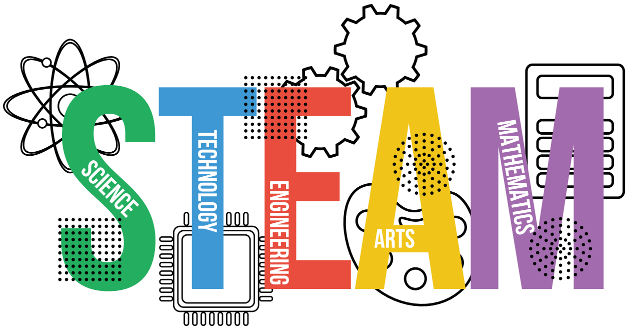
Cybersecurity Workshop

Securing the Future: Navigating the Evolving Threat Landscape

August 29-31, 2023
Westin Virginia Beach Town Center
Virginia Beach, VA

ITEA

itea.org



STEAMhack Chain Reaction Challenge

TUESDAY, AUGUST 29TH | 1:00 P.M. – 4:00 P.M.

Monarch III | Awards Ceremony at 5:00 P.M.

The STEAMhack™ Chain Reaction Challenge is a speed-building event where teams of 3–6 high school students receive a kit of materials and about 3 hours to build the most impressive chain reaction-style machine.

This year, students will have to "Catch a Meteor" by building machines to launch and catch a meteor, and integrate the reason for catching a meteor into the story described by the team prior to the triggering of the chain reaction.

Please join us for the Awards ceremony after the competition at 5:00 P.M.!

Support the Future T&E Workforce!

SCHEDULE-AT-A-GLANCE

EVENTS	DAY/TIME
Registration	• Monday, August 28 3:00 p.m. – 5:00 p.m. • Tuesday – Thursday 7:00 a.m. – 5:00 p.m.
Tutorials	• Tuesday, August 29 8:00 a.m. – 12:00 p.m. / 1:00 p.m. – 5:00 p.m.
Exhibit Hours	• Wednesday, August 30 9:00 a.m. – 5:00 p.m. • Thursday, August 31 9:00 a.m. – 3:30 p.m.
Technical Sessions	• Wednesday, August 30 3:00 p.m. – 5:00 p.m. • Thursday, August 31 1:00 p.m. – 3:00 p.m.
Opening Ceremony & Keynote Speakers	• Wednesday, August 30 8:00 a.m. – 10:00 a.m.
Featured Speakers	• Wednesday, August 30 10:30 a.m. – 2:30 p.m.
Cocktails with the Exhibitors	• Wednesday, August 30 5:00 p.m. – 6:30 p.m.
Featured Speakers	• Thursday, August 31 8:00 a.m. – 10:10 a.m.
Panel: Cyber T&E of Generative AI Systems	• Thursday, August 31 10:30 a.m. – 12:00 p.m.
Closing Keynote	• Thursday, August 31 3:30 p.m. – 5:00 p.m.

ATTENDANCE REQUIREMENTS

*The Workshop will contain some **Controlled Unclassified Information (CUI)** presentations, which will limit participation to U.S. citizens who are employees of the U.S. Federal Government or its contractors (C), or employees of the Department of Defense or its contractors (D). DoD common access cards (CAC) or personal identity verification (PIV) will be required for entry. If you do not have a CAC/PIV and submitted a Visit Request by the deadline, your name will be on the approved list of attendees.*

THANKS TO OUR SPONSORS

TECHNICAL EXCHANGE

Booz | Allen | Hamilton

PLATINUM

CPT COMMAND POST TECHNOLOGIES

GOLD

EWA Government Systems, Inc.

Georgia Tech Research Institute

SRC SCIENTIFIC RESEARCH CORPORATION

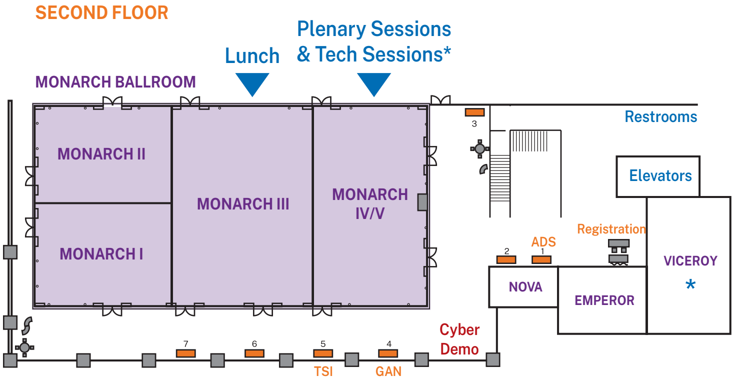
KBR

MTSI MODERN TECHNOLOGY SOLUTIONS, INC.

BRONZE

ADS ACQUIRED DATA SOLUTIONS

CYBER 2023
EXHIBIT HALL & MEETING ROOMS



Crescent room is located downstairs, next to the restaurant.

Exhibitors

Acquired Data Solutions	1
Geeks and Nerds (GAN)	4
Technical Systems Integrators	5

Exhibit Hours

Wednesday, August 30	**9:00 a.m. – 5:00 p.m.**
• Break with the Exhibitors	10:00 a.m.
• Break with the Exhibitors	2:30 p.m.
• Cocktails with the Exhibitors	5:00 p.m.
Thursday, August 31	**9:00 a.m. – 3:30 p.m.**
• Break with the Exhibitors	10:10 a.m.
• Break with the Exhibitors	3:00 p.m.

Wednesday, August 30 | 8:00 a.m. - 10:00 a.m.
Monarch IV/V

A Cyber Attack Experience

Simulation of live cyber attacks against emulated DoD-representative systems (sponsored by DoD's **Cyber Red Zone** cyber training activity)

Audience members will get a bird's eye view of actual DoD penetration testers conducting cyber attacks accompanied by explanation of attack goals and methods.

NOT TO BE MISSED!

ABOUT ITEA

The premier professional association of the international test and evaluation community.

For over 40 years, the International Test and Evaluation Association (ITEA), a 501(c)(3) not-for-profit education organization, has been advancing the exchange of technical, programmatic, and acquisition information among the test and evaluation community.

LEARN

- **Specific T&E education and training.**
- **Become certified as a T&E professional.**
- **Maintain a competitive and informational edge.**

SHARE

- **Submit a technical article, case study, or white paper to the ITEA Journal of Test and Evaluation.**
- **Present a relevant topic at a workshop or symposium.**
- **Volunteer.**

ADVANCE

- **Professional growth and networking opportunities.**
- **Become an ITEA leader.**
- **Get recognized within the T&E community.**

www.itea.org

Follow us on LinkedIn

INDIVIDUAL MEMBER BENEFITS

- Receive discounted registration at conferences
- Free registration to our monthly Lunch & Learns and other informative webinars
- Online access to the ITEA Journal of Test & Evaluation each quarter, includes archived copies
- Access to the Corporate Member Directory and Individual members
- Access to past conference proceedings and our online library to include all recorded Lunch & Learns, lecture series, and other webinars

CORPORATE MEMBER BENEFITS

- Five individual memberships for organizations with 50 or more employees
- Three individual memberships for organizations with less than 50 employees
- Listing in the Corporate Capabilities Directory
- Complimentary web link from the ITEA website to yours
- Discounts on exhibit booths, sponsorships, and registrations fees at ITEA events
- Use of Corporate News to gain visibility in the ITEA Journal of Test & Evaluation
- Product Showcase visibility on social media
- Highlighted on social media/LinkedIn

JOIN ITEA

The only Education Association for the Test & Evaluation Community.

MEMBERSHIP FEES

$45	$95	$25
Government	Industry	Students

$800/$1500

Corporate Membership Small/Large Business

PRE-WORKSHOP TUTORIALS

Purchase 2 tutorials and take the CTEP test for FREE!

The fee to attend a 4-hour tutorial is $300 for one or $500 for two.

TUESDAY, AUGUST 29

MORNING TUTORIALS | 8:00 A.M. TO 12:00 P.M.

Cyber Operations Lethality and Effectiveness (COLE) — How to Estimate Cyber Effects for Adversarial Offensive Cyber Operations

Viceroy

Charles Fisher & Kira Lindke, Applied Research Associates, Inc.

The Joint Technical Coordinating Group for Munitions Effectiveness (JTCG/ME) in concert with Applied Research Associates (ARA) will provide a hand-on demonstration of Cyber Operations Lethality and Effectiveness (COLE). COLE is a mission planning tool that enables users to model cyber networks, characterize properties and associated uncertainties, and model the effects of capabilities against those networks. COLE is the only accredited weaponeering and mission planning tool for estimating cyber effects for offensive cyber operations. The application sits on a National Information Exchange Model (NIEM) based data standard and is recognized as the standard for defining cyber networks and capabilities under the official cyber Joint Munitions Effectiveness Manual (JMEM).

COLE's ***Network Characterization*** function allows users to create, manipulate, and share portrayals of network topologies for use in planning Offensive Cyberspace Operations (OCO). Users leverage the best available intelligence to identify node properties and related uncertainties.

COLE's ***Mission Planning*** function enables planners to devise attack options and routes through an adversary's network to meet commander objectives within guidance limitations. Attack options for individual nodes using pre-loaded OCO capabilities and TTPs are rank-ordered by Probability of Effect. Mission Planning outcomes predict the probability of achieving a desired effect against selected target nodes.

Mission planners use COLE to adjudicate attack paths that consider the dynamic state of the target. The COLE State and Functional Models capture changes in the network over time and allows OCO efforts to consider stealth, access, operational impact, and risk when calculating the probability of effect. Further, this allows users to simulate and examine nth order cascading effects of cyber attacks, multiple courses of action, and different weapon-target pairing schemes for execution.

COLE's Principal Investigator will be providing a hands on overview and training of the COLE functions to interested DoD personnel, using COLE's general training version.

Lessons Learned from Safety Science Applicable to Cyberspace Test and Evaluation

Monarch IV

Michael Lilienthal, PhD, CTEP, CPE, EWA-GSI

Several studies and subject matter experts have concluded most cyber breaches are caused by human error. Program managers developing new weapon systems find the human error causal factor very seductive. Unfortunately, fixing only human error symptoms can easily become a continuous fight without identifying and mitigating contributory root causes. Safety engineers who also examine human error as part of accident investigations and hazard analyses repeatedly find complex systems almost always fail in complex ways. Safety engineering objectives dovetail with those of cybersecurity to achieve the goal of a high level of functional safety and cybersecurity resiliency during conception, design, operation, testing and maintenance of cyber-physical systems. The value that the safety science approach adds to cybersecurity is determining why people behaved in the way they did and what weaknesses in the system allowed the breach (loss/accident) to occur. Cybersecurity tests can benefit from the progress safety science has made in its methods of accident investigations and hazard analysis to supplement their analysis of emerging systems for cyber vulnerabilities and cyber survivability.

The tutorial reviews a case study of an actual cyber incident as well as a real world example of a naval incident to provide context for the T&E of a system that includes the human operating subsystem (HOS). Current directives and MIL-STDs for the HOS relevant to cybersecurity will be discussed. Categories of errors users make along with intentional and unintentional violations that contribute to a cybersecurity breach will be discussed. We will discuss how the effects of fatigue, system usability, workload, mental models, training, and the like will alter the cyber vulnerability and resiliency of a SUT. This will provide suggestions for the design and execution of OT&E. Class demonstrations will illustrate aspects of the limitations of human cognition, fatigue, mental models, and memory to reinforce the tutorial. Tools used for aircraft accident investigation and hazard analysis will be presented as potential frameworks to complement cyber resiliency especially in the context of a mission/system of system T&E.

The challenges of evaluating human teaming with autonomous and automated systems for cyber vulnerabilities will be discussed along with other emerging technologies being introduced to the multidomain battlespace.

Mission Based Cyber Risk Assessment (MBCRA) Tutorial and Exercise using the Unified Risk Assessment and Measurement System (URAMS)

Monarch V

William 'Data" Bryant, Technical Fellow, MTSI

Mission Based Cyber Risk Assessments (MBCRA) help set the foundation of good cyber testing by focusing limited test resources on the most significant risks. There are numerous MBCRA approaches available including Cyber Table Tops (CTT) and the Mission-based Risk Assessment Process for Cyber (MRAP-C). The Unified Risk Assessment and Measurement Process (URAMS) is another MBCRA and while it is lighter weight and faster than some methods, many of the principles and techniques use apply broadly across many different MBCRAs.

URAMS starts with an engineering analysis, and our preferred tool is Systems-Theoretic Process Analysis for Security (STPA-Sec). This tool was developed from leveraging the safety analysis work done at MIT and has since been used with great effectiveness across a range of military weapon systems and civilian aerospace systems. STPA-Sec is grounded in systems engineering and is focused on mission-level losses as the true drivers of relevant security design. STPA-Sec also enables analysis of a system's security posture early in the lifecycle, which enables true "baking in" of security.

From the analysis, a set of risk scenarios are developed that are specific to the system under consideration and its expected operating environment. Then, those risk scenarios are scored using any of a wide range of available scoring tools. URAMS scoring tools are characterized first by the model of risk and what factors are assumed to contribute to overall risk, and second by the type of input. Inputs can be provided as single point values, single point values with a confidence, three-point estimates, or 90% confidence intervals. Selection of input type depends on the training and experience of the assessors, as well as how important uncertainty is to the decision makers. While human subject matter experts (SMEs) are utilized as the basis for scoring in URAMS, automated and algorithmic based approaches can and should be used to inform those SMEs.

The risk scenarios can then be combined utilizing a simple Monte Carlo simulation to determine what the overall risk is for a system or portfolio of systems. The ability to combine risk facilitates building a structured assurance case that includes the analyzed mission structure connected to the specific risk scenarios and their scores, which flow up through the mission elements to the overall system. Perhaps most importantly, specific evidence such as testing results, design features, etc., can also be added to the assurance case to validate the risk scores. The assurance case is presented in a format that allows decision makers to rapidly assess whether the scoring is reasonable, based upon their understanding of the mission and the evidence provided.

This tutorial will teach students how to accomplish a URAMS MBCRA by presenting some of the theory behind the approach, showing how to utilize one set of URAMS tools, and providing practical experience by working through portions of a URAMS assessment on a notional aerospace system to include scoring selected risk scenarios.

T&E Fundamentals and Certified Test & Evaluation Professional (CTEP) Foundations

Crescent

Charles 'Chas" McKee, President & CEO, Taverene Analytics LLC

In this high-level short course we will review T&E fundamentals which are covered in the CTEP Foundational exam. We will review the Body of Knowledge (BOK) including the four subject domains used in developing the CTEP program. These will include: Test and Evaluation Planning (Organizational planning, Requirements Analysis, T&E strategy, Evaluation approach, Test Design and Adequacy, T&E Documentation, T&E Cost Management, Contracting for T&E, Specialized Types of testing, planning and resourcing, Risk identification and management, Cyber testing, Modeling and Simulation, Reliability-Availability-Maintainability); T&E Design (Test Adequacy, Scientific Test and analysis techniques, Software Testing); Test and Evaluation Execution (Test Control Management, Data Management, and Test Safety / Certification); and Test Data Analysis, Evaluation and Reporting (Data Verification and Validation, Validation of Test Results, Evaluation, Reporting, Cyber Resilience / Cybersecurity Analysis, Model Validation, and Data Analytics).

Who Should Attend: *Individuals in the T&E community (government and industry, members and non-members) who want to demonstrate their knowledge, skills and abilities in T&E and be recognized by the International Test and Evaluation Association for their professional growth. Requirements for Foundational level CTEP certification should have a Bachelor's degree and 1 year of T&E work experience or an Associates degree and 3 years of relevant T&E work experience or five years of relevant T&E work experience. Please note that the CTEP credential is becoming a 'preferred" requirement in many test engineer job postings.*

TUESDAY, AUGUST 29
AFTERNOON TUTORIALS | 1:00 P.M. TO 5:00 P.M.

5G NR Specification and System Engineering Aspects

Monarch IV

Achilles Kogiantis, PhD, and Ankur Sharma, Peraton Labs

5G wireless cellular networks, based on the 3GPP standard, are being widely deployed in the United States and the rest of the world. 5G is expected to increasingly dominate the worldwide cellular communication market due to its flexibility, wide adoption, and an ever-expanding supplier global ecosystem. The flexible 5G architecture allows multiple networks widely differing in physical, reliability and power characteristics to be supported over a common infrastructure.

This flexibility will be particularly useful to Testing Ranges where subnetworks simultaneously supporting high-bandwidth terrestrial communications, low-power sensors and broadband airborne telemetry systems can be flexibly implemented over a common 5G platform. This tutorial is intended to familiarize the Testing Range professionals with a) the key features of the 5G standards specifications – the basic vision, network architecture, the physical and MAC-layer characteristics of the air-interface, and b) the 5G system engineering aspects of deploying a new private network, dimensioning and planning, and its performance assessment. The first half of the tutorial will discuss the 5G standards specifications, while the second half will cover the 5G systems engineering aspects.

Mission Impact Assessment (MIA) Process

Viceroy

Teresa Barley Merklin, Cyber Fellow, Aeronautics Cyber Range, Lockheed Martin

Mission Impact Assessment (MIA) is a process used to identify and prioritize the mission essential functions of a system. Integrating MIA into the Acquisition and Development lifecycles creates a foundational understanding of cyber resiliency objectives. This process has proven to be valuable during project inception as a mechanism for eliciting meaningful cyber resiliency requirements. It also produces data which is useful for scoring Cyber Risk Assessment. For Cyber Test and Evaluation teams, the MIA process can be used as a basis for test planning as well as scoring the impacts of any findings. This tutorial provides an introduction to the process documented in the MIA Guidebook and a detailed overview of the Use Cases for using the resulting data. Each step of the process is illustrated using a case study.

Test and Evaluation in a Digital Engineering Environment

Crescent

Jean Petty, Cyber Resilience T&E Manager, Department of Homeland Security

This short course / tutorial will review digital engineering concepts in general and then deep dive into specifics for test and evaluation (T&E) in a digital engineering environment. The course will review concepts, methods, tools, and best practices for five Digital Engineering topic areas including models, an authoritative source of truth, technological innovation, innovative infrastructure, and workforce. Each topic area will be addressed in general, followed by discussion of specific issues and challenges for T&E. Discussion areas will include:

- How planning and the evaluation components of T&E need to evolve in the DE environment, given Model Based Systems Engineering, Mission Engineering, and automated testing.
- The characteristics of T&E tools within the DE environment and considerations and methods for automated tools selection.
- Data access, data sharing, and hurdles for building an authoritative source of truth.
- Special concerns for Cyber T&E in a Digital Engineering environment.
- Digital Engineering infrastructure and infrastructure providers.
- T&E workforce within a Digital Engineering ecosystem.
- Gaps in current infrastructure, capabilities, workforce, etc.

Who Should Attend: *This course is intended for T&E professionals who are new to Digital Engineering or are beginning to implement Digital Engineering in their T&E practices. The course will include lecture, discussion, and interactive exercises.*

PLENARY SPEAKERS

Monarch IV/V

Wednesday, August 30 | 8:00 a.m. – 10:00 a.m.

Jeannie Winchester, *PMP, CISSP, Project Manager Cyber, Test, & Training (CT2), U.S. Army Program Executive Office Simulation, Training and Instrumentation (PEO STRI)*
Opening Remarks

Dr. Jonathan Harris, *Lead Cybersecurity Engineer, Naval Air Warfare Center Training Systems Division*
"Live Cyber Attack Experience"

Patrick Lardieri, *Technical Director, National Cyber Range (NCR) Program, Lockheed Martin*
"Live Cyber Attack Experience"

Wednesday, August 30 | 10:30 a.m. – 12:00 p.m.

Mark Dominguez, *Director, Joint Information Operations Range (JIOR), 318th Cyberspace Operations Group*
"Joint Information Operations Range (JIOR) Mission" **[CUI: Distribution C]**

James S. Wells, (SES), *Director, T&E/S&T Directorate, Department of Homeland Security (DHS)*
"DHS T&E Challenges in the Cyber Domain"

Wednesday, August 30 | 1:00 p.m. – 2:30 p.m.

Rebecca Squalls, *Program Manager, National Cyber Range Complex — Unclassified (NCRC-U)*
"The NCRC-U: A Workforce Development Pipeline Strategy"

Sara Estill, *Chief, Information Advantage Division (A), Threat Systems Management Office*
"Information Protection in the Evolving Threat Landscape"

Scan QR code to read speaker bios

Thursday, August 31 | 8:00 a.m. – 10:10 a.m.

Arjuna (AJ) Pathmanathan, *Director, National Cyber Range Complex, Test Resource Management Center (TRMC)*
[CUI: Distribution C]

Chris Collins, *(SES) Executive Director, Developmental Test, Evaluation, and Assessments, Office of the Undersecretary of Defense (Research and Engineering)*
"Tomorrow's Cyber T&E Initiatives...Today"

Tom Walrond, *Cyber Advisor to Deputy Director for Strategic Initiatives, Policy & Emerging Technologies, Office of the Director, Operational Test and Evaluation, Office of the Secretary of Defense*
"Transforming T&E to Support the Joint Force in Multi Domain Operations"

Thursday, August 31 | 10:30 a.m. – 12:00 p.m.

Panel Discussion on Cyber T&E of Generative AI Systems

Moderator:

Nilo Thomas, *Software & Cyber Advisor to Deputy Director for Strategic Initiatives, Policy and Emerging Technologies, Office of the Director, Operational Test and Evaluation, Office of the Secretary of Defense*

Panelists:

Spencer Andrus, *Customer Engineer, Google Public Sector*

Joseph F. Bradley Jr., *(SES) Cyber Resiliency Office for Weapon Systems (CROWS) and the Director of Engineering and Technical Management, Air Force Life Cycle Management Center*

Dr. Jayashree (Jai) Harikumar, *Chief, Cyberspace Emerging Technologies and Integration Branch, U.S. Army Combat Capabilities Development Command (DEVCOM) Analysis Center*

Dr. Timothy Kelley, *Scientist, Naval Surface Warfare Center Crane Division*

Thursday, August 31 | 3:30 p.m. – 5:00 p.m.

Dr. Mike Shields, *Chief Scientist for the TRMC T&E/S&T Cyberspace Test Technology (CTT)*
Closing Keynote

AGENDA
Wednesday, August 30

Monarch IV/V

Opening & Plenary Speakers

8:00 a.m. Opening Ceremony
Presentation of Colors
National Anthem
Welcome
Erwin Sabile, Booz Allen Hamilton
Workshop Chair

8:20 a.m. Opening Remarks
Jeannie Winchester, PMP, CISSP
Project Manager Cyber, Test, and Training (CT2), U.S. Army Program Executive Office Simulation, Training and Instrumentation (PEO STRI)

8:35 a.m. ***"Live Cyber Attack Experience"***
Dr. Jonathan Harris
Lead Cybersecurity Engineer, Naval Air Warfare Center Training Systems Division

Patrick Lardieri
Technical Director, National Cyber Range (NCR) Program, Lockheed Martin

10:00 a.m. BREAK WITH THE EXHIBITORS

10:30 a.m. **Mark Dominguez**
Director, Joint Information Operations Range (JIOR), 318th Cyberspace Operations Group
"Joint Information Operations Range (JIOR) Mission" **[CUI: Distribution C]**

11:15 a.m. **James S. Wells (SES)**
Director, T&E/ S&T Directorate, Department of Homeland Security(DHS)
"DHS T&E Challenges in the Cyber Domain"

12:00 p.m. LUNCH

1:00 p.m. **Rebecca Squalls**
Program Manager, National Cyber Range Complex-Unclassified (NCRC-U)
"The NCRC-U: A Workforce Development Pipeline Strategy"

1:45 p.m. **Sara Estill**
Chief, Information Advantage Division (A), Threat Systems Management Office
"Information Protection in the Evolving Threat Landscape"

2:30 p.m. BREAK WITH THE EXHIBITORS

3:00 p.m. Technical Sessions

SESSION 1: Cyberspace Test Technology

Viceroy

Chair: **Dr. Mike Shields**, Chief Scientist for the TRMC T&E/S&T Cyberspace Test Technology (CTT)

Start Time:	**3:00 p.m.**
Presenter(s):	Steve Durst, R&D Engineer, Skaion Corporation
Presentation:	*Activity and Content Enhancement — Next Gen Traffic Generation Toolkit*
Start Time:	**3:30 p.m.**
Presenter(s):	Arch Owen, Program Manager for Weapon Security, Draper Laboratory
Presentation:	*Vader Modular Fuzzer (VMF) — USG Fuzzing Capability*
Start Time:	**4:00 p.m.**
Presenter(s):	Dr. Donald Pellegrino, CEO, DeciSym, LLC
Presentation:	*Measure and Share: TRMC T&E/S&T Cyberspace Test Technology's Project to Improve Cyber T&E Impacts Across DoD*
Start Time:	**4:30 p.m.**
Presenter(s):	Arch Owen, Program Manager for Weapon Security, Draper Laboratory
Presentation:	*Extensible QEMU for Broader Emulation Functionality and Application*

SESSION 2: Cyber Resilience Requirements

Crescent

Chair: **Jean Petty**, Cyber Resilience T&E Manager, Department of Homeland Security

Start Time: **3:00 p.m.**

Presenter(s): Timothy Fitzgerald, Cybersecurity Assessments Flight Director, 346th Test Squadron

Presentation: *Lessons Learned from Conducting Operational Cyber Testing for Mission Resilience*

Start Time: **3:30 p.m.**

Presenter(s): Djenana Compara, President, KDM Analytics

Presentation: *Automated Risk Assessment Process for DoD, DHS, & Other Agencies*

Start Time: **4:00 p.m.**

Presenter(s): Dr. Keith F. Joiner, Senior Lecturer Test, Evaluation and Aircraft Design

Presentation: *Australian Update on Cybersecurity of Critical Infrastructure: Governance Challenges and Approaches*

Start Time: **4:30 p.m.**

Presenter(s): Dr. Peter A. Beling, Director, Intelligent Systems Division, Virginia Tech National Security Institute

Presentation: *Test and Evaluation of Cyber Resilience using the Framework for Operational Resilience in Engineering and Systems Test*

SESSION 3: Cyber & Spectrum Warfare Considerations in 5G/6G

Monarch III

Chair: **Patrick Lardieri**, Technical Director, National Cyber Range (NCR) Program, Lockheed Martin

Start Time: **3:00 p.m.**

Presenter(s): LTCol Ben Pimentel, PhD, USMC

Presentation: *5G / FutureG Technology to Meet DoD Challenges*

Start Time: **3:30 p.m.**

Presenter(s): Jorge Laurel, NSA Cybersecurity Collaboration Center

Presentation: *Cyber Threats and/or Technology Robustness*

SESSION 3: continued

Monarch III

Start Time: **4:00 p.m.**

Presenter(s): Connor Bruso, Lockheed Martin Cyber & Intelligence

Presentation: *T&E Methods and Tools that Enable Assessment of the Operational Resilience of 5G Enabled Systems to Cyber and Spectrum Threats*

Start Time: **4:30 p.m.**

Presenter(s): Yong Zhou, Keysight Technologies

Presentation: *5G Security Assurance Specifications*

SESSION 4: Cyber T&E of Generative AI Systems

Monarch IV/V

Chairs: **Dan Rieken**, American Systems Corporation & **Dr. Natalie Kautz**, MITRE

Start Time: **3:00 p.m.**

Presenter(s): Josh Harguess, PhD, Department Manager, AI Security and Perception, MITRE

Presentation: *Securing the Attack Surface of AI Enabled Systems*

Start Time: **3:30 p.m.**

Presenter(s): Spencer Andrus, Customer Engineer, Google Public Sector

Presentation: *Supercharging Security with Generative AI*

Start Time: **4:00 p.m.**

Presenter(s): Ryan Ashley, Senior Software Engineer, IQT Labs

Presentation: *Auditing ML Collection Hardware*

Start Time: **4:30 p.m.**

Presenter(s): Dr. Timothy Kelley, Scientist, Naval Surface Warfare Center Crane Division

Presentation: *Opening the Door to the Mind's Eye: Cognitive Science, Cybersecurity, and Interfaces in ML Testing*

5:00 p.m. COCKTAIL HOUR WITH THE EXHIBITORS

Scan QR code to read Technical Abstract Descriptions

AGENDA
Thursday, August 31

Monarch IV/V

Plenary Speakers

8:00 a.m. Welcome to Day 2
Scott Bisciotti
Command Post Technologies
Technical Chair

8:10 a.m. **Arjuna (AJ) Pathmanathan**
Director, National Cyber Range Complex, Test Resource Management Center (TRMC) **[CUI: Distribution C]**

8:50 a.m. **Chris Collins, (SES)**
Executive Director, Developmental Test, Evaluation, and Assessments, Office of the Undersecretary of Defense (Research & Engineering)
"Tomorrow's Cyber T&E Initiatives... Today"

9:30 a.m. **Tom Walrond**
Cyber Advisor to Deputy Director for Strategic Initiatives, Policy & Emerging Technologies, Office of the Director, Operational Test and Evaluation, Office of the Secretary of Defense
"Transforming T&E to Support the Joint Force in Multi Domain Operations"

10:10 a.m. BREAK WITH THE EXHIBITORS

10:30 a.m. ***Panel: "Cyber T&E of Generative AI Systems"***
Moderator: Nilo Thomas, Software & Cyber Advisor to Deputy Director for Strategic Initiatives, Policy and Emerging Technologies, Office of the Director, Operational Test and Evaluation, Office of the Secretary of Defense

Panelists: Spencer Andrus, Customer Engineer, Google Public Sector

Joseph F. Bradley Jr., (SES) Cyber Resiliency Office for Weapon Systems (CROWS) and the Director of Engineering and Technical Management, Air Force Life Cycle Management Center

Dr. Jayashree (Jai) Harikumar, Chief, Cyberspace Emerging Technologies and Integration Branch, U.S. Army Combat Capabilities Development Command (DEVCOM) Analysis Center

Dr. Timothy Kelley, Scientist, Naval Surface Warfare Center Crane Division

12:00 p.m. LUNCH

1:00 p.m. Technical Sessions

SESSION 5: New Cyber DoD Manual and DoD 5000.89 Cyber Policy Brief and Cyber in DEVSECOPS

Monarch IV/V

Chair: **Tom Walrond**, Office of the Director, Operational Test and Evaluation, OSD

Start Time: **1:00 p.m.**
Presenter(s): Nilo Thomas, Software & Cyber Advisor to Deputy Director for Strategic Initiatives, Policy and Emerging Technologies, Office of the Director, Operational Test and Evaluation, Office of the Secretary of Defense
Presentation: *U.S. Department of Defense (DoD) Joint Cyber T&E Policy and Guidance—What's New?*

Start Time: **2:00 p.m.**
Presenter(s): Tim Chase & Pat Quilter, STAT COE/ALPI
Presentation: *Cybersecurity in DevSecOps—How to Test for Security in a Fast-Paced Development Environment*

SESSION 6: Test Automation and AI

Monarch III

Chair: **Mickey Rhodes**, Cyber Test Engineer, Booz Allen Hamilton

Start Time: **1:00 p.m.**
Presenter(s): Jenn Bergstrom, CTO, Mission Solutions Sector, Parsons
Presentation: *Incorporating Chaos Experiments into Automated Pipelines*

Start Time: **1:30 p.m.**
Presenter(s): Michael D. Brown, Principal Security Researcher, Trail of Bits, Inc.
Presentation: *Using Graph-Based Machine Learning Algorithms for Software Analysis*

Start Time: **2:00 p.m.**
Presenter(s): William D. Bryant, Technical Fellow, MTSI
Presentation: *Humans vs. Robots: Structuring Mission Based Cyber Risk Assessment (MBCRA) Inputs*

Start Time: **2:30 p.m.**
Presenter(s): Matt Lembright, Director of Federal Applications, Censys
Presentation: *Proactive Threat Hunting — Getting Left of Boom*

SESSION 7: Tomorrow’s Cyber Solutions.... Today

Viceroy

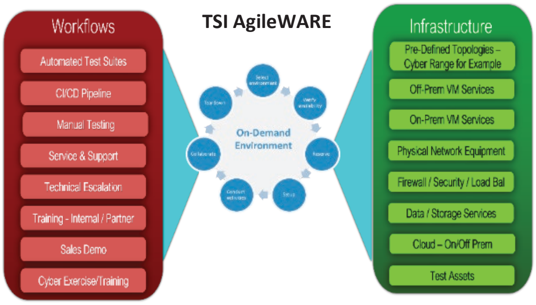
Chair: **Dr. Peter A. Beling**, Director, Intelligent Systems Division, Virginia Tech National Security Institute

Start Time: **1:00 p.m.**
Presenter(s): Nisha Patel, Software Engineer, Trideum Corporation
Presentation: *Cyber Table Top Toolset (CT3) Demonstration* **[CUI: Distribution C]**

Start Time: **1:30 p.m.**
Presenter(s): Zach Collier, Assistant Professor, Department of Management, Radford University
Presentation: *Risks and Opportunities for AI in Managing Disruptions to Hardware Supply Chains*

Start Time: **2:00 p.m.**
Presenter(s): Stephen Adams, Assistant Director, Intelligent Systems Division, Virginia Tech National Security Institute
Presentation: *Physically Unclonable Functions (PUFs) Using Protein-Self-Assembly and Deep Neural Networks*

Start Time: **2:30 p.m.**
Presenter(s): Dr. Sachin Shetty, ODU
Presentation: *Cyber Risk Scoring and Mitigation for Resilient Cyber Infrastructure*



SESSION 8: Cyber Automated Tools & Test

Crescent

Chair: **Eugene Costello**, Cybersecurity Director, OPTEVFOR

Start Time: **1:00 p.m.**
Presenter(s): Josh Young, AFRL ITEC Pen Test Lead, Booz Allen Hamilton
Presentation: *AFRL ITEC Pen Test Capability Brief* **[CUI: Distribution C]**

Start Time: **1:30 p.m.**
Presenter(s): Grant Willey, Information Systems Security Officer, Geeks and Nerds (GaN) Corporation
Presentation: *## Wave Function Collapse Algorithm for Automatic Design of Secure Networks*

Start Time: **2:00 p.m.**
Presenter(s): Jason Schalow, Chief, Special Missions Flight, 412th, Communications Squadron, Edwards AFB
Presentation: *Cybersecurity and the Rise of AI: Risks and Opportunities*

Start Time: **2:30 p.m.**
Presenter(s): Dan Turner, Booz Allen Hamilton
Presentation: *Building Automation System (BAS) An Industrial Control System Focused Security*

3:00 p.m. BREAK WITH EXHIBITORS

Monarch IV/V

3:30 p.m. Closing Keynote
Dr. Mike Shields
Chief Scientist for the TRMC T&E/S&T Cyberspace Test Technology (CTT)

5:00 p.m. Workshop Concludes

ACCELERATE

Digital Risk Assessment at Industrial Scale for OT & IT Systems

Achieving Resiliency & Survivability through Automation

- Systematic & Comprehensive Risk Assessment
- Risk Prioritization, Mitigation and Reporting
- Enhancement to Digital Engineering Framework
- Reduce Risk Assessment Time and Cost by 80%

KDMAnalytics
kdmanalytics.com

ACQUIRED DATA SOLUTIONS
acquiredata.com

VISIT US AT
BOOTH 1
FOR A DEMO

CPT COMMAND POST TECHNOLOGIES

Scan Here to Learn more About How CPT is working to Protect You from the Most complex Global Threats

01

DESIGN

Develop architectures, designs, and strategic roadmaps for enterprise IT systems. CPT continually evaluates new hardware, software, and technology to deliver integrated operational systems and components in a secure and efficient environment.

02

OPERATE

Maintain confidentiality, integrity, and availability Network Operations Security Centers (NOSC) on a 24/7/365 basis. We engineer, secure, and support Cyber mission rehearsals, Tactics development, R&D, demonstrations, and persistent environments for Combatant Commands, Services, Agencies, and Foreign Partners.

03

SECURE

Secure infrastructure through Risk Management Framework (RMF) security life cycle activities, 24/7/365 network monitoring, compliance auditing; and enterprise patch management, in accordance with Accreditation and Authorizing Official guidelines.

04

DEFEND

Defend operational environments from real-world adversarial exploitations. Our teams isolate and mitigate cyber threats to allow IT systems to promptly return to normal operations. We provide rapid remediation for emerging cyber threats.

The ITEA JOURNAL OF TEST AND EVALUATION

NOW ONLINE! www.itea.org

Themes for 2023 / 2024

Test the Way We Operate – Best Practices and Lesson Learned
June 2023 (Volume 44 / Issue 2)
Manuscript Deadline: **March 1, 2023**

DATAWorks Special Issue
September 2023 (Volume 44 / Issue 3)
Manuscript Deadline: **May 15, 2023**

T&E for Emerging Technologies
December 2023 (Volume 44 / Issue 4)
Manuscript Deadline: **September 1, 2023**

T&E for AI Enabled Systems
March 2024 (Volume 45 / Issue 1)
Manuscript Deadline: **December 1, 2023**

2023 EXHIBITORS

Acquired Data Solutions (ADS) Booth 1

Rockville, MD www.acquiredata.com

Acquired Data Solutions (ADS) is an engineering company and a certified small business. We have over 25 years' experience providing technology solutions for the engineering life cycle to industry and government agencies. Our expertise spans across cybersecurity, test automation, engineering integration, and data analytics.

Our cybersecurity and test automation design and development skills, gives us a clear understanding of the importance of securing organizations operational technology (OT) from prototype to delivery. With our partner KDM Analytics, Inc., the developer of the award-winning risk assessment product suite, we help organization save time, save money, and focus their cyber risk-assessment resources. KDM's solution brings together top-down risk analysis with bottom-up vulnerability analysis for faster, more targeted cyber risk mitigation and protection planning.

Geeks and Nerds (GaN) Booth 4

Huntsville, AL www. geeksandnerds.com

Geeks and Nerds (GaN) is an innovative solution developer. Our motto, Innovate with Purpose™, succinctly defines our commitment to provide solutions and services that positively impact our community and national security. Our innovation encompasses the entire spectrum of engineering and science including research, development, testing, evaluation, and training.

Technical Systems Integrators, Inc. (TSI) Booth 5

Maitland, FL www.tsieda.com

TSI Cyber Range as a Service® (CRaaS)

TSI's CRaaS is an industry leading automation and orchestration framework for the deployment and consumption of cyber training and exercise environments and workflows. The environments may include virtual/physical assets, legacy, future, and proprietary technologies in our 'Sandbox'. DELIVERING YOUR TECHNOLOGY 'as a Service'!

See Map on page 3 for Exhibitor locations.

ITEA IS EDUCATION

Reach your goal and gain your Professional Education Units

Short Courses

- Cybersecurity and Information Assurance
- DOE/Advanced Design of Experiments
- Fundamentals of Test & Evaluation
- Program Management and Systems Engineering
- STAT/Scientific Test and Analysis Techniques

Tutorials

- A Process for Distributed LVC in T&E
- Introduction to Cyber Resilience T&E
- T&E as a Part of Agile Development
- T&E in a Digital Engineering Environment
- TRMC Solutions for Test and Training

Webinars

- Adaptive Relevant Testing: Accelerating US Air Force Combat Capabilities
- Best Practices for Addressing New Challenges in Testing and Evaluating Artificial Intelligence Enabled Systems
- Interoperability T&E
- T&E in a Digital Engineering Environment
- Test & Evaluation in a Digital Engineering Enabled World

ONLINE | VIRTUAL | IN-PERSON
Find us on SAM.GOV

The above are examples of ITEA offerings.

CYBER RED ZONE

The mission of Cyber Red Zone (CRZ) is to train the cybersecurity workforce in an engaging way, focusing on team collaboration, knowledge transfer and skill acquisition. This event achieves this mission by developing an environment with specific cyber attack vectors based on relevant DoD needs (collected from Cyber-XSWG senior leaders). Its purpose is to provide the participants of CRZ an opportunity to explore and experiment with various cyber attacks against the most current threat vectors identified by senior leaders.

Join us at the CRZ 24-1 event that will be held from 2 Oct to 17 Nov 2023 with 11 two-day sessions and 5 participant slots within each session (i.e., 55 slots available). The CRZ environment will be provided by the National Cyber Range Complex in Orlando, FL. CRZ will be an unclassified event, protected at the secret level. Players can remotely access CRZ from either a JIOR or JMN site or can make arrangements to participate locally from NCRC sites in Orlando, Charleston, or Pax River. Remote sites will be added to the ISA and participation cannot occur without the appropriate AO's signature approving connectivity.

Previous CRZs have included Cyber Protection Teams, Mission Defense Teams, red teams, academy and university teams, security operations centers, and cyber test & evaluation teams. While the event will be held at CUI, all participants must have at least a secret clearance.

Thanks to Cyber Red Zone for conducting the hands-on Cyber Attack Demonstration at this ITEA workshop!

The mission of Cyber Red Zone (CRZ) is to train the cybersecurity workforce in an engaging way, focusing on team collaboration, knowledge transfer and skill acquisition.

CYBER RED ZONE 24-1 EVENT

October 2 – November 17, 2023

National Cyber Range Complex | Orlando, FL

Join us at the CRZ 24-1 event that will be held from 2 Oct to 17 Nov 2023 with 11 two-day sessions and 5 participant slots within each session (i.e., 55 slots available). The CRZ environment will be provided by the National Cyber Range Complex in Orlando, FL.

CYBER RED ZONE 24-1 EVENT

October 2 – November 17, 2023

What is CRZ?

CRZ follows an OCO/pentest-style CTF with a number of flags that need to be found and a hint system that, while reducing possible points available, may give players clues as to how to find the flag. Flags will be unveiled in a campaign format where there is an overall endpoint goal with points awarded along the way to reach that goal. Thus, all of the flags will not be available at the beginning of the event. An intel document will be provided to players prior to the beginning of the event. A standardized virtual fly-away kit will be provided for players which will be described in the intel document. For trusted agents and non-player stakeholders, a document describing the knowledge, skills, and abilities (KSAs) for each flag will be made available. Players who complete the event will be eligible for a participation certificate from the Test Resource Management Center for 16 hours of continuous learning credit.

Player objectives:

- Degrade, deny, deceive, and destroy identified resources within the operational space of the CTF.
- Provide for the execution of implanted agent operations through the introduction of tooling and compromise of specific information systems
- Exfiltrate key information of interest for future operations
- Complete nine primary objectives ensuring successful degradation of opposing force
- Find other opportunities to collect cyber intelligence and increase a team's score. (Easter Eggs)

Key contacts:

Event User: Dr. Jonathan Harris, Naval Air Warfare Center Training Systems Division (NAWCTSD) – Jonathan.T.Harris.civ@us.navy.mil

Event Director: Dr. David "Fuzzy" Wells, National Cyber Range Complex (NCRC) - fuzzywells@mitre.org

Event Designer: Mr. Daniel Seeman, National Cyber Range Complex - Orlando

Event Lead: Mr. Adler Clesca, National Cyber Range Complex - Orlando