2020 NDIA GROUND VEHICLE SYSTEMS ENGINEERING AND TECHNOLOGY SYMPOSIUM
CYBER TECHNICAL SESSION
AUGUST 11-13, 2020 - NOVI, MICHIGAN

HIDDEN VULNERABILITIES: OPERATIONAL TECHNOLOGY CYBERSECURITY SHORTFALLS

James Correnti[1], Josh Lospinoso, PhD[2], Michael Weigand[3], Kara Kramer[4]

[1,2,3,4] Shift5, Arlington, VA

ABSTRACT

The Department of Defense (DoD) lacks a unified cybersecurity solution to provides intrusion prevention and detection capabilities to existing weapons platforms, empowering crews, maintainers, and commanders to achieve understanding and inform confidence in the cyber health and status of their systems. In October 2018, the Government Accountability Office (GAO) reported that DoD weapons systems are highly vulnerable to cyber-attacks. We have identified several major inherent vulnerabilities and likely attack vectors for existing weapon systems. Our Technical White Paper will outline the changing threat landscape for operational technology (OT), the vulnerabilities in the cyber-physical systems and shortfalls in addressing these vulnerabilities, and our analysis on critical capabilities necessary to secure military OT.

Citation: J. Correnti, J. Lospinoso, M. Weigand, K. Kramer, "Hidden Vulnerabilities: Operational Technology Cybersecurity Shortfalls," In *Proceedings of the Ground Vehicle Systems Engineering and Technology Symposium* (GVSETS), NDIA, Novi, MI, Aug. 13-15, 2019.

1. INTRODUCTION

Today's weapon systems have little or no protection against cyber-attacks and next generation platforms must address this threat. Advanced persistent threats can leverage technical data stolen from major weapon systems to develop cyber capabilities that allow asymmetric power projection in near-peer conflicts. Adversaries can degrade, disable, deny, destroy, or manipulate entire fleets of weapon systems at a location and time of their choosing.

Automation, connectivity, and modular design are foundational elements of our modern military capabilities. As we move progressively closer to autonomous systems, the increasing complexity of the systems will enhance performance and functionality, but it also increases attack vectors and makes these systems more vulnerable to cyber-attacks and attractive to adversaries (see Figure 1. Threat Landscape). An October 2018 GAO report laid out the widespread nature of this problem. *"DoD testers routinely found mission critical cyber vulnerabilities in nearly all weapon systems that were under development."[1]* In the GAO study, test teams were able to gain access, disrupt, and control weapons system security controls, using only free, publicly available information or downloaded software from the Internet.

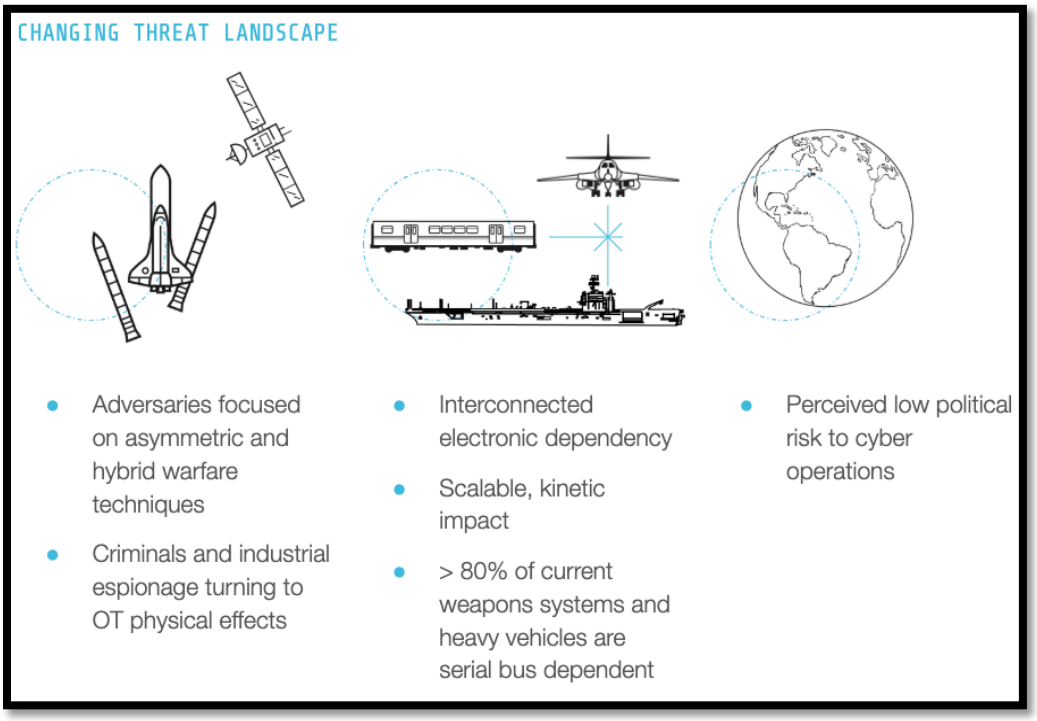

Figure 1. Changing Threat Landscape

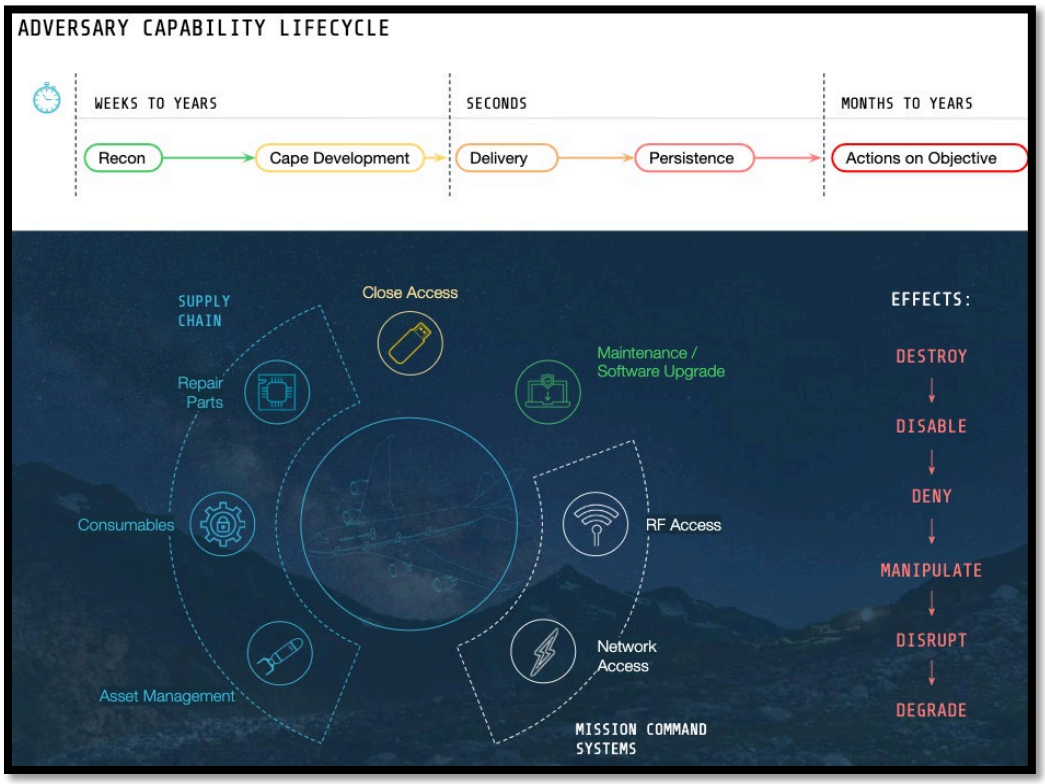

Figure 2. Adversary Capability Lifecycle

2. Cyber-Physical Limitations

Adversaries have many entry points to leverage cyber-physical security shortfalls in weapon systems. Currently available approaches to providing system protection are cost prohibitive, or cannot quickly and iteratively adapt at the same pace as cyber-attack techniques. "*Even though many weapon systems are air gapped (i.e., not directly connected to the internet), cyber-attackers can exploit external interfaces (e.g., radios, radars, and maintenance ports) to gain access to weapon systems' internal computers, networks, and data. If a weapon system was not designed with cybersecurity in mind, attackers can exploit their initial access to disrupt or degrade a weapon system's operation*." [2]

With the wide array of attack vectors (see Figure 2. Adversary Capability Lifecycle) and the inability to comprehensively extract and analyze data at the serial bus level from cyber-physical systems, operators and commanders have little to no insight into the cyber health of their systems. The maintenance personnel responsible for the systems may not be able to discern between a cyber-attack and true maintenance issue, and cannot quickly and effectively remediate the issue without that understanding. The Cyber Protection Teams (CPTs)—who are responsible for the cyber health of DoD assets—lack adequate software and hardware toolkits to interrogate and examine most weapon systems, as their current tool kits are tailored to internet protocols.

Based on our analysis of capability shortfalls for the cyber protection of weapon systems, these are most critical.

- Inadequate ability to monitor internal networks continuously for anomaly detection.
- Lack of capability to ensure cryptographically-signed software and firmware updates to all embedded system computers.
- Insufficient alerting mechanisms for crew and maintenance personnel to malicious software behavior.
- Lack of capability to provide full data capture and access of system behavior to incident responders.

3. The Path Forward

Securing the cyber-physical elements of weapons systems cannot detract from system reliability or function. In a DoD cybersecurity working group in 2019, an Army representative said, *"Reliability is everything. When a soldier pushes a button, steel has to be put on target,"* according to an industry report.[3] Many paths to securing the operational technology of the weapon systems would prove to be an unacceptable cost to weapon system reliability and overall likelihood of system failure.

Future weapon systems will need to prioritize cyber resiliency as a key characteristic to provide protection against quickly evolving adversarial cyber warfare tactics. Providing cyber resiliency at the serial bus level also provides potential cost savings for maintenance and analytics to inform Commanders.

Table 1. Benefits of Cyber Resiliency

Role	Benefit of Cyber Resiliency Capability
Commanders	Insight into the cyber health of the weapons platforms.
Weapon Systems Operators	Ability to quickly and effectively conduct cyber inspection of their systems.
	Ability to identify and report cyber anomalies in weapon systems quickly.
	Ability to quickly assess and react to cyber-attacks that aim to disrupt, degrade, deny, disable, destroy or manipulate (D5-M) their weapon systems
Cyber Protection Teams (CPTs)	Ability to rapidly download historical, enriched full-take data bus capture data.
	Analyze the historical data bus captured in a data mining and graphing software package.
	Rapidly gain insights to accomplish assigned CPT missions on weapon system platforms.

Role	Benefit of Cyber Resiliency Capability
	Effectively inform Commanders of the origin and mitigation of malicious code, giving them immediate insight into the cyber health of the fleet.

Future weapon systems need cyber resilience as a cornerstone characteristic to significantly increase deterrence and maintain superiority on the battlefield. System maintainers and CPTs would benefit from the full-take packet capture with over six months of data, and Artificial Intelligence/Machine Learning (AI/ML) models enhance the analysis and understanding of that data. Current training and fielded tools focus on TCP/IP (internet) networks and as the Army and wider DoD matures requirements for next generation platforms, the critical characteristics for the vehicle need to also be supported across the Doctrine, Organization, Training, Materiel, Leadership and Education, Personnel, Facilities, and Policy (DOTMLPF-P) spectrum.

3.1. Metrics of Success

We need specific metrics for cyber resiliency for weapon platforms to track both measures of performance and measures of effectiveness. Metric development is a foundational step in securing these platforms, and we offer this starting point.

Table 2. Cyber Resiliency Metrics

Cyber Resiliency Metrics
Reaction time of a program to enhance the platform's protection posture against an emerging adversarial cyber tactics, techniques, and procedures (TTPs).
Ability for a platform to reconstitute or self-heal after a cyber incident.
Average time for platform reconstitution or self-heal after a cyber incident.
Average time for a weapon system crew member to determine that a cyber-attack is underway against their weapon system.
Accuracy of maintenance personnel diagnosing system faults versus cyber anomalies and attacks.
Average time for a command element to recognize that their weapon systems are under attack and take appropriate actions to mitigate, recover, and/or reconstitute firepower.
Average time for an incident response team to collect and begin analyzing historical data captures of embedded weapon system networks.
Ability to monitor and identify anomalies against an established baseline.
Ability to sense and report current system configuration and cyber health.

1. REFERENCES

[1] Report to the Committee on Armed Services, U.S. Senate, United States Government Accountability Office, "Weapon Systems Cybersecurity, DoD Just Beginning to Grapple with the Scale of Vulnerabilities," GAO-19-128, October 2018.

[2] Dwyer, Morgan. Center for Strategic and International Studies (CSIS), "Prioritizing Weapon System Cybersecurity in a Post-Pandemic Defense Department," May 13, 2020. https://www.csis.org/analysis/prioritizing-weapon-system-cybersecurity-post-pandemic-defense-department

[3] ICF International, "Weapons System Cybersecurity: Determining a course of action to address weaknesses," May 15, 2019. https://www.icf.com/insights/cybersecurity/cyber-weapon-systems.