Starting the Engine: Fueling Communication and Collaboration

David Carroll

Vice President, Cyber Capability Engineering and Strategy,

General Dynamics Information Technology (GDIT)

From Cyber Warfare to Freight Defense – Why This Mission Matters to Me

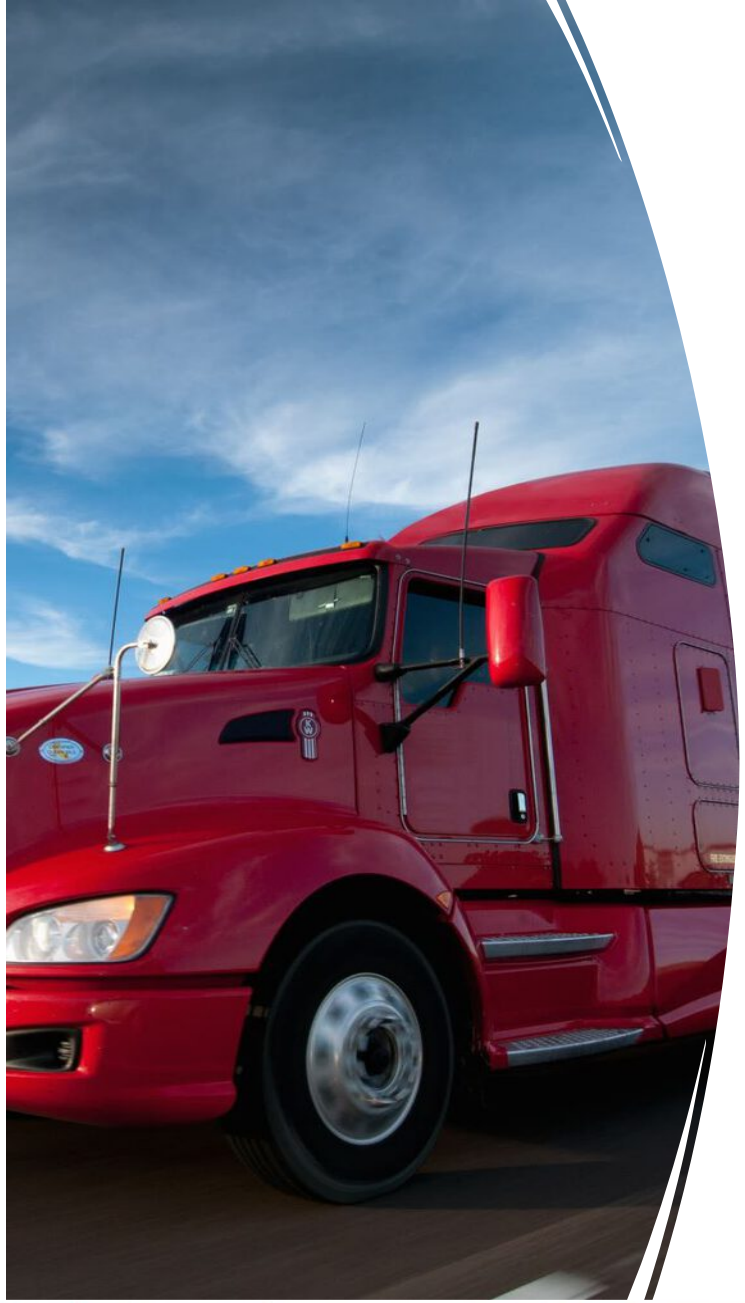
A little about me:

David Carroll – Vice President, Cyber Capability, Engineering & Strategy, General Dynamics Information Technology, Intelligence and Homeland Security

- 25+ years leading cyber and infrastructure defense across government and industry – Dual Focus on military and homeland defense
- Current US Navy Reserve Information Warfare Officer – leading efforts in offensive cyber operations and strategic cyber defense integration
- NATO “Coherent Resilience” Exercise ”Cyber Syndicate” Leader
- Former DHS Cyber Security Senior Executive – CISA Mission Engineering
- National Advisor on AI assurance frameworks and collective defense strategy

My Suggested Mission Focus and Call to Action for NMFTA Members:

“Connecting national security with logistics security — keeping America moving and protected.”



The Stakes

- $940B+ U.S. trucking industry = 72% of all freight by weight
- 80% of U.S. communities rely solely on trucking for essential goods
- Median ransomware loss in logistics: $1.3M/incident (2024)
- Message:
  - **If trucks stop, America stops.**

Threat Landscape

- Ransomware downtime = supply chain paralysis
- GPS/Telematics manipulation can reroute fleets
- Software/vendor vulnerabilities multiply entry points
- AI-enabled threats (deepfakes, adaptive malware) can cripple communications
- **Fact: 90% of major carriers report cyber intrusion attempts monthly.**

Real-World Impact

"Cyber incidents don't just hit IT — they hit deliveries, drivers, and customers."

2023 ransomware attack on port logistics system delayed 1M+ containers

Stranded freight and delayed medicine shipments have threatened lives and livelihoods

The Need for Collective Defense

- Cyber defense is a team sport
- Collective defense models reduce detection time by 40%
- Shared indicators of compromise (IOCs) are PROVEN to prevent cascading incidents

Pathways to Collaboration

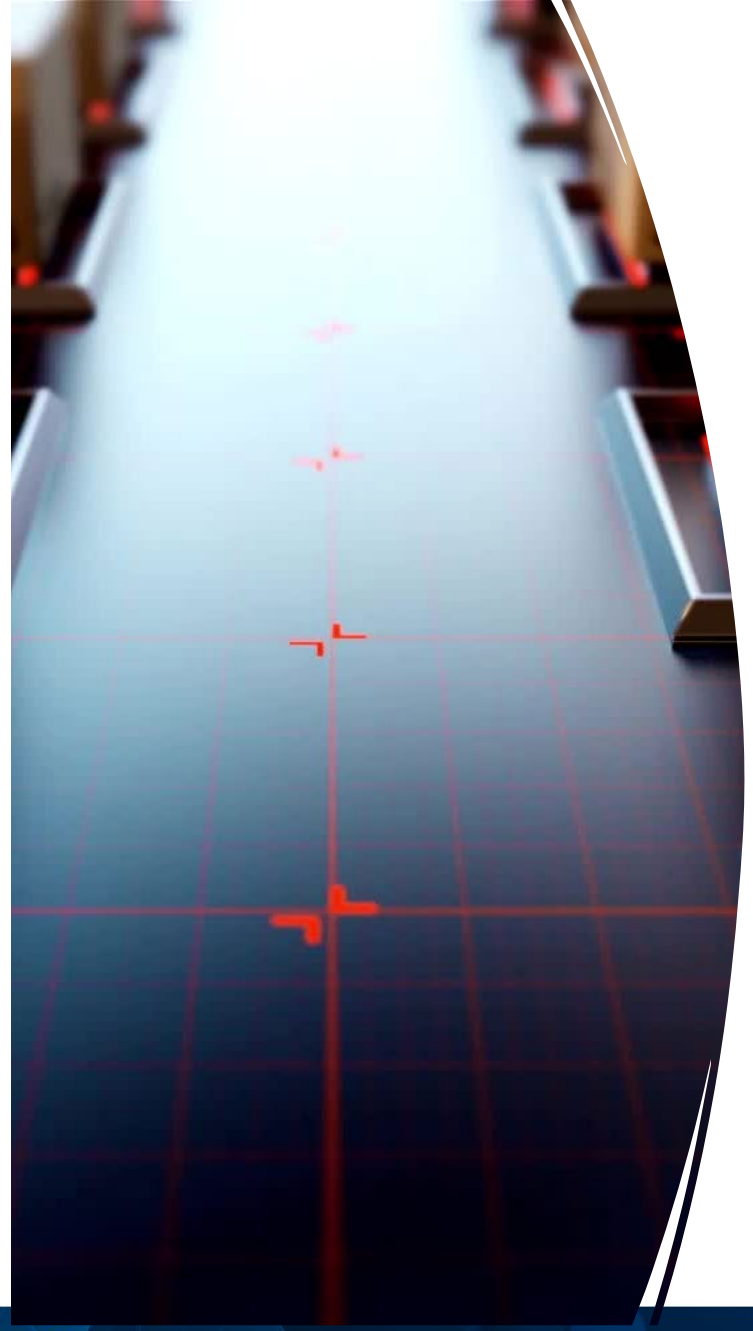
Cyber Data Sharing – near real-time, actionable intel is key…

Operational Collaboration – joint ransomware playbook exercises

Trusted Circles – competitors cooperating for system resilience

Connect to NMFTA and CISA JCDC feeds

Conduct 45-minute tabletop ransomware drills



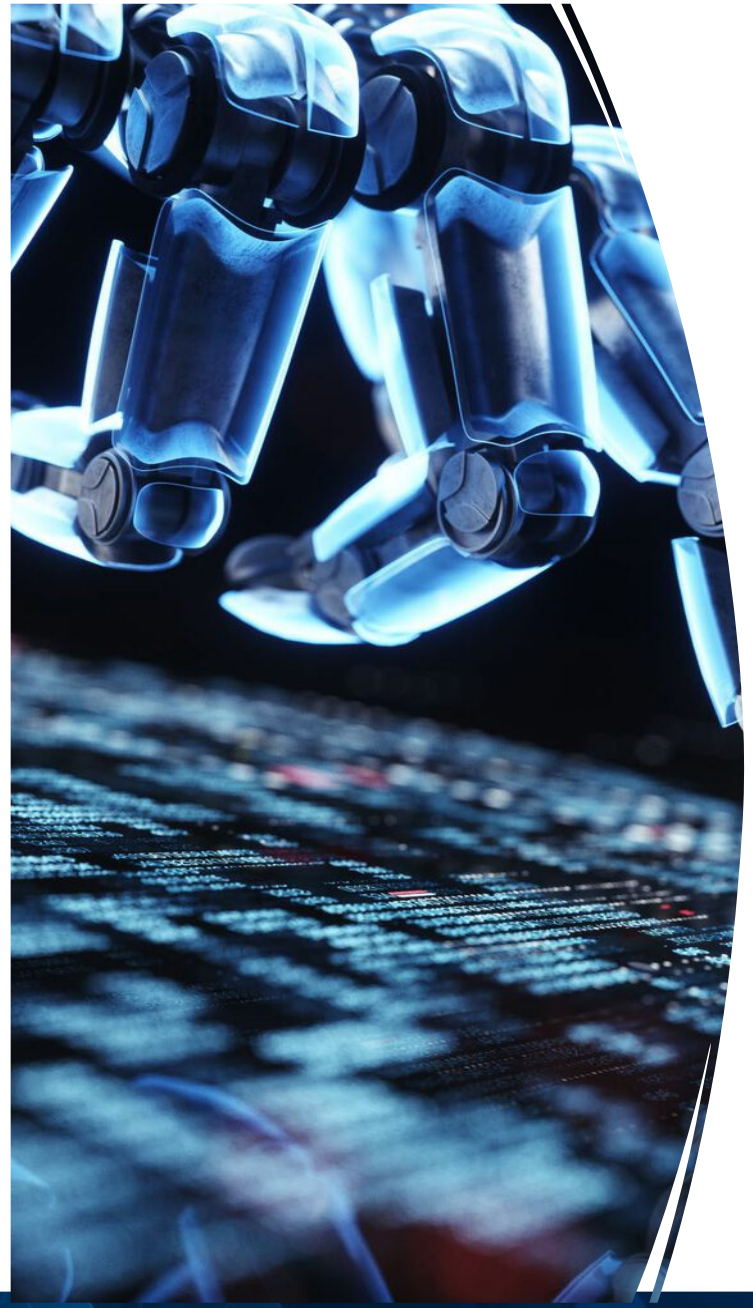
The Future with AI

- **65% of logistics CIOs plan to deploy AI-based cyber tools by 2026**
- AI triage can reduce incident response time by 60%
- Use Cases:
  - LLMs for anomaly detection across fleets
  - AI co-pilots for small carriers
  - Real-time, AI-driven intelligence clearinghouse

Vision: AI-Enabled Collective Defense

- Attack detected → anonymized AI analysis → shared insights → immediate co-piloted response

The Message: Machine-speed coordination builds national resilience.



Call to Action

- **Share threat data**; leverage national cyber resources
- **Invest in AI defense pilots** — the adversary already has
- **Build trust across industry** and showcase cybersecurity leadership
- **“The only way we win is together.”**

Closing

Thank You!

David Carroll – david.carroll@gdit.com

LinkedIn: linkedin.com/in/davewcarroll