NDIA Cyber Physical Systems Security Summit Agenda

NOTE: Final times for speakers and panelists will be provided closer to the event. More speakers and panels are still expected to be added to the agenda. For questions, please contact cyber@ndia-mich.org .

DAY 1 (June 16, 2026)

Designing for Compromise: Building Resilient Acquisition Programs in a Contested Ecosystem

Keynote: Ryan Hilger, Ph.D., Principal Program Manager, US Navy

Description: 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

Panel: The New Frontline: Foreign Proximity Threats to Critical Military and Civilian Assets

Moderator: Tim Waters, Global Security Director & CISO, GDLS

Speakers:

- Andy Sczygielski, Detroit FBI Cyber Task Force,
- David Spehar, Former Deputy Wing Commander - 127th Wing, US Air Force
- Luke Dembosky, Partner, Debevoise & Plimpton

Description: 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, deter, and respond to these ambiguous threats and prevent them from being used for espionage, sabotage, or as launchpads for kinetic attacks.

Panel: AI-Driven Warfare: Countering the Rise of Autonomous Cyberattacks

Moderator: Dariusz Mikulski, Ph.D., Lead Research Scientist, US Army DEVCOM GVSC

Speakers:

- Jon Smereka, Ph.D., STE (Robotics), US Army DEVCOM GVSC
- Matt Carpenter, Cyber Reverse Engineer, ICR.Inc.
- Rachelle Putnam, VP & CIO, GDLS

Description: 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.

Panel: The Invisible Battlefield: Novel Tracking and Infiltration Techniques

Moderator: Joe Gothamy, Branch Chief, US Army DEVCOM GVSC

Speakers:

- Chuck Brokish, VP, Green Hills Software
- Tim Brom, Principle Consultant, Vernda
- COL (ret) Raymond Stemitz, CIO/G6, Michigan Army National Guard

Description: 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.

Talk: Patching and Assurance for Trusted Cybersecure Hardened Libraries and Binaries

Speakers: Cameron Mott, Ph.D., Cybersecurity Manager, SwRI

Description: 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 Micropatching Program (AMP) 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 security and performance to embedded controllers regardless of access to the original source code.

Talk: Introduction to SAE J1939-91C: A Method to Defend In-Vehicle Network Communications

Speakers: Mark Zachos, President, DG Technologies

Description: 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.

DAY 2 (June 17, 2026)

Keynote Panel: Forging an Integrated Cyber Strategy: Aligning Federal Ambition with State-Level Action

Moderator: Mike Stone, Partner, Warner Norcross + Judd LLP

Speakers:

- Rob Blackwell, CEO & President, Blackwell Strategic Group
- Cheri Caddy, Senior Cybersecurity Advisor, Savannah River National Laboratory

Description: 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.

Talk: CMMC Hacks for Faster, Cheaper Compliance

Speakers: Maureen Miller, Senior Procurement Specialist, Macomb Regional APEX Accelerator

Description: 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.

Panel: The COTS Mandate – Threat or Opportunity for Cyber-Physical System Security?

Moderator: Jennifer Tisdale, Director, NDIA Michigan

Speakers:

- Maggie Shipman, SwRI,
- John Sheehy, COO, IOActive,
- Dan Zajac, Product Security, Ford

Description: 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.

Breaking the Code: How CTF Winners Think

Moderator: Sophia Kraus

Description: 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.