U.S. ARMY EVALUATION CENTER

Cybersecurity Evaluations of Army Robotic and Autonomous Systems

Mr. Robert F. McKelvey III

28 March 2019

Opportunity

- Big picture: Smart systems continue to be emphasized as force enablers and protection measures in strategic plans.

- Testable measures for Robotic and Autonomous System (RAS) survivability against cyberspace-based threats.

- "Autonomous and Robotic Systems Cybersecurity and Electromagnetic Activities (CEMA) Test and Evaluation Planning Guide".
  - Published: 8 Aug 2018. Distributed: Army ALT Magazine Oct – Dec 2018.
  - Army funded quarterly updates.

Measure Examples

- Cybersecurity:
  - How well do the system's cybersecurity capabilities protect the user's required data and information?
    - Adequacy of disk and file level encryption used for Data-at-Rest.
    - Security of data transfer and processing design.
  - How will cybersecurity detection measures support the user's ability to identify specific attacks?
    - Adequacy of system produced audit trails and logs.
    - Effective of system responses to an intrusion or incident and timeliness of user notification.
  - How is the mission impacted by cybersecurity vulnerability?
    - Impact to the mission by loss of data or inability to access the system.
    - Ability of the user to perform mission tasks if the system does not receive requested information.

- Electronic Warfare:
  - How well does the system survive an Electronic Attack?
    - Capability of the system to survive threat jammer effects long enough to complete the mission.
    - Message completion rate and speed of service in benign versus contest environments.
  - How effective is the system's Electronic Protection?
    - Mean time to recover.
    - Signature management and reduction.
  - What capabilities do the users gain for Electronic Warfare Support?
    - Location accuracy.
    - Probability of intercept.

M1-A2 SEPv3

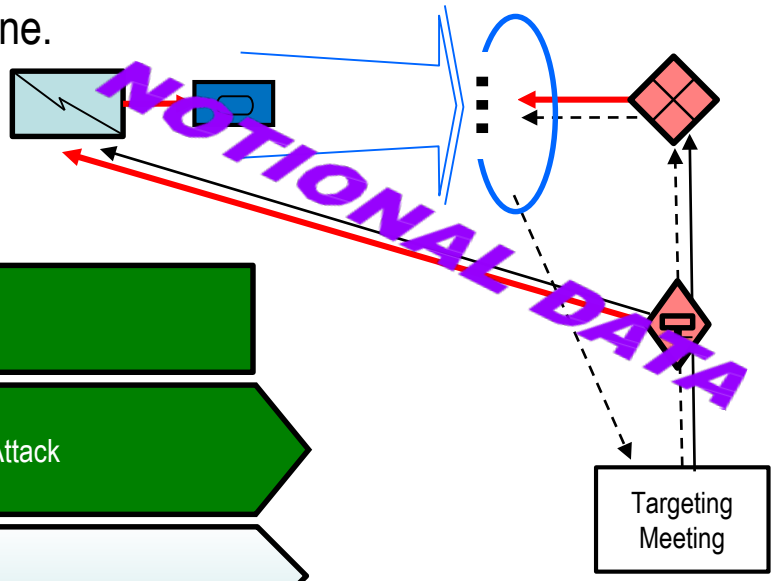
CVI ✓ | ACDT ✓ | CVPA ✓ | AA

❖ Adversarial Assessment (AA) Intent:

- Conduct non-cooperative AA with a threat-representative cyber adversary.
- Document operational impacts.

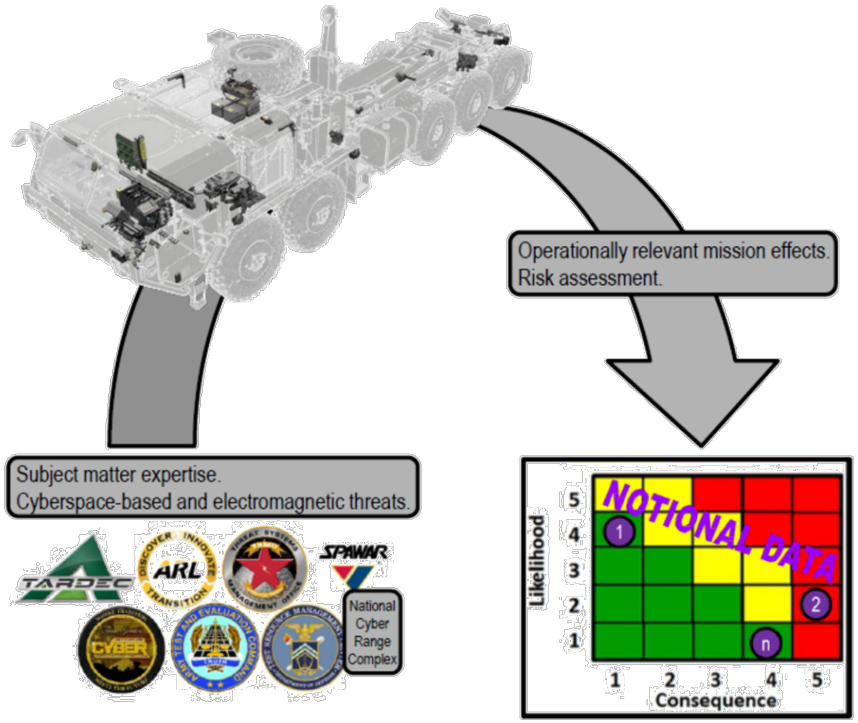
❖ RAS?:

- Effectiveness enhancements.
- Baseline.

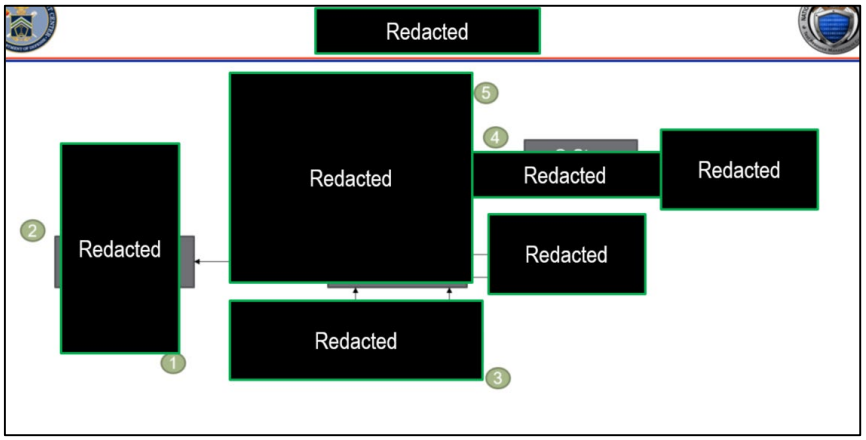


Org	**Pre-pilot Static**	**Pilot**	**Record**
TSMO	Initial Recon	Establish Access	Exploitation and Attack
SLAD	Protect, Mitigate, and Recover		

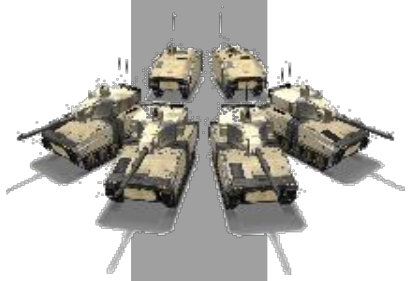
Leader Follower



- Survivability Critical Operational Issue: "Does TWV LF provide robustness and resiliency in threat contested environments in order to enable increased throughput of Line Haul and Local Haul missions?"
- Cybersecurity Test Efforts:
  - Risk Management Framework (Program Office Led).
  - "Developmental Testing" (NCRC Led & SLAD support).
  - Operational Technical Demonstrations (TBD).
- NCRC Benefits: Use Cases, Dependencies, & Timeframe.



Robotic Combat Vehicle



NDAA FY16 Section 804
Middle Tier Acquisition

- Next Generation Combat Vehicle – RCV: Company-sized element augmented with unmanned ground combat vehicles.
- Spiral Development and Prototyping.
- CEMA Resilience:
  - Unmanned systems are hardened to meet the operational requirements to survive in a CEMA-contested environment and maintain resilience through redundant low-probability of detection and low-probability of intercept defense mechanisms.
  - Unity of Effort.
  - Artificial Intelligence as force multiplier.

Notional pictures for representative vehicle characteristics only, not to be considered an endorsement or preference for any specific system or subsystem.

Conclusion

❖Guidance Provides Flexibility:

- Middle Tier Acquisitions and Cross Functional Teams will speed assessment schedules and broaden test community.
- New technology is opening new avenues.

❖Open Communication:

- Reviewing future iterations of CEMA Guide.
- Funding future analysis.
- Continued outreach.

Mr. Robert F. McKelvey III
ATEC-AEC-SVED
Lead Army Ground RAS CEMA Evaluator
robert.f.mckelvey2.civ@mail.mil