Space- RF Enabled Cyber

Background and Description

Understand the gaps related to testing RF Enabled Cyber attacks on Space assets.

Scope: Uplink Attack Vector, "Over the Air" attacks

PeopleTec will work with the Space Community to determine T&E efforts for RF Enabled Cyber attacks. This will include:

- How does the space community test against RF Enabled Cyber attacks?
- Does the space T&E community have the resources they need to test?
- What processes/planning do they utilize for test?
- Are the current T&E planning processes threat representative?

Approach

The following approach will be used to determine Space T&E gaps related to RF Enabled Cyber Attacks

- Develop roadmap and scope (COMPLETE)
- Use Case Deep Dive: NGO IPR, PTS
- Site Visits to Space T&E community members with a cyber focus
- Gap Analysis (Resources, Intel, Processes, etc.)
- Determine deltas between Space and other domains for assessments with RF enabled cyber?

Objectives

The deliverables and goals for the RF Enabled Cyber section of the Space/EW study

- A report that details the gap analysis findings
- Status on integration with program offices as it relates to RF Enabled Cyber attacks
- Intel portfolio of current TTPS/threat actors
- Proof of Concept for RF Enabled Cyber on Space Assets

Risks and FY24 Considerations

Risks:

- Space T&E Community
  - Changes in offices/personnel
  - Lack of T&E data

FY24 Considerations:

- CAP Practical Assessment based off FY23 PoC
- RF Enabled Cyber T&E Gap Analysis for other warfare domains
- Study/Recommendation on how space T&E community can prepare for emerging threat technology? (AI, etc.)

Cyber Threat Model Investigation/ Cyber Lab Support

Background and Description

Cyber Threat Model Investigation:
Investigate the gaps and limitations in Space related cyber threat models
- Understand the current environment for cyber threat models and the current need for space cyber threat models
- Identify use cases, resources & stakeholders for cyber threat models

Cyber Lab Support:
- Determine T&E lab gaps and stakeholders for threat focused lab
- Determine use cases for TETRA cyber lab
- Design architecture for cyber lab

Approach

Cyber Threat Model Investigation:
- Identify stakeholders and tool developers
- Gap Analysis on cyber threat models for space
- Analysis into collaboration with other domain cyber threat models and space assets

Cyber Lab Support:
- T&E Lab gap analysis
- Threat representative use case development
- Architecture design for cyber lab
  - Multi-classification design
  - ROM for hardware/software

Objectives

Cyber Threat Model Investigation Deliverables:
- A report that determines
  - Gaps in cyber threat models for the space T&E community
  - T&E resources needed to support space cyber threat models

Cyber Lab Support Deliverables:
- A report discussing Threat T&E lab gaps and TETRA cyber lab use cases
- ROM for cyber lab build out
- Architecture Design documents for initial cyber lab build out

Risks and FY24 Considerations

Risks:
- Construction timeline for cyber lab at MSIC

FY24 Considerations:
Cyber Threat Model Investigation:
- Develop working group for Space T&E community
- Use lab for cyber threat model repository and development

Cyber Lab Support:
- Cyber Lab build out (Hardware/Software, Network set up, etc.)
- Proof of Concept for use case 1

Threat Cyber-EW Digital Technologies

Background and Description

OT&E Threat Model EW Data, Process & Management

- Develop cyber and electromagnetic spectrum data standards to adequately collect and manage the system design data, threat effects, and vulnerabilities
- Develop digital technologies to automate the process of detection and recovery from cyber and electromagnetic spectrum vulnerabilities
- Adequately represent the latest cyber and electromagnetic spectrum threats in testing as compared to the latest intelligence reports
- Continuously identify, digitally document, prioritize and track new gaps in cyber and electromagnetic spectrum T&E shortfalls

Approach

- Define CEW threats by obtaining standard from intelligence community stakeholders
- Develop T&E data standards for each use case definition
- Research and provide PoC for digital technologies that automate detection and recovery from CEW
- Determine initial CEW threat use cases to design technology to prioritize and track shortfalls in threat intelligence
    - TIDE will support the tracking and trend analysis of intelligence supporting CEW

Objectives

Deliverables for this project will include:

- Initial draft of T&E data standards for CEW threat data
- Proof of concept for digital technologies to automate detection and recovery from CEW
- Development of TIDE to support a representative environment to host latest CEW threats against latest intelligence reports
    - This will be a module of TIDE

Risks and FY24 Considerations

Risks:

- Lack of intelligence to support data standards

FY24 Considerations:

- Use AI tools/techniques to develop trend analysis on Cyber/EW threat intelligence
- Develop MVP for digital technologies to automate the process of detection and recovery from CEW vulnerabilities