical area for both CDSs and other aspects of common data fabric will require enabling data owners and architects to use tools like DFDL for establishing common schemas for the variety of data models/standards (for example CMF, LINK16, USMTF, VMF, STANAG 4774/4778) and then being able to establish normalized data structure (for example XML) using standardized common models (such as NIEM, UCI, DDMS). In CDS, this enables standardized content control pipeline filters for inspection and sanitization to ensure clean collected data is transferred for analytic and exploitation processing. Similarly, consistent common data structure is required for similar evaluation for command and control, alerts and tips, and other reporting flows to ensure clean releasable data is transferred to engaged entities in contested environments. In both flows, those common data structures are denormalized into native formats prior to reaching the destination endpoints.

The next stage will be to increase the effectiveness of the common data fabric by enabling essential interrogatory and processing mechanisms, like Apache Drill, with DFDL so that common data, both defined and processed, is pervasive throughout the common data fabric. This effort will require close coordination among standards bodies, mission data processing capabilities and vendors, enabling tools and mechanisms to pervasively enable the common data fabric for the definition, access, processing and transfer through the different data infrastructure silos.

BIO: Shawn R. Campbell is Owl Cyber Defense Solutions' product manager for its Government Cross Domain Solution (CDS) and One-Way Transfer product portfolios. In this role, he is directing the company's efforts to provide hardware- and software-enforced transfer CDS capabilities to Owl's customers in defense, intelligence and other government markets.

Campbell's career started as a U.S. Air Force linguist developing analyst tools on PWB Unix minicomputers. Those efforts led to working as a network analyst on the transition of ARPANET to MILNET and packet switch networking technologies for BBN. From there, he started down the path working software, system and security engineering efforts. These efforts spanned from developing communications testing infrastructures to leading Blacker and Caneware product test efforts, to working on SDNS, DGSA and GOSIP standards and defining agency-level next-generation security architectures while providing agency and mission ISSE support and eventually leading to his CDS development and product management roles.

Zero Trust for Machines and Humans Alike

Christie White, Federal Field Marketing Manager, CyberArk •
christie.white@cyberark.com

ABSTRACT

Privileged access management is a foundational component of a zero trust architecture but must be addressed for both human users and nonhuman entities. CAC-enabled, including legacy, systems can still be operated in a risk-appropriate manner.

Today's cyber warfare and risk mitigation strategies require not only ensuring the identity of those on the network and what they are doing but also making sure the next step is taken in analytics with adaptive multifactor and automatic responses based on user behavior.

CyberArk aligns with U.S. Defense Department CIO Lines of Effort and combines both behavioral analytics and correlation analysis to truly be 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, federal customer success manager at CyberArk, is a dedicated engineering resource for U.S. federal customers, both civilian and U.S. Defense Department. With more than four years of CyberArk experience, Jermyn works with clients as a trusted advisor to ensure customers are following best practices by deploying their privileged account security programs and advising clients to help reduce attack surface and close common attack vectors.

Archon ZV Secure Laptop: CSfC Compliant

Dylan Conner, Chief Technology Officer, ID Technologies–Archon •
ksamarin@idtec.com

ABSTRACT

In this time of COVID-19, mobile access to essential systems has become even more critical to national defense. However, legacy commercial solutions for classified (CSfC) systems have been overly complicated, cumbersome and unable to scale to meet the needs of those at the pointed end of the spear. ID Technologies features the art of the possible with CSfC, providing the commercial scale and experience promised by CSfC yet with the military grade security required.

ID Technologies has developed a suite of CSfC-enabled products that securely connect the cyber warrior at the last mile endpoint to the cloud. ID Technologies' Archon ZV secure laptop or phone is a CSfC-compliant endpoint built on a Dell Laptop or Google Pixel phone that can be used for secure access to multiple domains. A secure RTOS and custom mobile OS provide military-grade security for the unique requirements of cyber operations.

The Archon CF, an enterprise gray cloud fabric solution, provides last-mile transport to critical end users. When paired, the Archon Suite enables secure cloud connectivity virtually anywhere in the world. This enterprise-class solution has been built from the ground up to scale to support any size organization and features factory configuration and remote certificate renewals.

In this critical time, the Archon Suite provides not only a work-from-home solution but also greater productivity for those tactical mission users and greater security for mission sensitive systems.

BIO: As chief technology officer and vice president of technology, Dylan Conner is accountable for making the company's Accelerating Simplicity mission a reality for customers and partners. The work involves sustaining a diverse partner portfolio that aligns with current and emerging customer requirements, developing the presales architecture team and advancing the company's technical capabilities. Prior to joining ID Technologies, Dylan spent 18 years in IT sales, engineering and leadership, working as chief architect on a range of major federal government IT programs. He takes a keen interest in the intersection of technology, government and the social impact of the digital transformation.

Big Data Platform/Data Fabric Cross-Domain

Steve Wagner, Vice President, Enlighten IT Consulting LLC •
swagner@eitccorp.com

ABSTRACT

Enlighten is an established provider of software-based systems and architectures to serve as a common data fabric for parsing information into a common ontology, storing it and sharing it with mission systems across security enclaves.

Enlighten's approach is to utilize the BDP, a government off-the-shelf technology, originally developed by Enlighten under contract with the Defense Information Systems Agency (DISA) and has evolved through joint collaboration, research and development with U.S. Cyber Command, U.S. Army Cyber, U.S. Air Force Cyber and U.S. Marine Corps Cyber.

Through the utilization of the BDP, Enlighten proposes the aggregation and standardization of multiple data sources to meet mission objectives. From a Cross Domain Solution (CDS) perspective, knowing where data originates, the transport architecture and where it ultimately ends on the destination domain helps provide end-to-end context. CDS dataflows vary widely—anything from sensor collection to the output of analytic or even an analyst's document transfer.

The process for a successful data flow implementation requires detailed engineering requirements such as identifying the data origination point, the path the data flows, the format of the data, the frequency of data collection/delivery, the landing zones where the data will be transferred to and from the cross-domain solution and ultimately the final destination of the data.

The CDS engineering process can be summarized in five steps: requirements gathering, engineering, filter adaptation, filter testing and implementation. Each of these functions involves varying levels of effort to complete, depending on the complexity of the dataflow need. Furthermore, Enlighten understands there is no one-size-fits-all dataflow model and that a robust set of solutions should be in place to meet customer needs without re-engineering the CDS platforms.

While new data sources are being developed, unstructured data and unknown formats can be common. Enlighten recommends a separate inspection process for unstructured data that will allow the data to be formatted and marked appropriately. If this use case is defined ahead of time and a process is available, taking on these types of requirements could be standardized by the requisite approving authorities.

BIO: Over the past four years, Enlighten IT Consulting LLC, a nontraditional defense contractor, has been providing the Defense Department with similar metadata extraction capabilities in support of U.S. Army Program Executive Office for Enterprise Information Systems, Army Cyber Command, Air Force Cyber, Marine Corps Cyber and U.S. Cyber Command networks.

A DevSecOps-Enabled BDP Distributed Data Fabric

John Eubank, Technical Director, Cyber Solutions, Alion •
john.eubank@alionscience.com

ABSTRACT

Big Data Platform (BDP) is currently in use across the joint force for full spectrum cyberspace operations. A key aspect of the BDP's architecture is its open software architecture facilitating bi-directional distributed query and analytics across the U.S. Defense Department's cross-domain solutions (CDS). Currently BDP is connected low-to-high and high-to-low across the WOLFDOOR CDS farm.

BDP for Army Cyber has been implemented as GABRIELNIMBUS (GN) on multiple classification networks. Drawing from the BDP's performance at multi-petabyte scale for the joint force cyber community the next iteration in the life cycle is to expand its use for noncyber use cases, starting in support of information warfare and Joint All-Domain Command and Control (JADC2) prioritized use cases.

The platform provides the U.S. Defense Department a common data fabric with data lake, data transport, cloud and hardware deployments, network throughput optimizations, a common ontology and sharing across security enclave capabilities. BDP does this using a government off-the-shelf approach, reducing license and total cost of ownership.

For the strategic success of BDP, a focused effort is needed to implement a joint force BDP [data] governance board. The ability to share data within a service is critical; however, for JADC2's success, cross-service interoperability is just as important. The open architecture of the platform is an enabler of the joint common data fabric underlying JADC2.

BDP also provides a Kubernetes ecosystem for rapidly integrating new data flows and capabilities using government and contractor DevSecOps resources. Rapidly being able to build new machine-to-machine interfaces is a critical aspect of the common data fabric. These interfaces must facilitate open, reliable and transparent data communications for auditing, a CDS requirement; tracing issues; and building new connectors.

BIO: John Eubank has spent the past eight years tackling the U.S. Defense Department's massive scale data challenges from the tactical edge to the joint enterprise. Most recently, Eubank has taken on leading the Alion Information Warfare transformation for Joint All-Domain Operations. His day-to-day role is Alion's cyber technical director, providing solution design on full-spectrum cyberspace operations.

Eubank has a master's degree from the University of Maryland in information management and a bachelor's degree from Towson University in computer information systems and business administration (dual degree). His extensive background prior to entering the big data space included cellular telecommunications, accounting, oversight of NSA's East Campus build out and software engineering.

Toward a Common Data Fabric via an Integrating Semantic Framework for Army Mission Systems

Forrest Hare, Solution Architect, SAIC • forrest.b.hare@saic.com

ABSTRACT

In today's military environment, advances in collection and storage technologies have led to an explosion in enterprise data volume. While the technology to scale out data storage, query and processing has matured significantly, approaches to integrate systems and their underlying data consistently under-perform expectations. Even once data has been aggregated, the customer still will be confronted with the challenge of sense-making for rapid decisions. To address this issue, SAIC proposes a semantic data fabric to integrate information across Army mission systems.

The company's approach develops a semantic framework—a suite of ontology modules—and implements novel semantic technologies and platforms to generate a common operating environment that improves information sharing, computationally assisted decision making and enhanced analysis. Implementing networks based on this architecture overcomes differences of syntax and semantics to take advantage of automation, augmentation and artificial intelligence capabilities that increases process efficiency and artifact quality. This semantic layer, leveraging knowledge of data relationships between systems, enables streamlined data access to previously disparate data silos.

To maximize interoperability and extensibility, SAIC proposes the use of a tiered ontology architecture where the top-level organizes the content of the middle and lower (i.e., application) levels. For example, Basic Formal Ontology (BFO), described by the developing ISO/IEC 21838-2 standard, presents a concise top-level ontology (TLO) designed to support the integration of more specific ontologies that extend from it. In addition to differentiating between TLOs and mid-level ontologies (MLOs), the company also considers their function—i.e., reference ontologies or application ontologies. This solution takes a knowledge modeling approach, aligned with standard Army-focused data models, to improve knowledge integration for the common operating environment starting with an understanding of the meaning of information (i.e., semantics) from a warfighters' perspective then moving to an integration of the physical data. In short, SAIC proposes linking a top-down with bottom-up approach.

The company recognizes that military systems require strict security controls and that integration of systems and data representations can significantly affect data classification and governance strategies. Additional components will be developed to provide for cross-domain solutions. In its presentation, SAIC will lay out this strategy and describe its benefits with supporting graphics and a demonstration with its partner, iNovex, using their ontology development and management platform, Mobi.

BIO: Col. Forrest Hare, USAF (Ret.) currently serves as a solution architect for SAIC. While assigned to Headquarters Air Force, Col. Hare was chosen to be on the Chief's Cyberspace Task Force to develop the vision for the service's operations in its newest warfighting domain. After this assignment, he served on the Secretary of Defense staff and helped draft the U.S. Defense Department Cyber Security policy. In his current position at SAIC, he is developing an ontology-based knowledge model for defense intelligence to improve the integration of cyber threat intelligence with traditional intelligence information.

Col. Bill Mandrick, USA (Ret.), is a senior ontologist with more than 18 years of experience converting natural language descriptions of domain knowledge into graph-theoretic (computable) ontologies with first-order logic. As a Fellow at the National Center for Ontological Research (NCOR), he collaborates with the world's leading experts in ontology development. Col. Mandrick also has more than 30 years of experience in the U.S. Army both on active duty and in the Reserve. In that role, he has planned and led numerous combat operations, produced critical intelligence and participated in highly complex, data-driven targeting processes.

iNovex, brings extensive experience working in integrated project teams to develop secure, ontology-based data fabric solutions across the Intelligence Community, the U.S. Defense Department and *Fortune* 500 customers.

Common Data Fabric with Cross-Domain Capability

Frank Mitchell, Chief Data Engineer, HPE • frank.r.mitchell@hpe.com

ABSTRACT

HPE enables a common data fabric with cross-domain capability, which accelerates data discovery for analytics in tagging to secure sensitive data, inferring hidden relationships, to drive smarter insights. This unifies data management across distributed resources to allow consistency and control of data mobility, security, visibility, protection and access. The data fabric represents a scalable platform to optimize data access based on infrastructure capabilities and application service-level requirements. As a result, users can seamlessly move exabytes of data across edge, on-premises and to cloud deployments.

To facilitate the transfer of data between differing security domains in a secure, consolidated, enterprise environment, HPE can integrate with accredited or existing cross-domain solutions. Integrated with Hitachi (HVF) Lumada Data Catalog (LDC), enabling automated data discovery, compliance and the ability to take action on data through artificial intelligence, machine learning, ratings and reviews and tribal knowledge to deliver an AI-driven (data fingerprinting) data catalog of trusted, mission-critical information. As a result, end users spend less time searching for data and more time using it to derive value while complying with data governance mandates, standards and directives.

Focused on high-volume applications that generate millions of files daily for preregistration of ingested structured and unstructured datasets, HPE enables validation and management of metadata for different roles, including data analysts, stewards, governance and stakeholders. This ensures that data is fully owned and cared for by appropriate end users and decision makers and that the effective usage of data from the outset ensures and enhances trust for facilitating the transfer of data between differing security domains in a secure, supported and consolidated enterprise environment within an approved cross-domain environment. Metadata versioning allows capture and display of technical metadata provided by the ingesting application, including file location, file size, file format, time of ingestion, partition, etc. This can catch unresolved schema evolution to produce discrepancy reports between reported and inferred schema and/or ontologies. That data is then made available to end users in a robust self-service visualization that features complex custom properties presented simply and cohesively to enable end users to quickly find and utilize the data.

Users derive new insights from all data by providing a platform to analyze, store, manage, distribute and process data at scale. The company's experience and solutions enable products to speed up the transmission of data across military networks from vehicle-mountable nodes that will collect data from the battlefield and semi-autonomously process it for Army commanders.

HPE has experience in data coming in from sensors around the world, whether mounted or dismounted, that is communicated faster than current command and control stations can process. HPE's solution will support automated collection, exploitation, processing and analysis toward correlation and fusion of multiple data types and formats across connected and disconnected environments. It can support ease of

integration with multisource sensors through existing and adaptable networks to enhance targetable data-to-fires networks while providing analytics, insights and capabilities for multidiscipline intelligence support to targeting and situational awareness and understanding for mission command.

BIO: Frank Mitchell is a Hewlett Packard Enterprise (HPE) chief data engineer and technologist. He is an experienced, energetic and action-oriented executive with national and international expertise in advanced and next-generation technologies, including data platform solutions, cloud computing, data science and engineering, mobile and sensor technologies. His roles in HPE include solution and product development and integration engineering and management of advanced and next-generation technology capabilities.

OFFENSIVE CYBERSPACE OPERATIONS (OCO) ACCESS EXTENSION CAPABILITIES

Mobile Vulneralytics Platform

Michael Chen, Technical Director, CACI • michael.chen@caci.com

ABSTRACT

Performing vulnerability research of mobile devices, operating systems, protocols and applications can be a time-consuming, often manual process. A security researcher has various tools available that can help automate portions of this analysis process. However, it is often up to the vulnerability researcher to develop a workflow that utilizes these disparate tools.

CACI's Mobile Vulneralytics (Vulnerability Analytics) Platform seeks to provide vulnerability researchers with a workflow of fundamental tools that assist in vulnerability research. Additional methods and tools can be integrated into the workflow over time, allowing the security researcher to speed up future analysis. Finally, workflows can be created and run autonomously against an array of mobile devices (different makes, models, operating systems and apps), enabling large-scale discovery of vulnerabilities across various device types and operating systems.

CACI's Mobile Vulneralytics Platform enables dynamic and static analysis of mobile devices in four main areas: client, server, traffic and open source. Client analysis focuses on the mobile application, how it is used and how it interacts with the operating system and filesystem. Server analysis involves investigating all of the servers with which the mobile application communicates. Traffic analysis evaluates the security of transport and application protocols and identifies potential information leakage. Finally, open source analysis involves gathering various information about the company/developer, usage statistics and any security articles related to the mobile application.

The Vulneralytics Platform has a web interface that allows a user to operate a mobile device while observing the resulting device, network and application behavior. A live, interactive session with a physical mobile device enables the security researcher to perform clicks and drags through the web browser that normally would be done through taps and swipes on the actual device. User activities also can be launched through this interface to perform automated testing or exploit discovery. Inspired by Wireshark's real-time interface for capture and analysis of network packets, the Vulneralytics Platform provides real-time stream of the state of the mobile device, network and application.

After a test or exercise is complete, a post-analysis is conducted on the resulting data. The Vulneralytics Platform is designed to be extensible, allowing the security researcher to create modules that initiate user- or system-level interactions with the mobile device as well as perform analysis of resulting characteristics collected from the device, network or application. This provides the researcher with a structured and repeatable workflow that is extendable and scalable, ultimately allowing for automated discovery of mobile exploits.

BIO: Michael Chen is a technical director of information assurance research at CACI. He has a background in software engineering, networking and information security. He has 20 years of experience working in technical areas such as network reconnaissance, anonymous Internet communications, network and application security analysis, red teaming, fingerprinting/classification, security automation, micro services, proxies, web and mobile apps, cloud, docker, virtualization and agile development. He received his Master of Science degree in electrical engineering from Stevens Institute of Technology in 2006 and his Bachelor of Science degree in computer science from Rutgers University in 2000.

SECURITY ORCHESTRATION, AUTOMATION AND RESPONSE (SOAR)

Cortex XSOAR and Big Data Platform

Steve Wagner, Vice President, Enlighten IT Consulting LLC •
swagner@eitccorp.com

ABSTRACT

Enlighten proposes the deployment of Palo Alto's Cortex XSOAR integrated with the ARCYBER Gabriel Nimbus Big Data Platform as a SOAR solution. As leaders in the industry, Enlighten and Palo Alto will integrate disparate tools and technologies into a cohesive system capable of quick response that enables technicians with different levels of training to safely and quickly respond to events on network. In addition, XSOAR allows products never designed to integrate to be an integrated solution.

Cortex XSOAR has proven to have industry leading capabilities in U.S. Defense Department applications with flexible and intuitive functionality. Cortex XSOAR provides a configurable and modifiable solution through its exceptionally intuitive playbook editor. This graphical user interface tool allows full construction, editing and maintenance of automated playbooks by utilizing drag-and-drop components and intuitive forms.

Also, Cortex XSOAR ships with an extensive library of common playbooks that can be used as templates. XSOAR playbooks can leverage other sub-playbooks as building components to enrich data further. This easy-to-use interface increases the speed of adoption and allows operators to hit the ground running.

Cortex XSOAR provides incident management and incident response through a robust case management system with a single interface. Through this single user interface, all operators can capture steps taken within a given case and actions taken by each XSOAR playbook. When analysts need to interact with a case, they can log into XSOAR and work alongside the playbook to resolve an incident. Analysts are notified when a playbook requires their intervention to ensure a timely response is provided. XSOAR cases capture all the automated and manual tasks in a single auditable repository. Chat-Ops complements the Cortex XSOAR case management functionality. The tool allows analysts to communicate with other team members in real time, allowing all communication to be captured in the XSOAR case for future audit purposes.

Cortex XSOAR is different from other products through its handling of unstructured incidents. In cases where the logic in a playbook has been completed and an analyst needs to do more work, XSOAR provides a War Room for analysts to execute additional commands, annotate the case with pertinent details and take other actions necessary to bring the incident to resolution. The War Room provides a complete chronology of each case and allows analysts to initiate any playbook, task or script live with all outputs captured for posterity.

BIO: During the past 11 years, Enlighten IT Consulting LLC, a nontraditional defense contractor, has been providing the U.S. Defense Department with similar security orchestration, automated and response (SOAR) capabilities in support of U.S Army Program Executive Office for Enterprise Information Systems, Army Cyber Command, Air Force Cyber, Marine Corps Cyber and U.S. Cyber Command networks.

Ground Resilient Infrastructure Model (GRIM)

Ken Zhang, Solution Architect, Cyber Systems, L3Harris Technologies Inc. •
leqiken.zhang@l3harris.com

ABSTRACT

Modern combat vehicles, even more so than their civilian counterparts, are effectively mobile processing networks. A typical vehicle contains more than 100 microprocessors, globally sourced with each processor running millions of lines of software code with uncertain provenance and uneven quality. Many adversaries wield remarkably effective hacking skills and, by its nature, the advantage in cybersecurity goes to the attacker because a defender must defend all his assets while the attacker can choose any point of attack.

To address this challenge, L3Harris recently developed a novel model-based system engineering (MBSE) approach to model and simulate the integration of disparate components that enables a full system assessment of the cyber risk in terms of vehicle availability. From here, we can evaluate factors that might increase that availability under continuous cyber attack.

The MBSE work uses L3Harris' executable SysML model called the Ground Resilient Infrastructure Model, or GRIM. This model has tailorable parameters that include the intensity of the attack, the vulnerability of the vehicle and the speed with which remediation is applied through the support infrastructure. Using this model, L3Harris explores the impact of a tiered cybersecurity support infrastructure and a resilient vehicle design on the availability of a combat vehicle fleet.

To evaluate how resilient tiered infrastructure and vehicle design will improve operational availability, GRIM provides a construct to model the relationships between the parameters of a tiered cyber support infrastructure and vehicle availability. A tiered cybersecurity infrastructure comprises a distributed network of security service nodes that provides cybersecurity maintenance services to vehicles and equipment. Such infrastructure consists of a centralized security operations center, distributed operations centers and security service centers.

The model is translated to a simulation to characterize vehicle availability based on threat environment and the tiered cybersecurity infrastructure configurations. The threat environment is characterized by the frequency of vulnerability exploits and probability of a successful cyber attack against the fleet. The cybersecurity infrastructure is characterized by how often vulnerabilities are identified, time required to develop mitigation and dispatch it through the network, time required for a vehicle or equipment to be serviced, time required to detect an attack and number of nodes in the infrastructure. The simulation results show that even with a relatively small tiered cybersecurity infrastructure, the availability of the fleet in presence of cyber attacks can be improved by 57 percent compared to singular traditional service infrastructure based on standard vehicle configuration. For a resilient vehicle configuration where it facilitates a degraded mode of operation, the improvement on availability is as much as 110 percent.

BIO: Leqi (Ken) Zhang has 15 years of systems engineering experience in the defense industry. His experience includes the design and development of NSA Type-1 High Assurance End Cryptographic Unit (ECU) equipment for tactical and satellite communications, key management infrastructure, RF communication systems, biometric systems and ground systems. Zhang's current role is architect in the L3Harris cyber division. He has been leading numerous cybersecurity design and analysis for multiple U.S. Defense Department tactical SATCOM and extensive expertise and excels at model-based engineering. Zhang has a Master of Engineering in systems engineering from Cornell Univeresity. He holds a Master of Science in computer engineering, Drexel University, and a Bachelor of Science in computer system and electrical engineering from Rensselaer Polytechnic Institute.

The Scalable, Innovative and Flexibilty of SOAR

Amanda Frame, Marketing Manager, Merlin Cyber • aframe@merlin-intl.com

ABSTRACT

Swimlane is a scalable and innovative leader in security orchestration, automation and response (SOAR). The flexible solution delivers powerful consolidated analytics, real-time dashboards and reporting from across the security infrastructure, maximizing the incident response capabilities of overburdened and understaffed security operations. As a result, organizations are now able to replace slow and manual activities with machine-speed decision making and remediation, empower technicians with different skill levels to respond to incidents and focus on higher priority breaches safely, and quickly integrate disparate systems to get the security automation needed to keep up with their advisories.

The scalable, innovative and flexible security solution offers a broad array of features aimed at helping organizations address both simple and complex security activities, including but not limited to the following:

- With Swimlane's API first framework, organizations now have a standardized way of accessing data that is independent of the UI or the application's own functionality. As requirements evolve, every component in a SOAR solution should be accessible through an API to enable the organization to add new capabilities as discrete plug-ins quickly. This also allows security and DevOps engineers to create integrations with homegrown or third-party apps without forcing use of the SOAR platform's UI. Some SOAR solutions don't have a full API architecture, making functionality difficult to enhance or modify. Swimlane has more than 250 out-of-the-box integrations supporting 5,000 unique actions.

Key takeaway: Every component and functionality of the SOAR solution should be accessible through an API and the platform needs to be extensible so it can accommodate growth by adding the new features and capabilities necessary to adapt to new threats and incident response processes.

- Dynamic case management consolidates all relevant event data into a single view where analysts can review, act on and remediate an incident easily within the case record. Swimlane tracks all security tasks and actions throughout the incident response process and provides an intuitive, flexible interface to easily manage ongoing cases. Within any case record, the analyst can interact with all relevant data and critical investigation and response components related to each specific incident. Analysts can execute incident response actions specific to each scenario from within the individual record.

Key takeaway: Dynamic case management empowers organizations to define and develop their security processes procedures, which speeds up investigations, enforces compliance, remediates more security alerts in a more timely manner and elevates staff of all levels to take on more complex cases.

- With multiheaded playbooks and workflows, Swimlane manages and automates the response to security alerts and incidents with automated workflow processes. The capability drives machine-speed SOC automation by executing predefined and easily configured playbooks and workflows that

formalize best practice incident response processes for immediate threat management. This ensures the enterprise will follow consistent policy and procedures that can be quickly and easily customized to fit current practices processes and technologies.

Key takeaway: Because organizations can automate routine tasks and procedures, they can now focus on critical attacks that are a greater threat to the mission.

BIO: Merlin is the premier cybersecurity platform with a one-of-a-kind business model that leverages security technologies, trusted relationships and capital to develop and deliver groundbreaking security solutions that help the federal government minimize security risk and simplify IT operations. In addition to selectively representing reputable cybersecurity brands, Merlin invests in visionary, emerging technologies and brings everything together into its lab where cybersecurity engineers integrate, test and deliver innovative security solutions. With these integrated solutions, Merlin helps federal civilian and defense customers save time, money and other resources while empowering them to more simply and effectively secure their systems, data and users no matter how the network, security threats and regulatory compliance requirements evolve.

Accelerating DCO Response by Enriching SOAR Data for AI/ML Workflow Automation

Duncan Stewart, Director, Strategic Development, Axellio •
duncan.stewart@axellio.com

ABSTRACT

Modern cyber adversaries use sophisticated multistage and multihost attack techniques. Because of the current limitations of intrusion detection and forensic analysis tools, reconstructing attack scenarios is extremely challenging and results in delayed anomaly detection, threat identification and resolutions. The volume, velocity and variety of attacks creates thousands of SIEM or SOAR events that leave frontline defensive cyber operators overwhelmed and unable to triage priorities among major threats, minor threats and false alarms effectively and efficiently. To combat complex cyber attacks, a new approach is needed that combines event data with detailed attack data then employs AI/ML algorithms to improve threat analysis and prioritization.

One solution uses an intelligent threat analysis framework that prioritizes the most severe threats while streamlining root cause analysis. Combining SIEM and SOAR event data with detailed attack data derived from actual network packets will increase available threat information and situational awareness while improving productivity of the limited analyst resources. It combines expert insight with AI/ML guidance to automate the manual task of alarm prioritization and response. This simplifies and accelerates access to the incident data by preselecting packets relevant to the reported alarm. It also automates the initial packet analysis rather than leaving this entirely to the analyst expertise—weeding out false positives and annotating the presented packet data, highlighting anomalies and identifying additional threats. This approach requires powerful hardware platforms that can ingest, store and simultaneously process vast amounts of network data. Axellio is employing its revolutionary edge computing systems to drive advanced AI/ML cybersecurity solutions.

Given the vast amount of data and constantly shifting threat vectors, AI and ML models are perfect to accelerate the learning process, avoiding lengthy manual re-programming of the analysis logic as typical in today's applications. This results in reduced time-to-threat mitigation by increasing the available attack information and situational awareness while reducing the time spent on false positive alerts. This improves the team's productivity, allowing it to focus on higher priorities and reduce case backlog.

BIO: Lt. Col. Duncan Stewart, USAF (Ret.), is the director of strategic development at Axellio Inc. He is responsible for exploring military and intelligence applications of the company's commercial innovations in edge computing. Col. Stewart served for 24 years in the active duty and reserve Air Force. During his career, he served as an acquisition program manager for advanced

avionics, sortie generation officer for fighter and tactical aircraft and senior logistics officer at the COCOM level. He created the Strategic Innovation course at the U.S. Air Force Academy and supported several major science and technology initiatives. He is the former CEO of the Colorado Springs Technology Incubator and CEO of Quadric Biomedical. He currently serves as the chairman of the board of ConcealFab, the technological leader in telecommunication mounting infrastructure. Col. Stewart earned a Bachelor of Science in management from the U.S. Air Force Academy, a Master of Science in aerospace management from Embry-Riddle and an MBA from Notre Dame University. He is a patented inventor of several electromechanical and biomedical devices and maintains a TS clearance.

COUNTERING POLYMORPHIC MALWARE

Rendering Polymorphic Malware Ineffective Through Behavior Computation

Richard Linger, Chief Technology Officer, AffirmLogic •
richard.linger@affirmlogic.com

ABSTRACT

It is well understood that syntactic, signature-based scanning for malicious content is not effective against code morphing by adversaries that can easily render malware undetectable by existing signatures. The reason is simple. Signature generation can never keep pace with the essentially infinite number of ways a malicious program can be syntactically modified. Not only does polymorphism hide malware, it also increases the workload necessary to counter it. The asymmetric advantage is with the adversaries. This is a major problem for defenders seeking to protect Army networks.

But while this problem has seemed insurmountable in the past, it will not be so in the future. Polymorphic malware can be rendered ineffective by the new technology of software behavior computation.

To mount successful attacks, adversaries must ensure that the intended malicious functionality of their code remains intact no matter how the code is morphed into new syntactic forms to avoid detection. The mathematics-based technology of behavior computation eliminates syntactic morphing to reveal malicious functionality, no matter how the morphing was carried out. There are an infinite number of ways to morph the syntactic structure of a malicious program, but there is only one underlying functionality that an adversary must preserve. Behavior computation reveals that functionality. No matter what syntactic variations are created, they all map into one canonical form where malicious operations have nowhere to hide.

Behavior computation is an automatic process carried out at machine speeds with no human intervention required. The technology automates the process of reverse engineering of malware to reveal its true canonical form and malicious functionality right down to the instruction addresses where it occurs.

This automation can substantially increase the effectiveness of defenders because behavior computation significantly reduces the work factor required to analyze malware. An agency in the Intelligence Community documented a 20 times reduction in time and level of effort required to reverse engineer malware to understand its functional effects.

Behavior computation technology originated in research carried out at Carnegie Mellon University was elaborated into a prototype system at the Department of Energy Oak Ridge National Laboratory and has now been transformed into a commercial product by AffirmLogic Corporation. This capability can be demonstrated to the Army to illustrate how polymorphism can be taken off the table as a weapon for adversaries.

BIO: Richard Linger is currently the chief technology officer at AffirmLogic leading the platform development of a cybersecurity solution for automated reverse engineering of software for rapid analysis and mitigation of cyber threats using behavior computation technology.

He served as a senior research and development staff member in the cyberspace sciences and information intelligence research group at Oak Ridge National Laboratory, where he led R&D in behavior computation for verification of smart grid software functionality and security.

He previously served as manager of the CERT survivable systems engineering group at the Software Engineering Institute, Carnegie Mellon University. He directed research and development on function extraction (FX) technology for software behavior computation, with a focus on applications to test and evaluate software and to analyze malware. He also served as a member of the faculty at the CMU Heinz School of Public Policy and Management. At IBM, Linger partnered with Harlan Mills, IBM Fellow, to create cleanroom software engineering technology for development of ultra-reliable software systems, including box-structure specification, function-theoretic design and correctness verification and statistical usage-based testing for certification of software fitness for use. He has extensive experience in project management; system specification, architecture, design, verification, testing and certification; software re-engineering and reverse engineering; and technology transfer and education. He has published three software engineering textbooks, 12 book chapters and over 60 papers and journal articles. He is a member of the AIAA and ACM and a senior member of the IEEE.

Big Data Platform/Cyber Indicator Threat Exchange

Steve Wagner, Vice President, Enlighten IT Consulting LLC •
swagner@eitccorp.com

ABSTRACT

Enlighten recommends the government off-the-shelf Big Data Platform (BDP) to allow U.S. Defense Department cyber teams to work closely with teams from other U.S. government agencies and the Intelligence Community (IC) to analyze near real-time threats to the government's information systems and networks. Pairing the Army malware teams with the broader U.S. Defense Department and IC malware teams and jointly collaborating on malware analysis will reduce duplicative work efforts, while reducing the time it takes to identify, isolate and extract the malware.

Utilizing the BDP as the underlying analysis platform deployed on the NIPRNet, SIPRNet and Joint Worldwide Intelligence Communication System connected via cross-domain farm with distributed query and distributed analytic capabilities will enable forensic and malware analysis teams to hunt for malware by running analytics across the U.S. Defense Department's collected data. The endpoint data already in the BDP can point to potential malware by using analytics that look for time-based (periodicity) events, clustering of alerts and other advanced algorithmic functions.

As part of this malware solution, Enlighten, in conjunction with the U.S. Cyber Command and Army Cyber Command, has built a tool called the Cyber Indicator Threat Exchange (CITE) for collaboration around indicators of compromise (IoCs). Just like the BDP, CITE is a government off-the-shelf capability currently funded by the U.S. Cyber Command and the Army.

Enlighten recommends the government off-the-shelf BDP and CITE as two capabilities that utilize the tools to collect, analyze and collaborate around malware analysis and the hunting of malware in the U.S. Defense Department networks. Additional BDP non-commercial tools include distributed query, distributed analytic and cross-domain capabilities that are needed to support the forensic and malware analysis mission.

Enlighten has provided malware analysis on more than 100 different data samples. WHIDDLER and UCATS are two examples.

- WHIDDLER is a GOT-developed application that implements a Bayesian filter to analyze portable executable files. The application performs rapid, accurate risk assessment of files by determining the probability of malicious activity through static, statistical analysis. It provides advanced threat detection capability, high-performance, scalable, static analysis of file characteristics with no execution, zero-day exploit detection and is multi-platform (Windows and Linux).

- UCATS, the Unified Code Analysis and Triage System, is a comprehensive solution for malware triage automating dynamic and static analysis of files, URLs, memory dumps and network traffic. UCATS identifies both known and unknown malware.

BIO: Over the past seven years, Enlighten IT Consulting LLC, a nontraditional defense contractor, has been providing the U..S. Defense Department with similar forensic and malware analysis capabilities in support of U.S. Army Program Executive Office for Enterprise Information Systems, Army Cyber Command, Air Force Cyber, Marine Corps Cyber and U.S. Cyber Command networks.

Countering Polymorphic Malware

Kristopher Willis, Senior Cybersecurity Researcher, CACI •
kristopher.willis@caci.com

ABSTRACT

Creating malware today is an extensive task where developers need to create multiple techniques to effectively keep malware undetectable and relevant. Polymorphic malware is not a new concept but is effective at subverting many anti-malware systems. Anti-malware continues to utilize archaic approaches such as hash checking and sandboxing that have undeniable evasion techniques.

CACI has extensive knowledge in command and control, malware design, implementation and analysis. Its solution to the detection of polymorphic software is to perform real-time monitoring of the binary control-flow. To achieve this, each executable binary on the system will go through an extensive ground-truth analysis using automated program analysis techniques to create an extensive baseline control flow.

When the user selects an application, the software will monitor that application using uniquely developed real-time control-flow monitoring (CFM). Utilizing CACI's extensive background in artificial intelligence (AI), the CFM software will compare the baseline control flow baseline with its current executable state. In the event the CFM detects a variation in the control flow, the monitoring service will perform an interrupt, closing the application and moving it to quarantine.

CACI's CFM software also makes it easier for enterprise-level customers. It works as a server/agent configuration. An administrator can initiate and perform the initial control-flow baseline that then can be sent to a secure centralized server. The CFM agents can retrieve a control-flow baseline of all applications on the client system and prevent applications that do not have the baseline as a reference from running.

This solution requires more compute resources and elevated privileges for monitoring than a traditional personal security product. The user can realistically expect the CFM to utilize up to half of the CPU compute ability, utilizing between three and four CPU cores per open application. With this in mind, the administrator can whitelist known safe applications to save compute resources. As this solution is further developed, CACI is focusing on several objectives, including limiting the need for elevated privileges, decreasing the amount of compute resource needed, monitoring for vulnerabilities within applications and integrating further with large-scale virtual environments with agentless capabilities.

CACI's CFM solution takes a proactive measure to prevent polymorphic capabilities within malware to execute on a secure system.

BIO: Kristopher Willis is a senior cybersecurity researcher currently located within the Washington D.C. metropolitan area. At CACI, he leads several strategic research and development programs for the company. Willis holds both a BS and MS from the University of South Florida

where he was also the first two-term president of Whitehatters Computer Security Club (WCSC), a professional capture-the-flag (CTF) organization. Willis has gone on to compete in CTF with other professional teams, including BORG and NASA Rejects, competing at the highest levels, including the DEFCON-CTF. His standout professional role was as a technical lead of AFRL Black Badge program, which facilitated DARPA's Cyber Grand Challenge.

How To Use Cyber AI To Combat Polymorphic Malware Attacks

Amanda Frame, Marketing Manager, Merlin Cyber • aframe@merlin-intl.com

ABSTRACT

The threat from AI-enabled malware is imminent. Forrester recently released a study finding that 88 percent of cybersecurity decision makers believe that it is inevitable for AI-driven cyber attacks to go mainstream.

Polymorphic malware that employs obfuscating algorithms to adapt and change its identifiable characteristics will reach a level of adaptability that renders it undetectable to antivirus software based in rules and signatures.

Traditional security controls are already struggling to detect attacks that have never been seen before in the wild—be it malware without known signatures, new command and control domains or spear-phishing emails with automated domain generation. Traditional tools will not be able to cope with future attacks as AI-driven attacks becomes the norm and easier to realize than ever before.

With its real-time visibility, granular detail, predictive uses and intelligent presentation of information, Darktrace's AI-driven cyber defense platform leverages unsupervised machine learning to detect never-before-seen attacks. Because its continuous detection algorithms rely on an ever-evolving sense of normal, it is able to approach defense in a protocol-agnostic capacity, identifying any and all unusual activity regardless of the nature of the attack. This makes Darktrace's Cyber AI platform an ideal solution when looking to combat polymorphic malware attacks, which easily evade traditional legacy defenses.

BIO: Merlin is the premier cybersecurity platform with a one-of-a-kind business model that leverages security technologies, trusted relationships and capital to develop and deliver groundbreaking security solutions that help the federal government minimize security risk and simplify IT operations. In addition to selectively representing reputable cybersecurity brands, Merlin invests in visionary, emerging technologies and brings everything together into its lab where cybersecurity engineers integrate, test and deliver innovative security solutions. With these integrated solutions, Merlin helps federal civilian and defense customers save time, money and other resources while empowering them to more simply and effectively secure their systems, data and users no matter how the network, security threats and regulatory compliance requirements evolve.

MACHINE LEARNING

Big Data Platform/Cyber Learning Engine

Steve Wagner, Enlighten IT Consulting LLC • swagner@eitccorp.com

ABSTRACT

Enlighten will utilize the existing implementation of its Big Data Platform (BDP) as the data repository for the application of a machine learning engine (MLE) to support identifying anomalous behavior in encrypted data streams.

The BDP is a government off-the-shelf technology originally developed by Enlighten under contract with the Defense Information Systems Agency (DISA) and has evolved through joint collaboration, research and development with U.S. Cyber Command, U.S. Army Cyber, U.S. Air Force Cyber and U.S. Marine Corps Cyber that have production implementations of the BDP with live network traffic for the training of machine learning models. The current BDP cyber data repositories range from multi-terabyte to multi-petabyte implementations.

One of the augmenting technologies is the Cyber Learning Engine (CLE), which enables machine learning models to be developed, tested and deployed against the BDP data repositories. These CLE models are being researched to predict new indicators of compromise that then can be validated and acted on by the U.S. Defense Department analyst community.

Enlighten's CLE is based on a deep learning (DL) concept of using artificial neural networks to process data in layers. As more data is entered, the model's conclusions about bad actors in the network become more accurate over time. For example, under testing, CLE progressed from a 75 percent probability of correctly identifying malicious content up to 95 percent accuracy. Even more significant, it identified signs of a network breach, also known as indicators of compromise, not previously reported in any open or non-open source data and later identified as threats. DL models that can search through terabytes of data and reach accurate conclusions without human intervention are essential for future success.

Additionally, for Enlighten's proposed solution, data can be utilized to train new machine learning models on NIPRNet, then the output of those models would be passed to SIPRNet via the WOLFDOOR cross domain solution (CDS). On SIPRNet, the NIPRNet machine learning results can be correlated with additional threat intelligence data and the outputs of the SIPRNet models can then be passed to the Joint Worldwide Intelligence Communication System (JWICS). On JWICS, additional machine learning correlation can be done. At each tier, the models will enable the augmentation of the analyst's work and the identification of previously unidentified threats.

BIO: Over the past four years, Enlighten IT Consulting LLC, a nontraditional defense contractor, has been providing the Defense Department with similar metadata extraction capabilities in support of U.S. Army Program Executive Office for Enterprise Information Systems, Army Cyber Command, Air Force Cyber, Marine Corps Cyber and U.S. Cyber Command networks.

Detecting Anomalous Network Behavior Through Encrypted Traffic Analysis

Bryan Ellis, Manager, Army Business Development, Juniper Networks •
bellis@juniper.net

ABSTRACT

Today, 70 percent to 80 percent of enterprise inbound network traffic is encrypted and encrypted traffic attacks have increased by 76 percent (Dark Reading, 2019). Currently, more than 40 percent of attacks use encryption to evade detection (Ponemon Institute, 2016). Stated another way, the bad guys are using their own encryption to mask attacks on networks.

One way to detect this malicious activity is to decrypt traffic before routing it through IPS systems; however, that introduces new problems such as vastly increased latency and corrupted applications.

Juniper Networks has developed a means of encrypted traffic analysis (ETA) that leverages AI and machine learning to identify encrypted threats without the need to break the encryption. ETA takes relevant data extracted by the SRX series firewall combined with behavior analysis provided by the Juniper Advanced Threat Protection (ATP) Cloud to provide insight and visibility into the underlying traffic. Based on metadata analysis via machine learning in the ATP Cloud, connections are classified as malicious or benign, identifying the hallmarks of botnet and malware command and control traffic. This is accomplished without the need to decrypt traffic and requires no new hardware, sensors or collectors.

The solution is scalable with network size and enables greater network visibility, confidence and the ability to respond more quickly via automated remediation. This is accomplished via the SRX firewall that extracts information from the initial transport layer security handshake. Questionable certificates are sent to the ATP Cloud, which then queries the certificate against certificates used for known malicious activity and sends them back to the SRX for blocking. File transfer protocol events are then correlated with user and device information and added to the infected host feed. This information is managed via a tailorable screen that provides analysis and can be configured to meet the user's relevant security needs.

In summary, what sets the Juniper Networks Encrypted Traffic Analysis solution apart from other solutions is that it is relatively inexpensive. An SRX firewall and Juniper ATP Cloud license is open standard/non-proprietary, operates in a multivendor environment and doesn't require additional sensors or collectors.

Juniper's Encrypted Traffic Analysis solution is a subset of a larger, comprehensive connected security portfolio that is used extensively in international commercial banking, health care and the U.S. federal government.

BIO: Bryan Ellis spent 28 years as an Army Signal officer prior to retirement in 2008. He commanded an airborne signal battalion and brigade. His final assignment was as the director of the Capabilities Development Integration Directorate at Fort Gordon. Since then, he has worked in industry with both General Dynamics and Juniper Networks.

Transforming Open Source Intelligence Using AI Machine Learning

Himanshu Garg, Lead Scientist, Perspecta • himanshu.garg@uspsector.com

ABSTRACT

Analysts struggle with identifying anomalies in encrypted data because of the volume of open source intelligence (OSINT). To address this, Perspecta has developed an interactive, artificial intelligence/machine learning platform that extracts and highlights operationally relevant information from news and social media channels.

Designed for the needs of the Intelligence Community, this solution uses advanced natural language processing algorithms to track emerging patterns and trends in near real time. Analysts get an integrated dashboard that shows all open source intelligence channels. They can drill down to original OSINT information for more in-depth analysis, more readily reach conclusions about tone and intent and get presented potential actions to take.

The highly co-related nature of information today requires a methodology and technology to stay ahead of malicious activity, and Perspecta's investment in this artificial intelligence/machine-learning platform accomplishes that.

BIO: Himanshu Garg is Perspecta's product manager and chief machine learning scientist for open source intelligence. He focuses on the architecture of natural language process solutions powered by artificial intelligence. His cumulative expertise comes from more than 25 years in open source intelligence, business intelligence and data engineering.

Network Traffic Analysis Through Machine Learning

Nancy Peaslee, Project Manager, Graham Technologies •
npeaslee@graham-tech.net

ABSTRACT

Malicious actors subject government and U.S. Defense Department networks to a barrage of encrypted traffic. How can malicious traffic be filtered out and isolated to be able to protect networks and systems from these threats? While intrusion detection systems and endpoint protection provide point information relating to this traffic through signature or statistical anomaly-based detection, further analysis is warranted.

What if it was possible to profile traffic for patterns of misuse to provide additional security? And what if large amounts of this data could be collected in aggregate to further define more potential threats to government networks? There are limitations of point data and how to look at trends over time can be demonstrated. In addition, further analysis of this information helps determine whether or not the traffic may be a threat.

This can be done without costly and time-consuming decryption attempts. Utilizing cloud-based analytics and machine learning, the Army's cybersecurity capabilities can be enhanced by collecting and analyzing this data. By fingerprinting encrypted traffic through machine learning, packet size, packet direction, sequence of packets and track temporal changes can be examined. Pattern recognition over time can provide valuable data.

By collecting this data, a baseline can be established for further analysis and observation. Tools such as Splunk will allow for the porting as well as the collection and analysis of this data.

BIO: Nancy Peaslee, PMP, CISSP, is a project manager at Graham Technologies. Peaslee's prior experience includes 20 years as an IT contractor with roles ranging from web development to server management to project management to cybersecurity. She is currently evaluating cybersecurity tools utilizing data analytics in the cloud environment. She holds a Bachelor of Science in accounting, a Bachelor of Science in electrical engineering and an MBA.

Machine Learning to Detect Cyber Threats

Amanda Frame, Marketing Manager, Merlin Cyber • aframe@merlin-intl.com

ABSTRACT

When it comes to performing anomaly detection in any context—be it encrypted communications in cyber ecosystems, or digital interactions in the cyber-physical ecosystems that sustain critical national infrastructure—Darktrace AI leverages machine learning techniques in multiple crucial capacities.

By continuously monitoring all network traffic—with a granular view into more than 1,000 data features for every connected device and user—Darktrace AI utilizes unsupervised machine learning to develop an evolving understanding of what is normal for a cyber ecosystem. Darktrace AI draws on this evolving understanding of normal to perform anomaly detection and, with its autonomous response capabilities enabled, takes action against emerging threats with machine speed and precision.

The vast majority of threats can be detected by Darktrace based on the metadata level and derivative or inferred features that are available from encrypted packets. Darktrace is at the forefront of implementing novel techniques to analyze encrypted traffic and in fact considers encryption among the many attributes used to model behavior via the many mathematical models under the hood. An example of this is leveraging JA3 for anomaly detection and metadata such as details in SSL certificates.

In some cases, human threat analysts may want to decrypt traffic for forensic investigations, which Darktrace can support. In this context, Darktrace has the ability to do passive TLS decryption, ingest already decrypted streams of data from dedicated MITM devices, or integrate with logs produced by an established MITM device. In every case, the default setting is to only decrypt those traffic streams that might contribute to specific cyber anomalies (i.e., connections that are already rare or unusual for other purposes). This is designed to maintain privacy, maximize performance and prevent security teams from having to cope with huge amounts of whitelist/blacklist pre-configurations.

BIO: Merlin is the premier cybersecurity platform with a one-of-a-kind business model that leverages security technologies, trusted relationships and capital to develop and deliver groundbreaking security solutions that help the federal government minimize security risk and simplify IT operations. In addition to selectively representing reputable cybersecurity brands, Merlin invests in visionary, emerging technologies and brings everything together into its lab where cybersecurity engineers integrate, test and deliver innovative security solutions. With these integrated solutions, Merlin helps federal civilian and defense customers save time, money and other resources while empowering them to more simply and effectively secure their systems, data and users no matter how the network, security threats and regulatory compliance requirements evolve.

Detecting Adversary Activity in Encrypted Traffic

Aaron Rosenmund, Head of R&D Security, Pluralsight •
aaron-rosenmund@pluralsight.com

ABSTRACT

Adversaries are increasingly using SLL encrypted traffic over valid ports to deliver, communicate and control malware and C2 capabilities within the cyber domain. SSL decryption has a high cost of implementation monetarily, technically and in network speeds. More than that, it is not always possible to implement because of constraints of data collection on citizens by title.

Leaving the data encrypted avoids these issues but does not allow for traditional signature inspection of the payloads. In situations in which there is no direct control over the network, SSL decryption is simply not even an option. Machine learning and statistical analysis of various components of the traffic is in some cases more effective at identifying adversary activity than the inspection of the unencrypted payload itself. Further, it can be done with the open source tools already leveraged for defensive cyber operations by U.S. Defense Department cyber forces.

There are two focuses to detect of adversary activity in SSL encrypted traffic. The first is on the unencrypted portions of the sessions that provide information that can be leveraged to fingerprint malicious traffic. JA3 hashes, developed by Salesforce and now integrated into many open sources network analysis tools, gather the provided cipher suites by each side of the conversation prior to encryption to create a unique hash. These unique hashes correlate to the specific version of the binary running the application to generate the session and as such can be used to identify traffic from unknown or malicious binaries. In a similar fashion the certificate traffic is exchanged in clear text and though they are often valid certificates, they often include anomalous information for files such as location and company/organization.

The second focus is leveraging machine learning to identify anomalous activity from baseline in single metrics such as volume of traffic, number of packets, size or other attributes of the packets sent. Even more effective are multimetric correlations looking for coincidence of anomalous traffic metrics such as volume-to-timing based on the historical time-based activity of the organization. Time-based analysis is used to compare the timing of established connections or gaps between connections to discover computer-based connection activity versus human activity, defeating “jitter.” Lastly, methods for identifying anomalous activity of a specific member of a population by metric can identify computers that are communicating in SSL in a way that is outside of the norm of the peer computers performing the same function and numerous other detection capabilities with a higher positive detection rate than traditional signature inspection of unencrypted traffic.

This presentation would include quick explanations and examples of this capability that is already being leveraged in many advanced cyber defense operations.

BIO: As the head of research and content development for security at Pluralsight, national red team lead for Cyber Shield and NCOC of Discovery and Counter Infiltration NCOC for 601 AOC Cyber Mission Defense Team, Aaron Rosenmund is a committed cybersecurity leader who actively participates in the fight against the adversary while ensuring that the capability and knowledge to do so is passed on through innovative research, education and training.

RESILIENT NETWORK TRANSPORT CAPABILITIES

Leveraging Intelligent Multibonding Technology To Provide High Bandwidth and Highly Secure Tactical Communications

Alan Sosa, AI/AR/Quantum, Agile Defense Inc. • alan.sosa@agile-defense.com

ABSTRACT

The HALO communication platform provides high bandwidth, highly secured transmission channels for transmitting live data, video and audio in real-time anytime, anywhere by bonding multiple 3G/4G network, LTE, Wi-Fi, Internet and/or satellite communications services. HALO performs automatic and intelligent splitting of data and video over multiple communication channels (e.g., by using four or more sim cards), thus increasing the amount and security of data that is transmitted and received. The splitting process also creates highly secured tunnels that require an authorized user to capture all communication channels, decrypt the data and connect the parts. This is all done simultaneously and in real time.

The HALO platform main advantages are:

- Adaptive Data/Video: Adapts the video quality (bit rate and resolution) to the overall bandwidth available at any given moment in a dynamic way.
- Full redundancy that provides high reliability: Automatically detects failed communication channels and immediately transfers the information via an alternate channel available all in real-time, so there are no back-end breaks.
- High-level encryption: Generates a complete secured network tunnel that enables safe and encrypted data traffic.
- Increasing bandwidth: Allows multiplexing communication channels with unlimited quantity links, so that each channel increases the bandwidth available for use in the system. The HALO platform as a standalone device comes with four cellular modules that produce four independent communication channels that enable the use of various operators.
- Automatic energy management: Features an energy-management mechanism that turns the device off while it is not in use. This enables the device to work on battery over time in unmanned areas (for example, concealed posts).
- Low power consumption: Operates with extremely low power consumption, enabling it to be integrated in many different platforms without compromising operating times.
- Low heat index: The HALO platform has a very low heat index that makes it ideal for integration into existing platforms.
- Low latency: Algorithm manages to decrease latency up to 160 MS, that enables real-time operations beyond the visual line of sight.

Uses and capabilities of the HALO platform:

- connectivity solution for drones and robots, thus controlling the drone and/or robot in real time, with live video, audio and data transmission;
- connected communication channels both for uploading and downloading information and a LAN terminal that allows local data transfer capabilities that can connect to other devices and become a gateway for them;
- portable or stationary, users can receive the device as a stand-alone in case unit or as and OEM unit for integration into existing platforms;
- send and synchronize files at the highest encryption level at unprecedented speeds both for download and upload.

Transport Virtualization Ecosystem

Michael Young, Senior Director of Advanced Programs, Envistacom •
myoung@envistacom.com

ABSTRACT

There is an increasing reliance of military systems on information networks. Whether for command and control, logistics, targeting, reconnaissance or navigation, the demand for connectivity has grown exponentially. The reliance on these networks and the geographic unpredictability of military engagements, means that military commanders must be able to support connectivity, anywhere on earth, at a moment's notice. The pace at which technology is advancing on the battlefield is at an unparalleled rate never seen before. To maintain positive ground force control and resilient communications, battlefield commanders are required to have multiple disparate and often proprietary, communications equipment to ensure mission success.

Virtualization and more specifically the virtualization of communications waveforms and realizing the power of virtual modems (VMs) and how VMs may be utilized in cloud-based, headend and tactical edge (remote) environments allows the military to support multi-domain operations (MDO) and enables resilient network transports. Virtualization also enables related real-time, continuous processing applications, including interference mitigation, cryptography, machine learning, artificial intelligence and data analytics. Combined with innovative antenna systems a complete terminal solution would be able to provide an unparalleled multiband, multiwaveform and single-solution support for GEO, MEO and LEO applications.

A Transport Virtualization Ecosystem (TVE) architecture approach allows any qualified organization to deliver products into this ecosystem. This is accomplished using open-standard development techniques for both open standard and/or proprietary waveforms as software applications for implementation in VMs. This eliminates the challenges associated with bringing new waveforms to purpose-built modems and having to tailor the code for specific hardware. VMs provide a benefit to the government by streamlining the process to support growth in user demand as measured by additional modems and/or additional waveforms.

This approach to virtualization within the TVE is a departure from legacy software-defined modems (SDMs) and software-defined radios (SDRs). SDMs and SDRs are built with proprietary hardware and programmed using low-level languages such as Verilog or Very High-Speed Integrated Circuit Hardware Description Language, resulting in a nonstandard and nonportable solution. Programs written in these languages present significant challenges when the need arises to port them from one generation of hardware to the next.

A TVE avoids this challenge altogether by using high-level, open-standard software and provides a hardware abstracted product. An open-standards VM code and that written by other qualified organizations, can be ported to the next generation of HPC hardware without modification and is open to any and all participating in the common ecosystem.

Because every VM function is implemented as application software in the TVE, users can accept changes and new waveforms via software updates, often over-the-air. This allows the government to streamline the logistics trail associated with supporting VM users in the field. Furthermore, because VM applications are hardware-agnostic, a population of users equipped with different generations of hardware can take advantage of the same over-the-air software updates.

BIO: Michael Young has more than 24 years of leadership and management experience in the communications and network management fields. He holds an MBA from the University of Virginia Darden School of Business and was the program manager and technical lead on numerous satellite communications programs during his military career in the Army. Young is the senior director of advanced programs at Envistacom where his duties include leading capture and proposal team activities, performing profit and loss analysis, identifying potential business development opportunities, supporting M&A activities, supporting strategic long-range planning, market analyses and forecasting data for government and commercial market sectors. Prior to Envistacom, Young was responsible for the L-band Tactical (L-TAC) capability and its fielding by the U.S. Defense Department for use in augmenting UHF/VHF LOS radio capability, and he was one of the original members that stood up a satellite communications section within a Special Missions Unit in the Department of the Army.

HIGH CAPACITY BEYOND LINE OF SIGHT (BLOS) COMMUNICATIONS

LEO/MEO/GEO COMSATCOM Terminal Status

Steve Richeson, Vice President, Sales and Marketing, Mission Microwave Technologies LLC • steve.richeson@missionmicrowave.com

ABSTRACT

Combined low Earth orbit (LEO)/medium Earth orbit (MEO) [LEO/MEO]/geostationary Earth orbit (GEO) commercial SATCOM terminals are in the early stages of deployment using wideband Ka-band SATCOM terminal components to cover the bands required for LEO/MEO or traditional GEO networks.

Mission Microwave is the established radio frequency industry leader in supporting GEO satellite-based tactical SATCOM platforms in the 29 to 31 GHz range. It creates awareness of progress made in support of emerging LEO and MEO networks that require the full International Telecommunications Union (ITU) band of 27.5 to 31 GHz supporting commercial and military SATCOM operations.

Tactical VSAT terminals able to access LEO or MEO networks while being able to work on traditional GEO networks are required to support network migration to new architectures. The nonproprietary work completed with Mission Microwave's commercial SATCOM customers deploy radio frequency solid state amplifiers and frequency converters in support of these wideband Ka-band networks over the 27.5 to 30 GHz range. Early testing has confirmed throughputs in excess of 400MB/s with 16-ary waveforms and modeling confirms throughput of more than 1 Gb/s with path latencies under 50 msec. The same radio frequency components have been shown to support 32-ary waveforms on robust maritime terminals capable of transitioning between LEO/MEO and GEO networks. There also is a range of commercial standards encountered in supporting the cross-platform networks with commercial off-the-shelf products.

Mission Microwave has supported trials for maritime and land-based terminals in support of its testing of extremely high throughput LEO and HTS networks and are becoming widely deployed in SATCOM communications ground terminals for MILSATCOM application. These amplifiers use gallium nitride semiconductors and unique design and linearization techniques to provide drastic increase in performance in roughly 25 percent of the weight of traditional radio frequency amplifiers, which makes them suitable for deployment on tracking terminals where lightweight robust solutions are required.

BIO: Steve Richeson, vice president, sales and marketing, Mission Microwave Technologies LLC, joined Mission Microwave in 2017 and is responsible for sales and marketing. He has 30 years of satellite and radio frequency experience in engineering and sales leadership roles at Advantech Wireless, Exelis Inc., Harris Corporation, EchoStar, Scientific-Atlanta, GTE Spacenet International, SATCOM Technologies and Schlumberger. Richeson is a senior member of the IEEE and a registered professional engineer. He earned his engineering degree at Georgia Tech and an MBA at Georgia State University. Richeson is a 1980 graduate of Augusta's Butler High School and grew up in an Army family based at Fort Gordon.

Satellite-as-a-Service

Michael Young, Senior Director of Advanced Programs, Envistacom •
myoung@envistacom.com

ABSTRACT

Commercial SATCOM is leading the satellite industry with evolutionary low Earth orbit (LEO) satellites that can provide greater network throughput and support smaller and mobile satellite terminals. There also is a large infrastructure-based capital expenditure requirement to support these LEO assets and an added cost to set up these networks with the latest technologies.

Government-owned satellite networks are expensive and are at a technological disadvantage compared to their commercial counterparts in regard to size, scale and price as well as the immense amount of resources required to operate and maintain these networks. Additionally, near-peer adversaries are aware of government-owned satellite networks and will actively target such networks looking to block or at a minimum disrupt communications. This is why a Satellite-as-a-Service model may make sense as it allows the government to leverage the vast capital expenditure in R&D and operational costs that commercial satellite operators expend as they develop the latest technology in support of their commercial customers.

Commercial LEO architectures are a critical part of the new proliferated national security space architecture. Commercial LEO systems offer the ability to distribute military communications through a variety of paths and numbers of spacecraft to provide a mesh network that is resistant to single-point failure.

Furthermore, these architectures offer inherent low probability of intercept (LPI) communications architectures: LEO systems utilize geographically small and isolated spot beams, each of which is far more difficult to interfere with than the traditional GEO beam structures, whose narrowest spot beams cover hundreds of kilometers, giving an adversary that wants to interfere a wider area in which to operate and hide.

Any interference along a static geometry will be transient because of the movement of the user-satellite link geometry. The ability to reduce interference:

- Is native because of the design but also because it can use telemetry stream-back and an analytics engine to avoid bad geometries;
- Presents a low probability of intercept inherent in a multisatellite system with small satellite beams, beam-hopping and multiple satellites as it must be collocated within the footprint and looking at the same satellite;
- Includes a low probability of detection inherent with moving satellites, burst transmissions, hopping beams and narrow beams on user terminals;
- Features diverse and redundant paths and potential data obfuscation; and
- Provides multiple satellites that alternate paths.

Some commercial LEO networks add a critical feature for communications resiliency. These LEO spacecrafts are connected to an on-orbit mesh network of other LEO satellites via optical inter-satellite links (OISLs). A military user in a contested theater can communicate up to the LEO network and, via satellite-to-satellite communications, utilize a downlink on the other side of the earth without the need to downlink into a teleport anywhere near the contested theatre of operations. This also is applicable in regard to embassies and key military bases globally that will be able to communicate with sovereign locations without ever having to use a local terrestrial network from a foreign country. These commercial LEO networks with OISL address the core need of the national security space missions.

BIO: Michael Young has more than 24 years of leadership and management experience in the communications and network management fields. He holds an MBA from the University of Virginia Darden School of Business and was the program manager and technical lead on numerous satellite communications programs during his military career in the Army. Young is the senior director of advanced programs at Envistacom where his duties include leading capture and proposal team activities; performing profit and loss analysis; identifying potential business development opportunities; supporting M&A activities; supporting strategic long-range planning; market analyses; and forecasting data for government and commercial market sectors. Prior to Envistacom, Young was responsible for the L-band Tactical (L-TAC) capability and its fielding by the U.S. Defense Department for use in augmenting UHF/VHF LOS radio capability, and he was one of the original members of the team that stood up a satellite communications section within a special missions unit in the Department of the Army.

COMMAND, CONTROL, COMMUNICATIONS, COMPUTERS, INTELLIGENCE, SURVEILLANCE AND RECONNAISSANCE/ELECTRONIC WARFARE MODULAR OPEN SUITE OF STANDARDS (CMOSS) COMPLIANT CAPABILITY

REAL-TIME SPECTRUM AWARENESS VISUALIZATION

UWB Vector Sensor Technology

Marty Cunningham, President, MC Connect • mc@mcconnect.us

ABSTRACT

The electromagnetic spectrum (EMS) is increasingly congested and changing at an extremely demanding pace. The Army's need for real-time means the service members must be able to sense a local environment that ensures spectrum-dependent devices operate as intended; provide commanders EMS situational awareness of their own systems; and help inform tactical decisions based on current EMS and electromagnetic operational environment (EMOE) in real time.

Applied Signals Intelligence Inc. (ASI) has developed an ultra-wideband vector sensor that provides real-time EMOE input and interfaces with and is displayable on the Electronic Warfare Planning and Management Tool (EWPMT).

Vector sensors that incorporate polarization diversity make it possible to distinguish two signals with the same angle of arrival (AoA), assuming that they have different polarizations. Additionally, it has been shown that for a vector sensor as many as five signals with distinct AoA can be identified and estimated. Further, the polarization diversity allows finer AoA resolution than traditional linear arrays.

ASI is working with university partners to develop algorithms adapted to its vector-sensor array manifold data to distinguish overlapping spectrum users transmitting from different AoAs. The approach is to compare Eigenstructure-based approaches (e.g., MUSIC, ESPRIT) with machine learning (e.g., deep neural networks) approaches. Currently algorithms are under evaluation using ASI generated simulated vector-sensor array manifold data with promising early results.

ASI provides direction-finding (DF) systems on fixed and mobile mast mounts, fixed-wing aircraft and tethered UAS (TUAS). The vector sensor elements are dual port antennas (DPA) able to measure the electric and magnetic fields of a wave front to determine directionality. Three orthogonal elements (3D configuration) can measure all six field components (electric and magnetic fields) to determine azimuth and elevation angles. Two orthogonal elements (2D configuration) returns azimuth only.

The DF system detects and collects and in the near future will classify all the DF's emitters in its operating band (450 kHz to 20 GHz). It also locates emitters to an azimuth instantaneously—without motion required—from a single sensor and can integrate with other sensors to geolocate in latitude and longitude.

ASI's staff are experts in deploying radio frequency systems, antennas, signal processing, ISR, radar, communications and direction finding. With more than 100 patents, ASI delivers differentiated systems for direction finding, signal intercept and electronic warfare. The scalable vector sensor antenna design with associated signal processing is covered under U.S. patent 9,279,880. The antennas are electrically small (<10 percent wavelength), lightweight and extremely wide bandwidth and require minimal spacing for optimum performance. The technology uses software-defined radios with wideband instantaneous bandwidth to detect and locate frequency agile radio transmitters and other SOIs.

BIO: MC Connect is submitting this abstract on behalf of Applied Signals Intelligence ASI, which was founded in 2007 and is located in Sterling, Virginia.

The Importance of Intelligence to Multi-Domain Operations and EMSO

Laurie Buckhout, Director, Castellum Inc. • laurie.buckhout@gmail.com

ABSTRACT

Real-time spectrum visualization absolutely relies upon intelligence and sensor information, yet the fields are slow in coming together to trade and integrate data. As intelligence, signal, cyber and electronic warfare work more closely together, this relationship and the associated real-time data exchange requirement emerges as a critical area of improvement.

Intelligence, cyber and electronic warfare leaders such as Maj. Gen. Patricia Frost, USA (Ret.); Lt. Gen. Lori Reynolds, USMC; Lt. Gen. Karen Gibson, USA, at the DNI; and Maj. Gen. Laura Potter, USA, commander of the Intelligence Center of Excellence, should be brought together to discuss roles of intelligence in electromagnetic spectrum operations. Bringing these senior thought leaders together to discuss electromagnetic spectrum operations would be useful to the U.S. Army as well as other services.

BIO: Col. Laurie Moe Buckhout, USA (Ret.), is the founder and CEO of The Corvus Group, a strategic consulting and services group. She served as an Army officer from 1984 to 2010. She attended James Madison University, was commissioned in 1984 and served in Army leadership and staff positions from the 3rd Infantry Division to the White House and from platoon leader to a combat battalion commander, ending her career as chief of electronic warfare for the U.S. Army. In addition to a Bachelor of Science degree from James Madison University, she holds a master's of military arts and science, Command and General Staff College, Fort Leavenworth, Kansas; and Master of Science in information systems management, Webster University, St. Louis, Missouri. Her awards include the Distinguished Service Medal, the Bronze Star, the Defense Meritorious Service Medal (two awards), the Meritorious Service Medal (four awards) and several awards of joint and army commendation and achievement medals and well as other various service awards.

REAL-TIME SPECTRUM AWARENESS VISUALIZATION

Electromagnetic Metamaterial Exterior Treatment (EMET)

Tanner Metzmeier, Cybersecurity Engineer, CACI • tanner.metzmeier@caci.com

ABSTRACT

CACI proposes Electromagnetic Metamaterial Exterior Treatment (EMET), a paint-on metamaterial treatment that masks the electromagnetic emissions of an asset without interfering with the asset's capabilities. The EMET's concepts that comprise its value are:

- photonic metamaterials filter out specific wavelengths of EM waves;
- a coil permeated substrate with a capacitive tunable electronic load allows for electronic control of metamaterial permeability at echelon; and
- the paint-on method allows for low-cost and large-scale fabrication of metamaterial substrates into a usable applicator.

The application of these steps to an asset such as a forward operating base allows for the direct tunable control at echelon of the outward traveling electromagnetic emissions once the treatment is applied and power is connected. This would prevent on-the-ground clandestine intelligence operations such as Van Eck phreaking, which involves the capturing and decoding of electromagnetic emissions to gain previously displayed information on certain digital displays and to gain access to assets that contain sensitive intelligence.

The first concept of the EMET relies on the use of photonic metamaterials, which are naturally occurring materials that have been engineered to have newly designed structures smaller than the wavelengths of the phenomena they influence. These engineered structures allow the photonic metamaterials to have polarization and attenuation effects on EM waves that make contact. For example, when using silver ink as the dielectric and latex paint as the substrate, a thickness of 12.7 μm of dielectric must be achieved on the surface so that the 12.5 GHz band will not be allowed to permeate through the material and will therefore be filtered out of the EM emissions spectrum measured beyond that surface.

For concept two involves connecting two types of coils to a capacitive-tunable electronic load, an inductance value and a capacitive load is generated within the metamaterial substrate. A resonant permeability of the substrate caused by the variable capacitive load allows for the filtration of an EM wavelength range depending upon the substrate material used and the amount of voltage applied. This can be directly used to control the polarization and filtration of electromagnetic emissions at echelon.

Concept three provides value by using metamaterial substrate with latex paint to yield a paint-on method of application for the metamaterials. This method allows for high-absorbency, low-cost and large-scale fabrication of metamaterials for application on assets. An absorbency rate of 94 percent was achieved when using substrate in the shape of the perfect absorber during this low-cost and large-scale production method. Every layer of the substrate-paint amalgamate will only act as a limited wavelength polarizer and

filter out wavelengths specific to the property of the substrate. Therefore, multiple layers of paint with different substrates must be deposited onto the asset to cover the whole spectrum of EM emissions necessary for full EM masking. Once the layers that are necessary have been deposited, the resulting effect will be a photonic polarizer that filters out the specified wavelengths when the designated EM emissions attempt to permeate the material.

BIO: Tanner Metzmeier is a cybersecurity engineer currently located within the Washington, D.C., metropolitan area. At CACI, he leverages his prior industrial automation experience to develop innovative and creative solutions for industrial control system focused projects. Metzmeier holds a Bachelor of Science degree in mechanical engineering from Rose-Hulman Institute of Technology.

Signature Reduction and Deception in the Electromagnetic Spectrum

David Sharman, Military and Technical Advisor, Transhield Inc. •
davids@transhield-usa.com

ABSTRACT

Concerns about active radio frequency (RF) interrogation are well known. RF interrogation of communication, radar and combat systems enable the interrogator to determine the operating characteristics of that equipment and potentially to conduct electronic warfare. Protective covers manufactured from RF shielding drapeable materials, developed under a cooperative research and development agreement with Naval Surface Warfare Center Port Hueneme Division, prevent both asset interrogation and electronic warfare.

The RF shielding material also can prevent the scanning of a sensitive asset to determine its shape. This step is critical if the asset's performance can be deduced by knowing its shape. With slight modification, the material can be used to retrofit existing laboratories and sensitive sites with RF shielding.

RF shielding material that is perpendicular to the incoming energy will provide a return signal. However, because the RF shielding material is drapeable, the majority of the incoming RF energy will be deflected and scattered, thus reducing the signature of the covered asset.

The nature of the material facilitates its creative use in the realm of deception. In this instance, key elements that enable deception are the draping of material over a frame, adhering it to solid surfaces, the selective use of a non-RF shielding material or a combination thereof.

RF shielding covers could also be employed, for example, on a Navy ship to suggest additional communication, radar and combat systems are on board. These covers could also be employed to suggest the development and transition of next-generation communication, radar and combat systems when in fact nothing was developed.

Ground forces also could reap the benefits of employing the RF shielding covers to provide the adversary with multiple dilemmas. RF shielding covers could be employed to deceive an enemy by suggesting critical equipment is deployed at one location when in fact it is elsewhere. Employing RF shielding covers over a frame that appears to be multiple launch rocket systems, MLRS and HIMARS, for example, forces an adversary to ponder exactly where these combat systems are. Furthermore, it forces the adversary to: consider attacking all multiple launch rocket systems with an RF signature provided by the cover and unbeknownst to them expend munitions on decoys or attack only a portion of the targets, thus increasing the survivability of those combat systems.

BIO: David Sharman has been Transhield's military and technical advisor since 2015 and is responsible for identifying and executing research and development into advanced protective covers that provide the U.S. Defense Department with advanced protective covers for RF, EMP, IR and directed energy weapons threats. As Transhield's principal investigator, Sharman successfully executed a cooperative research and development project with NSWC PHD to develop RF shielding advanced protective covers. Those covers currently are available for acquisition. Sharman is preparing to lead Transhield's effort in a second cooperative research and development agreement with NSWC PHD to understand how to employ RF shielding materials to manage asset RF signatures, to develop decoys and to develop drapeable materials that will provide protection against high-altitude electromagnetic pulse (HEMP) and ground-based EMP.

SMALL FORM-FACTOR LONG-RANGE SENSOR AND/OR ANTENNA

Long-Range EW Sensor

Marty Cunningham, President, MC Connect • mc@mcconnect.us

ABSTRACT

The Army requires long-range electronic warfare (EW) sensors and/or antennas built in a small deployable form factor that can achieve ranges greater than 40 kilometers.

Applied Signals Intelligence Inc. (ASI) understands the importance of detecting, identifying and locating electromagnetic spectrum (EMS) signatures at significant distances to provide friendly and adversary situational awareness and to enable lethal and nonlethal targeting capabilities in large areas of operations.

ASI is currently supplying long-range electronic warfare (EW) systems built in a small deployable form factor that can achieve ranges greater than 40 kilometers to various military organizations. The sensors are based on ASI's recent advance in ultrawideband (UWB) vector sensor technology that enables a much smaller footprint than traditional DF systems. Current productizations operate from HF to 6 GHz. HF to 20 GHz will be operational in calendar year 2021.

The sensor delivers single-platform RF detection, classification, collection and DF. Extended range is enabled by the small form-factor, which allows the sensor to be located on a tall mast or on a tethered UAS (TUAS). The TUAS system, at 100m altitude, has been demonstrated to detect, collect and DF low power emitters (e.g., 2 W) in the VHF and HF bands at ranges in excess of 40 km. It locates emitters to an azimuth instantaneously without motion required from a single sensor and can integrate with other sensors to geolocate in latitude and longitude.

The wide IBW of ASI's vector sensor technology makes it well suited to DF complex waveforms. The system has demonstrated detection, DF and blind de-interleave of relevant frequency hopped waveforms typical for MILCOM radios (hopped digital modulations, 100 Hz and 20 kHz) and air defense radar (hopped modulation-on-pulse).

Direct sequence code division multiplexing and noise-like waveforms spread the baseband signal energy in frequency and time. These are generally LPD waveforms. Knowledge of the underlying spreading function (e.g., codes) is required to de-spread the signal. ASI does not have technologies to find spreading codes; it has developed technology to operate in a code-assisted mode where another system de-spreads the signal and ASI systems DF it.

ASI delivers the latest in DF and geolocation systems. The technology is lightweight and small and operates over extremely wide instantaneous bandwidths.

BIO: MC Connect is submitting this abstract on behalf of Applied Signals Intelligence Inc. (ASI) located in Sterling, Virginia. The company's staff members are expert in deploying RF systems, antennas, signal processing, ISR, radar, communications and direction finding. The team has more than 100 patents in RF technologies. ASI delivers differentiated systems for direction finding, signal intercept and electronic warfare.

CYBER DOMAIN MODELING AND SIMULATION (M&S) CAPABILITIES AND THEIR INTEGRATION WITH OTHER DOMAIN M&S

BDP as a DevSecOps M&S System

John Eubank, Technical Director, Alion • john.eubank@alionscience.com

ABSTRACT

As the joint forces integrate capabilities in support of Joint All-Domain Operations (JADO), a solution is needed that is service and domain agnostic to provide modeling and simulation (M&S) capabilities from the tactical/deployed/afloat edge to the enterprise in a seamless manner. Recently, the Joint Strike Fighter (JSF35) Joint Program Office (JPO) has invested in evolving Big Data Platform (BDP) to become a data integration ecosystem and DevSecOps environment for M&S. For the Army, the BDP that has been implemented is Gabriel Nimbus (GN) for cyberspace operations use cases. Combining the Army's investment in the BDP with the JSF35 JPO investment will result in a domain agnostic M&S system for cyber, information warfare and other use cases across JADO.

The BDP provides a data source agnostic data ingest, storage, fusion/processing, visualization and sharing/transport system accredited for use on all classification environments. It comes with existing integrations to cross-domain solution farms to enable low-to-high and high-to-low data correlations using queries, analytics, models and algorithms.

The BDP, for instance, can rapidly field new capabilities such as Kubernetes containers or Rapid Deployment Archives using an Agile DevSecOps approach combining government and contractor resources in a software factory. In a matter of weeks, integrated force-on-force cyber domain modeling capabilities can be implemented on the existing multipetabyte-scale repository of data in GN, GN-S and GN-TS. In parallel, additional data sets can be brought into GN or a new BDP can be stood up to handle broader information warfare data sets (e.g., electromagnetic spectrum (EMS)). The GN's architecture facilitates the integration of disparate data types with an agnostic approach to the analytics, algorithms, models and other applications to be deployed onto the data. In addition, its architecture was designed with integration in mind, and the system can connect to other M&S systems across the JADO ecosystem.

BIO: John Eubank has spent the past eight years tackling the U.S. Defense Department's massive scale data challenges from the tactical edge to the joint enterprise. Most recently, Eubank has taken on leading the Alion Information Warfare transformation for Joint All-Domain Operations. His day-to-day role is Alion's cyber technical director, providing solution design on full-spectrum cyberspace operations.

Eubank has a master's degree from the University of Maryland in information management and a bachelor's degree from Towson University in computer information systems and business administration (dual degree). His extensive background prior to entering the big data space included cellular telecommunications, accounting, oversight of NSA's East Campus build out and software engineering.

Combating Adversarial Information Warfare in the Cyber Domain

Melissa Sowerwine, Manager, Business Development, IDS International •
msowerwine@idsinternational.com

ABSTRACT

The information environment has become an arena for malign influence activities and cyber dominance, including attacks against critical infrastructure, incapacitating government and private-sector cyber infrastructure, digital authoritarianism by nation-states and online member recruitment by terrorist organizations. These nefarious state and nonstate actors are weaponizing social media platforms and other online information sources to disseminate propaganda, control citizens and stoke distrust and chaos among U.S. and allied civil societies. Furthermore, they use the Internet as a platform to reach a vast audience to communicate and collaborate, often through undetected channels that are typically buried in the overwhelming volume of online traffic.

IDS International is using its unparalleled expertise and current technology innovations in cyber and information operations (IO) training, modeling and simulation (M&S) and live experimentation to support the military's fight against adversarial cyber and influence operations. The company has created and is further developing a digital training environment called the Synthetic Internet for Training and Exercises (SITE) for the Combating Terrorism Technical Support Office (CTTSO). SITE provides Special Operations Forces (SOF) a full-range, free-play, immersive, realistic and scalable operational range in which warfighters can conduct full-spectrum information warfare training while replicating realistic Internet ecosystems in a closed network environment. This project allows cyber, intelligence, IO and exercise scenario development personnel to incorporate the inimitable nature and effects of online information into comprehensive training and exercise environment without the risk and confines of using the open Internet.

Content in SITE is flexible and customizable, covering everything from social media analysis and engagement to offensive and defensive cyber scenarios. It incorporates proven commercial and government off-the-shelf cyber and information tools and interoperates with cybersecurity and publicly available information analysis tools. A holistic and dynamic training environment, SITE hosts realistic replications of the Internet and other features, including social media platforms, instant messaging platforms, search engines, online auctions, video games, replicated world news with RSS feeds, e-mail, discussion blogs, government and NGO websites, online radio for messaging, video streaming, a robust cyber library, sentiment generation with artificial intelligence (AI), malicious and benign traffic generation, and deep and dark web capability. Additionally, the training environment has a simulated Internet backbone that replicates realistic network environments and also has access to website data from application programming interfaces (APIs) and databases using real-world analytic tools.

The training environment also features microservices, including docker containers as container-orchestration systems for automated deployment, scaling and management of application containers; Event Bus, which is a background messaging system used internally by SITE to broadcast user activity and system events across the entire SITE system for storage and later consumption and/or real-time analysis; an enhanced search engine that returns realistic broad results; the proprietary Exercise Development and Management Tool that allows exercise controllers to monitor and control every component of SITE; and the ability to support up hundreds of concurrent users via elastic load balancing and autoscaling.

This program demonstrates IDS' ability to plan, implement, manage and execute large-scale, complex cyber operations live experimentation; systems engineering, troubleshooting and real-time network monitoring; and modeling and simulation of global Internet networks and cyber effects in support of the military's strategic objectives.

BIO: Melissa Sowerwine's previous experience conducting social media monitoring and developing social media strategies for *Fortune* 50 clients at the CEO advisory firm Teneo Holdings allows her to bring a fresh perspective to IDS that can easily be translated to government customers. She also supported Teneo as a Middle East policy SME by providing clients key insights into policy implications and events in the region that could impact various industries, including energy, finance and technology. Prior to joining IDS, Sowerwine was the vice president of operations at Red Six Solutions (RS2), a red teaming firm that provides commercial and government customers with over-the-horizon insights into imminent threats that can significantly impact reputation, valuation, resource allocation and strategic decision-making. While there, she organized and facilitated strategic tabletop exercises (TTX) and live training events for commercial and government customers. Through RS2, she supported a contract as a Middle East and Turkey analyst for Predata, a predictive analytics firm that enables customers to anticipate global events and market moves by better understanding human behavior through the use of alternative data and machine learning. She also supported the U.S. Army and Intelligence Community in live small unmanned aircraft systems (sUAS) experiments, where she helped customers test vulnerabilities in their counter-UAS technologies before they were used in a real-world scenario. Sowerwine has a Bachelor of Arts in political science with a concentration in international relations.

Use of Cyberspace Battlefield Operating System Simulation (CyberBOSS) for Integration of Cyberspace Training with Army Modeling and Simulation (M&S) Capabilities

Omar Hasan, Chief Architect, Dignitas Technologies •
ohasan@dignitastechnologies.com

ABSTRACT

Combatant commanders are most effective in warfighting when directing the employment of forces within a combined theater of operations, including land, maritime, air, space and now the cyberspace domains. In the modern battlespace, offensive and defensive cyberspace operations play a critical role supporting traditional domain operations, ensuring information flow to the warfighter and disrupting opposing force communications. Battle staffs need training to better identify and exploit offensive and defensive actions in cyberspace in coordination with the more traditional kinetic and nonkinetic effects they are more accustomed to deploying.

The existing Army live, virtual, constructive and gaming (LVC&G) training systems contain accredited models for traditional operational domains; however, they are not developed to incorporate offensive and defensive effects of cyberspace operations as a part of combined training. Through modeling and simulation (M&S), the Army is incorporating a cyberspace representation with existing LVC&G systems. The results will support various training echelons, system fidelities and resolutions and interoperability across federations.

To better incorporate the essential cyberspace domain into collective LVC&G training, Cyberspace Battlefield Operating System Simulation (CyberBOSS) provides both a common representation for cyber effect models in synthetic systems and a supporting architecture that brokers properly abstracted representations across systems. CyberBOSS can inject cyberspace effects and actions into existing Army training systems. Those systems typically have little to no cyberspace effects or models and do not meet emerging training needs. Most current training simulation systems focus on the kinetic battlespace and exclude cyberspace effects, accurate communications, digital systems and cyber-based models. These training systems do not consider the concepts of fidelity and resolution of the cyber terrain and how cyberspace models impact kinetic models.

CyberBOSS research and development activities are establishing a path for the inclusion of the cyberspace domain and cyber training operations into LVC&G training systems such as One Semi-Automated Forces (OneSAF) and Joint Land Component Constructive Training Capability (JLCCTC). Initial integration tests with OneSAF have demonstrated that CyberBOSS can provide cyber-capable forces and cyberspace effects on OneSAF modeled devices.

The CyberBOSS broker architecture supports the correlation of cyber terrain between connected synthetic battlespaces and cyber ranges. It also supports delegation of attribute modeling depending on connected systems to allow federations with and without high fidelity cyber terrain models. This approach supports the ability to broker cyberspace effects between disparate systems to represent cyberspace operations in federated environments. CyberBOSS has already been integrated with several other federated training systems, including the Network Effects Emulation Service (NE2S) to provide network effects and the Ares Tactical Planner for visualizations. The CyberBOSS research and system development activities support both cyber-for-others and cyber-for-cyber training activities to enhance LVC&G environments to prepare the Army for holistic multidomain operations.

BIO: This work is being conducted by Omar S Hasan, Ph.D.; Jeffrey L Welch; and Bob Burch of Dignitas Technologies LLC; Nathan L. Vey and J. Allen Geddes of the U.S. Army Combat Capabilities Development Command–Soldier Center (CCDC SC); and Specialist 1st Class Paul Ray Smith, USA, Simulation & Training Technology Center (STTC).

Cyber Domain Modeling and Simulation (M&S) Capabilities and Their Integration With Other Domain M&S

Jason Crabtree, CEO, QOMPLX Inc. • jason@qomplx.com

ABSTRACT

Current Army modeling and simulation (M&S) tools, specifically ONESAF and WARSIM, do not adjudicate enemy or friendly cyber actions, severely limiting the training value of integrating the cyber domain into current training simulations. QOMPLX has built a scalable, concurrent, multi-user agent-based simulation toolkit, Q:SIM, and an underlying data fabric, Q:OS, that is well suited to handle the cyber domain M&S tasks and is easily federated with other domain M&S tools.

Q:OS allows several such models to share data with each other or with other enterprise applications concurrently, at scale and in a multi-user environment. Q:OS also enables scalable storage and ingestion of graph-based network data and of sensor-obtained time-series data. Q:SIM supports agent-based modeling, discrete event simulation and massively multiplayer participation similar to online-gaming simulations with templated WYSIWYG agents that can be instantiated in several different models.

QOMPLX presents an agent-based cyber-domain model(s) specification that illustrates the market-leading capabilities of Q:SIM and Q:OS. The company illustrates how the cyber-domain model, built and operated inside Q:SIM, can serve as a federated instance of a model that informs operations strategy in a wider operational domain by sharing dependent and independent inputs with other such instances and through API-enabled modeling and parametric-study requests.

BIO: Jason Crabtree is a cofounder and serves as the chief executive officer and board member at QOMPLX. He is an expert on cybersecurity, operational risk management, decision support/automation technology and simulation/predictive modeling of complex-adaptive systems. As a Rhodes scholar, Crabtree researched artificial intelligence-based optimization of engineering design processes at Oxford University. First Captain of his class at West Point, he is a licensed professional engineer who served as a Ranger/Sapper-qualified infantry leader in Afghanistan before completing military service as a special assistant to senior U.S. Defense Department cyber leadership with emphasis on the development and operational integration of advanced technology initiatives including work with DARPA. Crabtree also was a 2014 Cyber Policy Fellow with the Madison Policy Forum in New York City and a 2016 Cyber Fellow for the New America Foundation. He has been an invited participant, panelist and speaker on energy, risk management, finance and security for organizations, including the Casualty Actuarial Society, Financial Services Roundtable, the Center for New American Security, the Markle Foundation, the Ditchley Foundation, the Gridwise Architecture Council and RAND in both the United States and United Kingdom.

WHAT IS AFCEA?

AFCEA is a member-based, non-profit association for professionals that provides highly sought-after thought leadership, engagement and networking opportunities. The association focuses 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