U.S. ARMY COMBAT CAPABILITIES DEVELOPMENT COMMAND GROUND VEHICLE SYSTEMS CENTER

MDEX 2021 and Detroit Arsenal Opportunities Conference

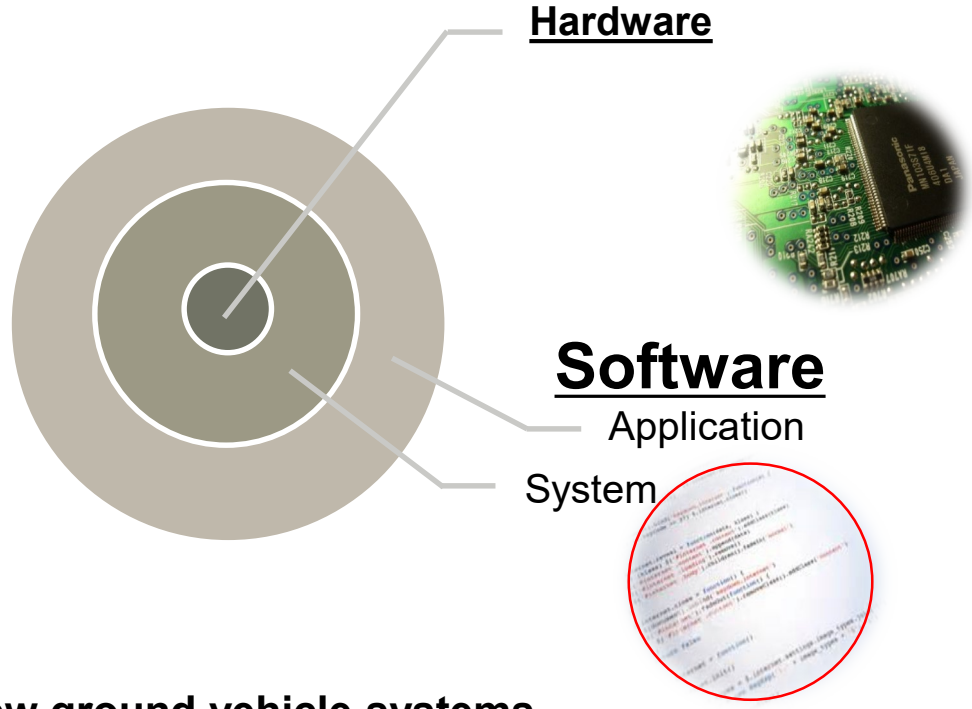
Jeffrey Jaczkowski
Associate Director, Ground Systems Cyber Engineering

GROUND SYSTEMS CYBER ENGINEERING

Mission
To identify cyber vulnerabilities and adaptively secure joint service ground vehicles, watercraft and support systems by engineering resilient cyber solutions.

A holistic approach to cybersecurity from project inception to decommission

Securing the System Architecture



Priorities
#1 Ensure cyber resiliency for new ground vehicle systems
#2 Mitigate "critical" vulnerabilities in fielded systems

Baking security into the vehicle architecture will significantly reduce the cyber attack surface.

GROUND SYSTEMS CYBER ENGINEERING

- Increased technology on military and commercial platforms can add vulnerabilities and entry points for hackers to attack.

- DoD will continue to leverage commercial cyber technology as appropriate to the military environment.

- DoD will continue to collaborate with the private sector on dual-use cyber innovations.
  - Develop military-specific solutions and strategically feed innovations back to the private sector
  - Leverage commercial trucking/automotive economies of scale for affordability

- There is a need to develop, recruit and train a national vehicle-centric cyber workforce geographically aimed at the point of need.

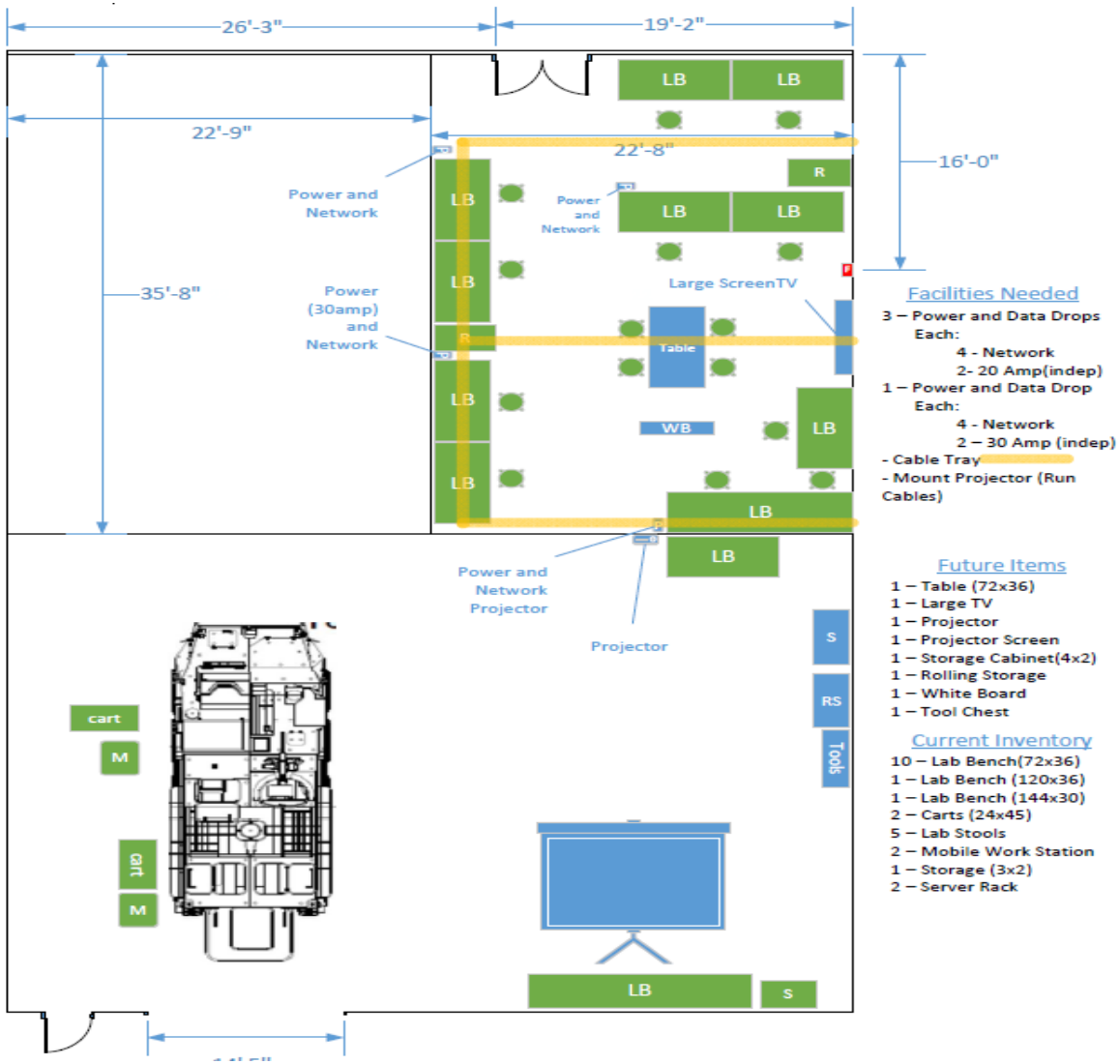
- DoD and Industry must continue to work together on Cybersecurity processes and technology efforts by doing the following:
  - Include Cyber early in the development process
  - Implement quantitative measures for cyber-resiliency and automated quantitative assessment methodologies
  - Develop high fidelity modeling and simulation capabilities and cyber realistic vehicle and threat models

DoD and Industry co-investment in our national cyber workforce, research and development and sharing best practices and threat intelligence is essential to national defense and economic security

GROUND SYSTEMS CYBER ENGINEERING CYBER VULNERABILITY TESTING

Test Service Agreements and Cooperative Research and Development Agreements

- Full Vehicle Cooperative Testing
- Black Box Adversarial Testing
- Cyber Security Consulting Services
- Firmware Integrity Verification
- Data Anthropology
- Component(s) Bench Testing
- Hardware Reverse Engineering
- Vulnerability Research
- Software Assurance



TECHNICAL FOCUS AREA: AI ENABLED ADAPTIVE CYBER RESPONSE

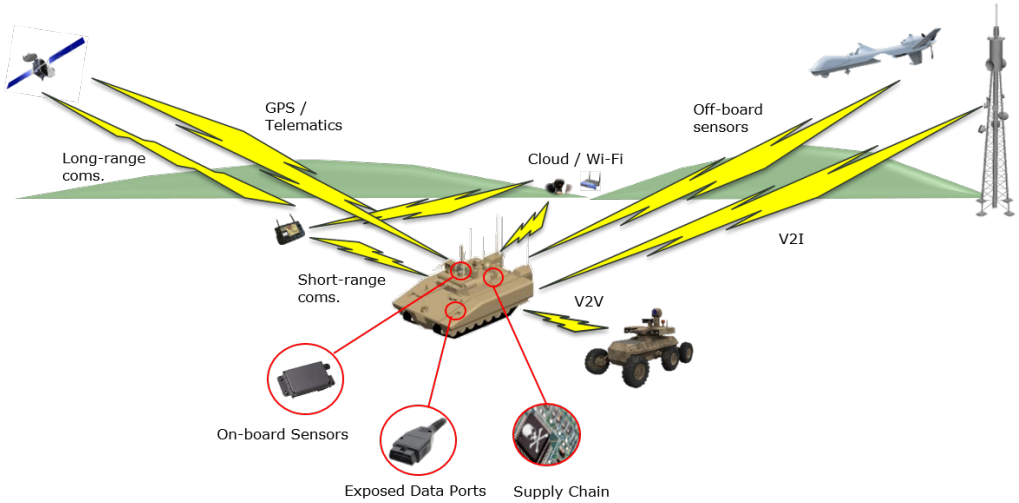
- **Technical Challenge 1: Ability to accelerate/enhance the observe, orient, decide, act (OODA) loop using artificial intelligence/machine learning for adaptive cyber response to vehicular cyber attacks.**
- **Gap: Lack the ability to detect, isolate and mitigate vehicle cyber attacks in real time to avail a wide range of responses to make military vehicles more resilient in multi-domain operations.**
- **Barrier: Reliance on heuristics and rule based reasoning using single attributes for a limited range of cyber response.**
- **Resolution Timing: 2–4 years.**

TECHNICAL FOCUS AREA: SUPPLY CHAIN RISK

- **Technical Challenge 2: Device Security/ Supply Chain Provenance**
- **Gap: Lack the ability to harden against reverse engineering, tampering or unauthorized updates to hardware and software; Lack the ability to mitigate malicious supply chain risk and latent vulnerabilities in microelectronics and embedded software**
- **Barrier: Vehicle system, subsystem and component level supply chain is global and diverse**

TECHNICAL CHALLENGE: SECURING AUTONOMOUS SYSTEMS

- Technical Challenge 3: Securing Connected and Autonomous Systems.
- Gap: When cyber vulnerabilities in a current military vehicle's firmware are found, the vehicle firmware must be updated by manually plugging in a diagnostic and maintenance device in order to service and update firmware located on several devices located within the vehicle.
- Barrier(s): The development of a secure centralized onboard vehicle controller utilizing robust and secure protocols to arbitrate the on-vehicle unpacking, verification and secure distribution of received firmware updates. This is already a significant problem with manned vehicles, in the future this problem will be compounded with autonomous vehicles due to the lack of manned personnel on the platform to perform this function directly, especially if continuous and uninterrupted remote operation of the platform is required.
- Resolution Timing: 3–5 years.



INVESTMENT STRATEGY

- **Existing Contract FY21**

DATC/Detroit Arsenal Automotive (DA2) OTA RFPP (Closed 1 May 2020)

Assurance and Verification of Vehicular Microelectronic Systems (AV2MS) single award ~ (up to $1M) to Perspecta Labs/Noregon

- **Opportunities for Partnership FY21-22**

DATC/Detroit Arsenal Automotive (DA2) OTA RFPP (Closed March 2021)

Military Vehicle Hypervisor, single award planned May 2021 ~ ($500K-$1M)

- **Future Opportunities - DATC Cyber Affinity Group**

Future RFP(s) for Advanced Vehicular Cyber Resiliency capabilities

Base with options - under Ground Vehicle Systems OTA or Detroit Arsenal Automotive OTA

- Funding estimated ~$1.0M-$3M/year

GROUND SYSTEMS CYBER ENGINEERING

Join the Ground Systems Cyber Engineering team tomorrow for One-on-One conversations