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

GVSC Industry Days 2022 – Ground Systems Cyber Engineering

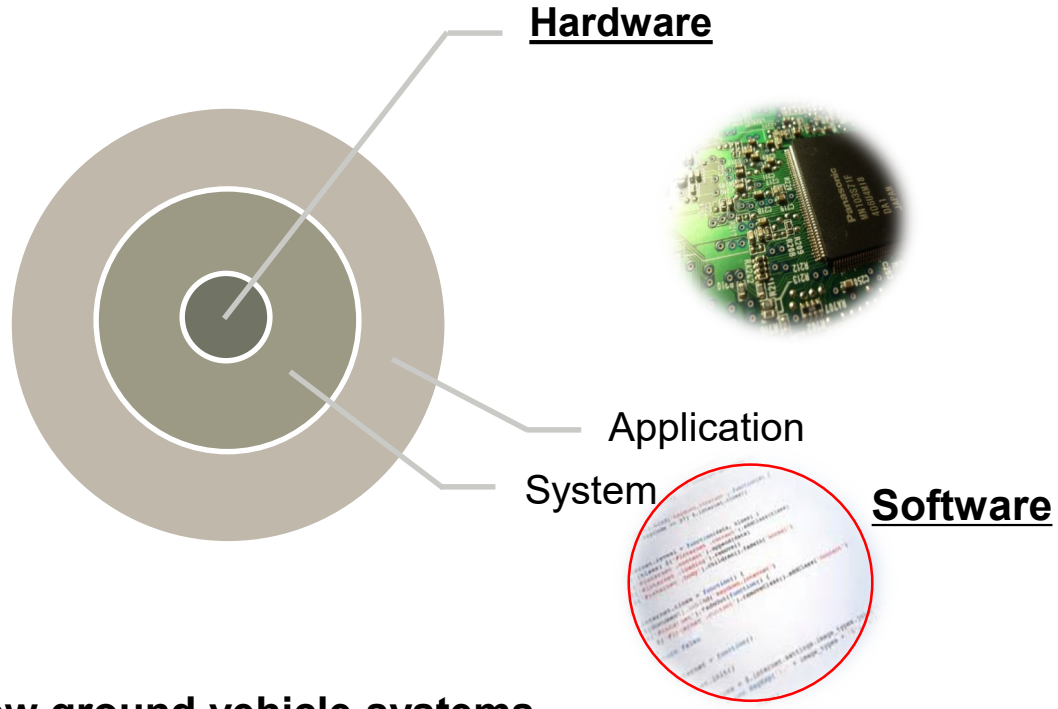
Jeffrey Jaczkowski
Associate Director, Ground Systems Cyber Engineering

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.

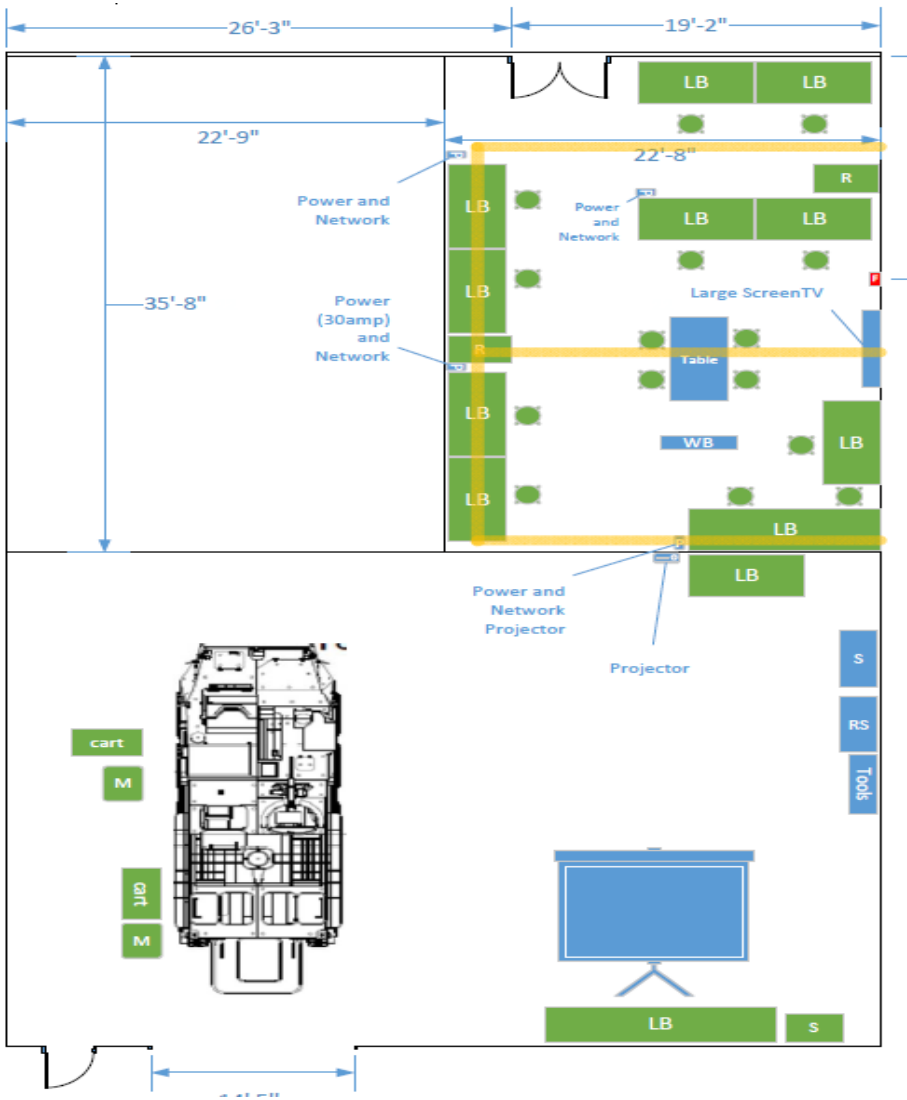
- DOD and Industry must continue to work together on Cybersecurity processes and technology efforts by doing the following:
  - Include Cyber early in the development process
  - Implement quantitative measures for cyber-resiliency and automated quantitative assessment methodologies
  - Develop high 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 RESEARCH AND PENETRATION 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 (AI/ML) for adaptive cyber response to vehicular cyber-attacks. AI/ML vehicular cyber defenses using predictive analytics through training of advanced deep learning threat models and threat signatures.
- **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 and provide warfighter cyber situational awareness.
- **Barrier:** Reliance on heuristics and rule-based reasoning using single attributes for a limited range of cyber response.
- **Resolution Timing:** 3-6 years

TECHNICAL FOCUS AREA: SUPPLY CHAIN CYBERSECURITY RISK

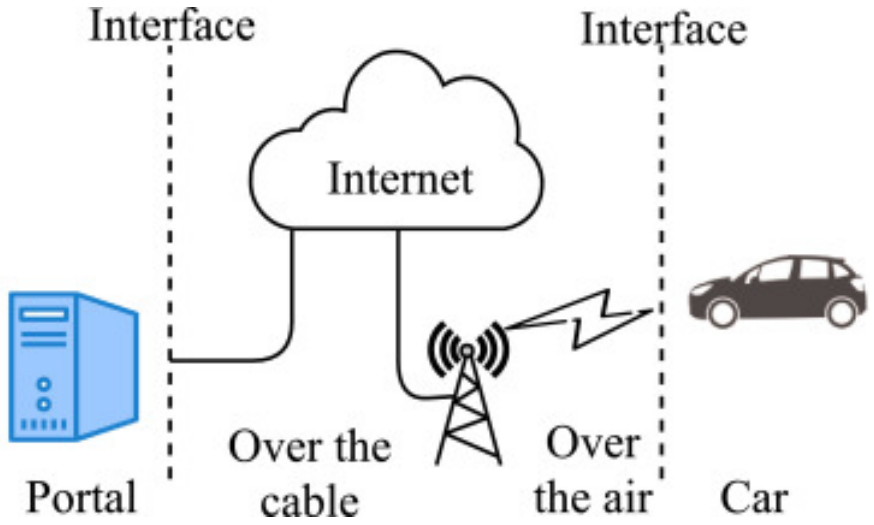
- **Technical Challenge 2:** Compromised microelectronics and software can create persistent vulnerabilities allowing for:
  - Exploitation to alter device microelectronics hardware
  - Exploitation to alter device firmware
  - Modifying embedded software
- **Gap:** Lack the ability to harden against 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 FOCUS AREA: CYBER MODELING & SIMULATION (M&S)

- **Technical Challenge 3:** Ability to include modeling of vehicle system effects in soldier-in-the-loop simulations/virtual experiments, as well as software and/or system integration lab (SIL) level modeling of cyber-attack and defensive system behaviors.
- **Gap:** Lack the ability to realistically emulate vehicle, subsystem and operational technology attack surfaces, cyber vulnerabilities and adversarial cyber-attack effects in a mixed M&S/SIL environment.
- **Barrier:** The need to account for varying security, vulnerabilities and processing capabilities of individual and connected components (hardware and software).
- **Resolution Timing:** 2-4 years

TECHNICAL FOCUS AREA: SECURE OVER-THE-AIR (SOTA) UPDATES

- **Technical Challenge 4:** Ability to remotely, rapidly and securely patch our systems to evolving and emerging vulnerabilities to allow ground vehicle systems to deploy cyber defenses and maintain cyber situational understanding in machine-relevant timescales to rapidly emerging AI-enabled threats.
- **Gap:** Secure Over the Air (SOTA) not employed on military vehicles due to heightened security concerns versus commercial vehicles.
- **Barrier:** Security is paramount to enabling telematics, health monitoring and remote software and patch management.
- **Resolution Timing:** 2-5 years



FY22 EFFORTS & INVESTMENT STRATEGY

FY22 Contract Award Actions:

DATC/Detroit Arsenal Automotive (DA2)

Military Vehicle Hypervisor, single award March 2002 ~ ($500K-$1M) Dorner Works

- Virtualization of Line Replaceable Unit functionality for advanced cybersecurity protection through military vehicle Hypervisors.
- Provide resiliency to augment traditional vehicle electronics systems.

NAMC OTA Basket Pull

Hardware Security Module, single award planned April 2022 ~ $500K Synergistic/Guard Knox

- Secure authentication modules for military vehicular engine control units (ECUs).
- Provide for secure firmware updates to ECUs.

Future Opportunities:

- CRADA's and TSAs
- Participation in DATC Cyber Affinity Group
- Future RFP(s) none specific at this time

*Join the **Ground Systems Cyber Engineering** team for One-on-One conversations at Table #7*