NDIA Cyber Physical Systems Security Summit Agenda

June 16, 2026 (Day 1)

Time	Topic	Speaker
8:00a	**CHECK IN & BREAKFAST**	
9:00a	Opening Remarks	• Dariusz Mikulski, Ph.D., Co-Chair, NDIA-MI CPS3 • Jennifer Tisdale, Co-Chair, NDIA-MI CPS3
9:05a	**Keynote: Designing for Compromise: Building Resilient Acquisition Programs in a Contested Ecosystem** In 2021, a ransomware attack on the Colonial Pipeline didn't target a weapon system. It targeted one node in a sociotechnical ecosystem — and the cascade did the rest. That is the operating environment for every defense acquisition program today. Drawing on doctoral research in cyber resilience and direct experience acquiring unmanned systems in contested trilateral environments, this talk argues that building secure systems is not enough. We must build programs — and program office cultures — that operate effectively despite compromise	• Ryan Hilger, Ph.D., Principal Program Manager, US Navy
9:30a	Fireside Chat with Dr. Ryan Hilger	• Ryan Hilger, Ph.D., Principal Program Manager, US Navy • Dariusz Mikulski, Ph.D., Lead Research Scientist, US Army DEVCOM GVSC (moderator) • Jennifer Tisdale, Director, NDIA Michigan (moderator)
10:15a	**MORNING BREAK**	
10:35a	**Capture-The-Flag: Introduction**	• Sophia Kraus, Cyber Engineer, GDLS
10:40a	**Iranian Responses to Operation Epic Fury** This presentation outlines the escalating cyber conflict resulting from the joint U.S.-Israeli "Operation Epic Fury," detailing Iran's multi-faceted response, code-named "Operation True Promise," and its role in sparking a broader trans-regional conflict. It analyzes the real-world impacts of this retaliatory campaign, focusing on a sustained series of cyber attacks targeting critical infrastructure—including financial institutions, energy facilities, and water systems throughout the Middle East. Additionally, it examines the evolving tactics of state-sponsored threat actors, specifically their strategic deployment of destructive wiper malware, and reviews proactive defensive measures required to counter these advanced persistent threats.	• John Doyle, Director of CTI Services, Palo Alto Networks Unit 42
11:05a	**The New Frontline: Foreign Proximity Threats to Critical Military and Civilian Assets** This panel will analyze novel threat vectors that exemplify "gray-zone" conflict—state-sponsored hostile acts that fall below the threshold of armed conflict. It will focus on how physical proximity to sensitive locations is exploited as a primary vulnerability, such as foreign-controlled commercial operations near military bases being used for espionage or electronic warfare. The discussion will cover how to identify,	• Tim Waters, Global Security Director & CISO, GDLS (moderator) • Rich Foran, Special Agent, FBI Detroit Cyber Task Force • COL (ret) David Spehar, Former Deputy Wing Commander – 127th Wing, US Air Force • Luke Dembosky, Partner, Debevoise & Plimpton

	deter, and respond to these ambiguous threats and prevent them from being used for espionage, sabotage, or as launchpads for kinetic attacks.	
12:00p	**LUNCH**	
1:00p	**Towards Automating Firmware Testing (and how AI can help)** Firmware sits at the boundary between software and the physical world, making testing embedded and cyber-physical systems both critical and uniquely challenging. Automating that testing can reveal bugs earlier, improve repeatability, and scale security analysis beyond what manual workflows can realistically cover. This talk will explore practical approaches to firmware testing, with an emphasis on both traditional methods and new AI techniques that can be applied across a range of targets including unmanned systems, vehicles, industrial devices, sensors, controllers, and other embedded platforms.	• Ryan Chow, Co-Founder & CEO, Metalware • Zion Basque, Ph.D., Research Fellow, Metalware
1:25p	**AI-Driven Warfare: Countering the Rise of Autonomous Cyberattacks** With AI now able to independently find and exploit vulnerabilities, this panel will address the paradigm shift in cyber conflict. Experts will discuss the first documented large-scale AI-driven cyberattack and debate defensive strategies, including the use of defensive AI agents and the ethics of autonomous cyber response. The discussion will also cover new frameworks for continuously testing and hardening systems against AI-powered threats.	• Dariusz Mikulski, Ph.D., Lead Research Scientist, US Army DEVCOM GVSC (moderator) • Jon Smereka, Ph.D., STE (Robotics), US Army DEVCOM GVSC • Matt Carpenter, Cyber Reverse Engineer, ICR.Inc. • Rachelle Putnam, VP & CIO, GDLS
2:20p	**AFTERNOON BREAK**	
2:45p	**The Invisible Battlefield: Novel Tracking and Infiltration Techniques** This session will cover two emerging threats: the exploitation of ubiquitous remote access tools by cybercriminals and the use of new technologies, like Wi-Fi sensing, to physically track individuals. Experts will discuss how these evolving vectors can be combined to compromise both digital networks and the physical security of key personnel.	• Joe Gothamy, Branch Chief, US Army DEVCOM GVSC (moderator) • Chuck Brokish, Director, Green Hills Software • Tim Brom, Principle Consultant, Vernda • COL (ret) Raymond Stemitz, CIO/G6, Michigan Army National Guard • Ronald Kraus, Cyber Specialist, Michigan State Police Information Technology Division
3:35p	**Patching and Assurance for Trusted Cybersecure Hardened Libraries and Binaries** Post-quantum computing poses significant risks to cryptographic protocols used in military ground vehicle systems, making modernization essential for operational resilience. New research by SwRI addresses the challenge of leveraging DARPA's Assured Micro-Patching (AMP) program tools to upgrade legacy software systems without source code access, with the goal of integrating quantum-secure algorithms like AES-256 and Module Lattice-based Key Encapsulation Mechanism (ML-KEM). Using advanced reverse engineering techniques, cryptographic vulnerabilities in classical methods such as AES-128 are being addressed, ensuring compatibility with post-quantum systems while maintaining original functionality. Testing is ongoing to demonstrate the effectiveness of modular solutions for embedded binaries, providing enhanced	• Cameron Mott, Ph.D., Cybersecurity Manager, SwRI

	security and performance to embedded controllers regardless of access to the original source code.	
4:00p	**AUVSI Trusted Cyber UGV Certification Program** As ground-based robotic and autonomous systems move from experimentation to fielding in both the military and civilian sectors, cyber resilience of these systems is becoming increasingly critical. To that end, AUVSI has launched the Trusted Cyber UGV Certification Program, allowing vehicle providers to be evaluated against a common set of requirements. In this talk, Neya Systems will discuss our role in leading the industry working group, the process that was used to develop the four Trusted Cyber Framework documents, and the function of the corresponding Implementation Guides.	• Dakota Myers, Cybersecurity Engineer, Neya
4:25p	**Introduction to SAE J1939-91C: A Method to Defend In-Vehicle Network Communications** The new SAE J1939-91C standard defines cybersecurity methods of Network formation, Rekeying, and Secure Message Exchange between in-vehicle Electronic Control Units (ECUs). The SAE J1939-91C network security protocol operates over a CAN-FD network to perform cryptographic operations such as key generation. This presentation will provide an overview of the standard and an example implementation. Also, in order to evaluate network performance, test vectors will be described for validating SAE J1939-91C cybersecurity methods and message exchanges.	• Mark Zachos, President, DG Technologies
4:50p	Wrap Up and Closing Remarks	• Dariusz Mikulski, Ph.D., Co-Chair, NDIA-MI CPS3 • Jennifer Tisdale, Co-Chair, NDIA-MI CPS3
5:00p	**ADJOURN**	

June 17, 2026 (Day 2)

Time	Topic	Speaker
8:00a	**CHECK IN & BREAKFAST**	
9:00a	Opening Remarks	• Dariusz Mikulski, Ph.D., Co-Chair, NDIA-MI CPS3 • Jennifer Tisdale, Co-Chair, NDIA-MI CPS3
9:05a	**Keynote Panel: Forging an Integrated Cyber Strategy: Aligning Federal Ambition with State-Level Action** This panel will dissect the challenges of creating a cohesive integrated cybersecurity strategy that can effectively counter modern threats. The discussion will explore how to bridge the gap between federal and state authorities while also ensuring the integrated strategy provides clear protocols for responding to gray-zone cyber operations that fall below the traditional threshold of armed conflict. Experts will debate how to define a unified policy framework that is strong enough to deter state actors yet flexible enough to adapt to local needs and ambiguous threats.	• Mike Stone, Partner, Warner Norcross + Judd LLP (moderator) • Rob Blackwell, CEO & President, Blackwell Strategic Group • Cheri Caddy, Senior Cybersecurity Advisor, Savannah River National Laboratory • Jeff McLeod, Senior Manager (Strategy, Growth, & Transformation), Deloitte Consulting LLP
10:15a	**MORNING BREAK**	

10:35a	**CMMC Hacks for Faster, Cheaper Compliance** This 30 minute session provides a clear overview of the differences between CMMC Level 1 self attestation and a third party CMMC Level 2 certification, as well as the important distinction between being compliant and being certified. Join Maureen Miller, Senior Procurement Specialist with the Macomb Regional APEX Accelerator, as she highlights no cost tools and support services—including Project Spectrum, the CyberAB, and APEX Accelerator assistance—that can help organizations within the Defense Industrial Base manage requirements outlined in FAR Clause 52.204 21 while minimizing expenses. Designed for both newcomers and established contractors, this session offers practical strategies to prepare for CMMC efficiently and cost effectively.	• Maureen Miller, Senior Procurement Specialist, Macomb Regional APEX Accelerator
11:05a	**The COTS Mandate – Threat or Opportunity for Cyber-Physical System Security?** Executive Order 14271's 'COTS-First' directive presents a fundamental dilemma for the security of our nation's cyber-physical infrastructure. Does this policy accelerate modernization, or does it introduce unacceptable risks by relying on third-party code? This panel will feature a candid discussion on the security vulnerabilities, integration challenges, and potential benefits of shifting away from bespoke government systems toward commercially available solutions.	• Jennifer Tisdale, Director, NDIA Michigan (moderator) • Maggie Shipman, SwRI, • John Sheehy, Senior VP for Research & Strategy, IOActive, • Dan Zajac, Product Security, Ford
12:00p	**LUNCH**	
1:00p	**How to Partner with the Army Research Office** This presentation is a critical opportunity for small R&D businesses to gain a competitive advantage by learning how to partner with the DEVCOM Army Research Office (ARO). Dr. Paul Yu will discuss research areas the ARO Information Assurance program is currently prioritizing, giving you direct insight into future needs. Following his overview, Ms. Steffanie Burgos will provide a practical guide to the DoW's Small Business Innovation Research (SBIR) and Small Business Technology Transfer (STTR) programs, explaining how your business can plug into these programs to secure funding and become a key partner in developing next-generation technology for our soldiers.	• Paul Yu, Ph.D., Program Manager (IA), US Army DEVCOM ARO • Steffanie Burgos, Program Manager, US Army DEVCOM ARO
1:25p	**Breaking the Code: How CTF Winners Think** Ever wonder how CTF winners actually solve those "impossible" challenges? In this panel, top competitors will revisit standout problems from the competition and explain their thought process step by step. From first glance to final solve, they'll share how they approached each challenge, what clues mattered, and where things got tricky. Whether you are new to CTFs or a seasoned player, you'll walk away with practical techniques and new ways to think about solving problems.	• Sophia Kraus, Cyber Engineer, GDLS (moderator) • Winners of the 2026 CPS3 CTF
2:15p	Wrap Up and Closing Remarks	• Dariusz Mikulski, Ph.D., Co-Chair, NDIA-MI CPS3 • Jennifer Tisdale, Co-Chair, NDIA-MI CPS3
2:30p	**ADJOURN**	