Multi-Domain Operations Workshop
2022 Technical Program

Wednesday, July 20, 2022, 2:45 – 4:45 p.m.

Session 1 **JETS: EW T&E Capabilities Enabling MDO** **CUI: Distribution C**
Chair Geoff Wilson, T&E/S&T PM, Test Resource Management Center (TRMC)

2:45 p.m. **"Joint Electronic Warfare T&E Strategy"**
Geoff Wilson, T&E/S&T PM, TRMC

TBD

3:15 p.m. **"Open-Air Battle Shaping"**
Scott Weed & Rick Shelley, TRMC

TBD

3:45 p.m **"Knowledge Management/Big Data Analysis"**
Billy Williams & Gene Hudgins, KBR

TBD

4:15 p.m. **"Advanced Multi-Variate Time Series Analytic Techniques using AI & ML"**
Kenny Sanchez, TRMC; Tony Triolo, Perspecta Labs; Kathy Smith & Bill Wolfe, GBL Systems; Kent Pickett, MITRE

TBD

Wednesday, July 20, 2022, 2:45 – 4:45 p.m.

Session 2 **Mission Based Cyber Risk Assessment and Data Acquisition for MDO T&E**
Chair Kenny Hill, Business Development & Program Manager, Trideum

2:45 p.m. **"Data Acquisition System (DAS)"**
Jason Martin, Senior Solutions Architect, Trideum

The Data Acquisition System (DAS) product is an easily reconfigurable data collection, processing, and streaming system tailored to meet the data collection demands of low-cost, small form factor system-level testing. With a projected cost of under $15,000 per unit, a size of approximately 4"x4"x2.5", and a weight of < two (2) pounds, it brings powerful data collection capability into a size and form factor compatible with the most demanding environments. The DAS offers a combination of essential features into its own chassis, but also allows for the connection of modular peripherals which expand its capabilities based upon the requirements of the test. Best of all, it is more than just a data acquisition system; it is also a powerful and rugged miniature supercomputer with advanced data processing and machine learning capabilities. The DAS combines a powerful embedded computational platform, streaming and recording technologies, fast and reconfigurable wireless capabilities, and an array of attachable sensors and peripherals. It is easily configuring, deploys and operates via a wide array of power supplies, including batteries. At a typical "full load" power draw of less than 20W, batteries for up to two (2) hours of constant data collection are still practical in size.

3:15 p.m. **"Leopard"**
Jason Martin, Senior Solutions Architect, Trideum

Leopard designs bring a high degree of situational awareness, control, and insight into test events conducted at Test & Evaluation ranges and facilities. The ability to integrate multiple data sources - and leverage that information to provide consistent, accurate, and useful information - is key to maximizing value of test events, and in turn provide maximum value to Test & Evaluation customers. The data generated by instrumentation, cameras, and other relevant data sources can be immense. A single test event may involve collecting data from large numbers of System Under Test (SUT) and other data sources, each providing Time/Space Position Information data, high resolution video, system bus traffic within the SUT, and other sensor inputs. This data can be overwhelming, especially if disparate systems are sending data in separate ways, using different timescales, and different formats.
Leopard designs fill this capability gap. It is a single solution that is scalable, intuitive, flexible, and provides an extensible data management and visualization platform designed from the ground up to provide real-time intelligence through critical insight to testers and event managers. Leopard provides data management

and analytics extended from and powered by CloudHybrid Edge-to-Enterprise Evaluation & Test Analysis Suite, combined with intuitive visualizations to provide users immediate and actionable insight. When paired with video distribution hardware such as the Galileo video wall systems from RGB Spectrum, it can even integrate with these systems to further customize and control the in-event visualization experience.

3:45 p.m **"Cybersecurity Vulnerability and Assessment Test Environment (CVATE)"**
Aaron Gould, Senior Solutions Architect, Trideum

The Cybersecurity Vulnerability and Assessment Test Environment (CVATE) Other Transaction Authority advances the Redstone Test Center (RTC) Distributed Test Control Center into a robust, repeatable, and instrumented environment to support the challenging need for cybersecurity vulnerability testing for U.S. Army weapon systems. CVATE leverages RTC resources and partner test organizations to provide Testing and Evaluation capability. CVATE developments go beyond compliance-based cyber assessments. CVATE consists of capabilities for assessing the effects of adversarial cyber operations at the subsystem, system, and system of system levels as well as at the mission level, while the test article merges in a representative mission environment.
As the foundation of the RTC's overall cyber–Developmental Test and Evaluation strategy, CVATE uses a realistic operational environment with simulation/stimulation as well as representative cyber threats based on the latest intelligence information. State-of-the-art instrumentation is available for high-speed and high-quality data collection, analysis, and visualization. Mission-impact from cyber threats reports and archives to inform cyber risk to Program Managers.

4:15 p.m. **"TBD"**
TBD

TBD

Wednesday, July 20, 2022, 2:45 – 4:45 p.m.

Session 3 **Cyberspace Test Technology**
Chair Min Kim, Deputy Executing Agent, TRMC T&E/S&T Cyberspace Test Technology (CTT)

2:45 p.m. **"Measure and Share"**
Dr. Michael Shields, TRMC T&E/S&T CTT Chief Scientist, &
Pete Firey, MITRE

Current DoD Cyber testing is conducted in a stove piped and independent event manner resulting in testing inefficiency. There is no universal mechanism to quantify the efficacy of a cyber test, and mechanism to promulgate test results to the T&E community and the broader DoD community. The goals of this project is to develop an initial set of measurement tools that provide quantitative analysis of test events, and develop "perspectives" which provide the information that are domain (e.g., T&E perspective, Operational perspective, Acquisition perspective and Intel perspective) specific. This presentation provides a proposed solution to measure the efficacy of cyber test event and share the test results at an appropriate classification level.

3:15 p.m. **"Vader Modular Fuzzer: What, Why and How"**
Arch Owen, Program Manager, Draper

TRMC is developing "Vader Modular Fuzzer" to address the broad range of U. S. Government fuzzing needs. The Vader Modular Fuzzer is based on Draper's Vader modular software fuzzing framework. Its modularity permits fuzzing developers to quickly create new fuzzing capabilities by designing specialized modules and integrating those modules into the existing framework. Ongoing development is focusing on usability, enhanced modularity, application to embedded systems, and advanced fuzzing features. The Vader Modular Fuzzer will provide the DoD and other Government agencies an open source, modular, no-fee solution for fuzzing the critical software and systems.

3:45 p.m **"Automated Machine Learning for Cybersecurity"**
Dr. Himanshu Upadhyay, Florida International University, Principal Scientist

Florida International University in collaboration with Test Resource Management Center has developed Cyber Threat Automation and Monitoring (CTAM) system to detect, analyze and monitor the test vector behavior during cyberspace attacks in the virtualized environments. CTAM is designed to identify the impact of test vector on the specified mission using advanced instrumentation tools focused on smart memory acquisition with virtual memory introspection (VMI) and advanced cyber analytics using the state-of-the-art artificial intelligence methodologies. Team has developed an automated machine learning system using the AI based advanced

analytics platform of the CTAM. This is a standalone system which allows machine learning model building, advanced analytics and visualization of predictions using the data collected from different test technology domains using traditional machine learning / deep learning and ensemble learning approaches. This system has automated machine learning through various platforms like AI based Advanced Analytics, Analytics Control Center and Data Source platforms. This presentation will start with AI/ML basics and further discuss the AAML features.

4:15 p.m. **"Automated Attack Framework for Test & Evaluation (AAFT)"**
Andrew Shaffer & Bruce Einfalt, The Applied Research Laboratory,
The Pennsylvania State University Research and Development Engineer

Red Team cybersecurity testing is critically important to ensure that new systems will perform as expected without compromising mission success. Unfortunately, no individual Red Team can keep up with the torrent of new threats that are being discovered every day. Also, a lack of cybersecurity Red Team availability often delays system accreditation and forces procurement programs to move forward with less mission assurance than is desired.

The Automated Attack Framework for Test & Evaluation (AAFT) enables Red Teams to keep pace with the threat by providing a framework for Red Teams to collaboratively capture and share information about threat cyberattacks in a format that is intelligible to an autonomous cybersecurity testing system. It also improves Red Team utilization and efficiency by automating the execution of threat cyberattacks and emulating basic and intermediate-level cyber threats so that Red Teams can focus on emulating more sophisticated threats, increasing the overall scope of cybersecurity testing that can be performed.

The basic AAFT framework has now been implemented and a wide range of different cyberattacks have already been integrated for use in AAFT-enabled automated testing. Development of the AAFT system is ongoing, and plans are in place to scale up the complexity and scale of the attacks that AAFT can autonomously execute.

Wednesday, July 20, 2022, 2:45 – 4:45 p.m.

Session 4 **T&E Methodologies and Approaches to Advance MDO**
Chair Gina Sigler, Scientific Test and Analysis Techniques (STAT) Center of Excellence (COE)

2:45 p.m. **"A Novel Concept for T&E of Autonomous Systems in Multi-Domain Operations"**
Charlie Middleton & Dr. Lenny Truett, Scientific Test and Analysis Techniques Center of Excellence

Not releasable

3:15 p.m. **"Applying STAT Concepts of Model Validation with Multiple Sources"**
Nick Jones & Kyle Provost, Scientific Test and Analysis Techniques Center of Excellence

The Department of Defense (DoD) currently faces rapidly changing operational environments and emerging threats that require complex engineered multi domain defense systems to be developed on ever-shorter timelines. To meet this need, the DoD is placing increasing trust in modeling and simulation (M&S) for the design, development, and engineering of new capabilities. Therefore, it is crucial that decision makers and developers understand whether models are valid and trustworthy representations of the systems under development. Validation is a process which determines the trustworthiness of a model by assessing whether the model has sufficient fidelity relative to an appropriate referent(s) for a specific intended use. Validation referents are needed to quantify fidelity: the level of consistency between a model and reality. However, validation is often complicated by the need to use multiple sources of information as referents for the true system behavior. These referents could include other more established models, more than one lab source, or even more than one live fire test event. Scientific Test and Analysis Techniques (STAT) provide the methods to quantify the fidelity. This brief will utilize a case study to delineate how to use STAT as the foundation for quantifying fidelity and account for differences in scope when validating models versus multiple referents.

3:45 p.m **"Applying Design of Experiments (DOE) to Testing and Evaluating Performance Across the Cyber Domain"**
Dr. John Hong, Institute for Defense Analyses, Assistant Director

The core of the emerging National Defense Strategy will include "integrated deterrence,… a framework for working across warfighting domains, theaters and the spectrum of conflict." Thus, successfully executing Multi-Domain Operations (MDO) will remain key to the strategy. Enabling successful execution will include

resilient performance across the Cyber Domain, an important and increasingly contested part of MDO. Comprehensive and efficient cybersecurity testing will be needed to rigorously evaluate the resilience of performance across the Cyber Domain. It has become standard practice to use Design of Experiments/Scientific Test and Analysis Techniques (DOE/STAT) to develop efficient tests and evaluate their results without considering every of the many combinations of factors that can affect system performance. This approach has been widely applied to conduct both developmental and operational testing outside the Cyber Domain. This presentation demonstrates how DOE could be applied to support efficient and rigorous cybersecurity testing and evaluation.

4:15 p.m. **"Digital Engineering Enabling T&E Planning Through the Integrated Decision Support Key (IDSK)"**
Jean Petty & Suzanne Beers, PhD, MITRE

The Integrated Decision Support Key (IDSK) provides a framework for articulating cradle to grave lifecycle decision making, informed by an evaluation of both operational and technical capabilities, drawing data from the full test continuum of early contractor testing through full-up system of system operational test and/or modeling and simulation. Applying the IDSK thought process to multi-domain operations use cases could inform the effectiveness of the existing JADC2 reference architecture in meeting MDO mission objectives, guide the design of the campaign of experimentations and demonstrations to gather the data needed to evaluate architectural components' mission contributions, and inform system/architecture refinements to better accomplish mission objectives. This presentation will walk through the IDSK's evaluation-based decision support concept and illustrate its use with a notional MDO application.

Thursday, July 21, 2022, 1:00 – 3:00 p.m.

Session 5 **Multi-Domain Initiative**
Chair Hans Miller, Project Leader, OSD Programs, The MITRE Corporation

1:00 p.m. **"TBD"**
TBD

TBD

1:30 p.m. **"TBD"**
TBD

TBD

2:00 p.m **"TBD"**
TBD

TBD

2:30 p.m. **"TBD"**
TBD

TBD

Thursday, July 21, 2022, 1:00 – 3:00 p.m.

Session 6 **Workforce Development**
Chair Richard Martinez, GreyBeards Group

1:00 p.m. **"TBD"**
Brendan Sullivan, NMSU

TBD

1:30 p.m. **"TBD"**
TBD

TBD

2:00 p.m **"Leading to T&E Excellence"**
Jason Farley, UTEP, College of Engineering, TMAC

Global security threats aren't just changing, they're adapting and they're doing it faster than ever… on all fronts! The diverse and rapidly evolving capabilities of our adversaries requires a defense and security response that is even more dynamic and comprehensive. As a part of that response, the Department of Defense organizes the development and fielding of solutions through the Defense Acquisition System. Great work has been achieved in modernizing that organization and its processes, including the Adaptive Acquisition Framework, the New 5000 Policies, MOSA, etc., that enable effective program management, facilitate agility, and enhance delivery capability to produce at the speed of relevance. A critical component of the DAS is Test and Evaluation. It is not enough for T&E to keep pace with other components of the DAS, it must be out in front! Said another way, it is required that the T&E function sustain performance excellence.

Test and Evaluation can be done better, no matter the current state. This statement represents a principle. Of course, there are many principles… literally countless. So, does this particular principle deserve to be prioritized and cultivated, perhaps even elevated into a value for organizational units working within the T&E for MDO enterprise? To wit, test and evaluation for MDO can be designed and developed to be precisely what is needed, delivering the most accurate and trustworthy results. It's a matter of how well the system is designed and executed. There are many disciplines at work in the enterprise of T&E for MDO: engineering, science, business management, etc. Subsequently, there are many associated approaches, models, and frameworks that can lead to the use of many more methods, techniques, and tools. The T&E for MDO enterprise presents a complex environment. Management has the daunting task of organizing, including continually developing and effectively using, a precisely focused T&E system that

delivers on a value promise in pursuit of the third Imperative of Combat: "believe in your weapons and equipment".

How can management achieve operational excellence in T&E for MDO? Fundamentally, it begins with achieving organizational excellence and culminates in the validated delivery of value. The pursuit of excellence begins on a foundation of principles that drive behavior and decision-making. And yet, an enterprise does not always select or fully understand appropriate principles, that is principles of consequence. How does this happen if there are bodies of knowledge, supposed "best practices", and standards? The answer can be found in understanding the nature of the system of interest and scrutinizing the principles upon which the system is and should be designed and operated.

The T&E for MDO enterprise is a socio-technical, adaptive system of systems in which thousands of principles drive decisions every day. If the system is to be optimized, participants must be enabled and empowered to take informed action guided by appropriate principles, i.e., responsible and aligned agency as a building block for operational excellence. Competent leadership and management are critical in developing a value creation system and culture that are engaging and produce maximum value.

2:30 p.m. **"TBD"**
TBD

TBD

Thursday, July 21, 2022, 1:00 – 3:00 p.m.

Session 7 **WSMR Supporting MDO CUI: Distribution C**
Chair Zoe Aguirre, White Sands Missile Range

3:30 p.m. **"TBD"**
Rocio Rangel, White Sands Missile Range, Range Operations - Lead Engineer/Optics

TBD

4:00 p.m. **"TBD"**
Brian Johns, White Sands Missile Range, Range Operations - Lead Engineer /TSPI

TBD

4:30 p.m **"TBD"**
Jesus Nevarez, White Sands Missile Range, Range Operations - Lead Engineer/Telemetry

TBD

5:00 p.m. **"TBD"**
TBD

TBD

Thursday, July 21, 2022, 1:00 – 3:00 p.m.

Session 8 **Cyber - Army Combat Capabilities Command**
Chair Cedric Baca, C4ISR Division Chief, Army Futures Command (AFC), DEVCOM Analysis Center

3:30 p.m. **"Electromagnetic Warfare (EW) Threat Environments for Lab Based Risk Reduction (LBRR), Experimentation, and Testing"**
Cedric Baca, C4ISR Division Chief, Army Futures Command (AFC), DEVCOM Analysis Center

Provide an overview of the state of art Electromagnetic Warfare (EW) for open air experimentation and testing, laboratory experimentation, and EW assessments across the Electromagnetic Spectrum (EMS). Discuss the leading edge tools, techniques, and methodologies used to ensure electromagnetic spectrum dominance for the Warfighter.

4:00 p.m. **"Cyber Experimentation, Analysis & Assessment in Support of Army Modernization Enterprise"**
Humberto Mendoza, Army Futures Command (AFC), DEVCOM Analysis Center (DAC)

The cyber division from the DEVCOM Analysis Center (DAC) executes cyber experimentation & analyses in support of Army Modernization priorities, readiness programs, and acquisition T&E. DAC will provide an overview of cyber tools, techniques, and methodologies used to identify vulnerabilities and collaborate with Army PEOs/PMs to develop remediation solutions that enhance the cyber resilience of Army technologies. DAC will also provide overview of future development capabilities in distributed cyber experimentation and analysis, as well as capabilities in coordinated Cyber Electro-magnetic Activities (CEMA) techniques within an MDO environment.

4:30 p.m **"TBD"**
TBD

TBD

5:00 p.m. **"TBD"**
TBD

TBD