JOHNS HOPKINS
APPLIED PHYSICS LABORATORY

Cybersecurity and Resiliency Test and Evaluation Considerations

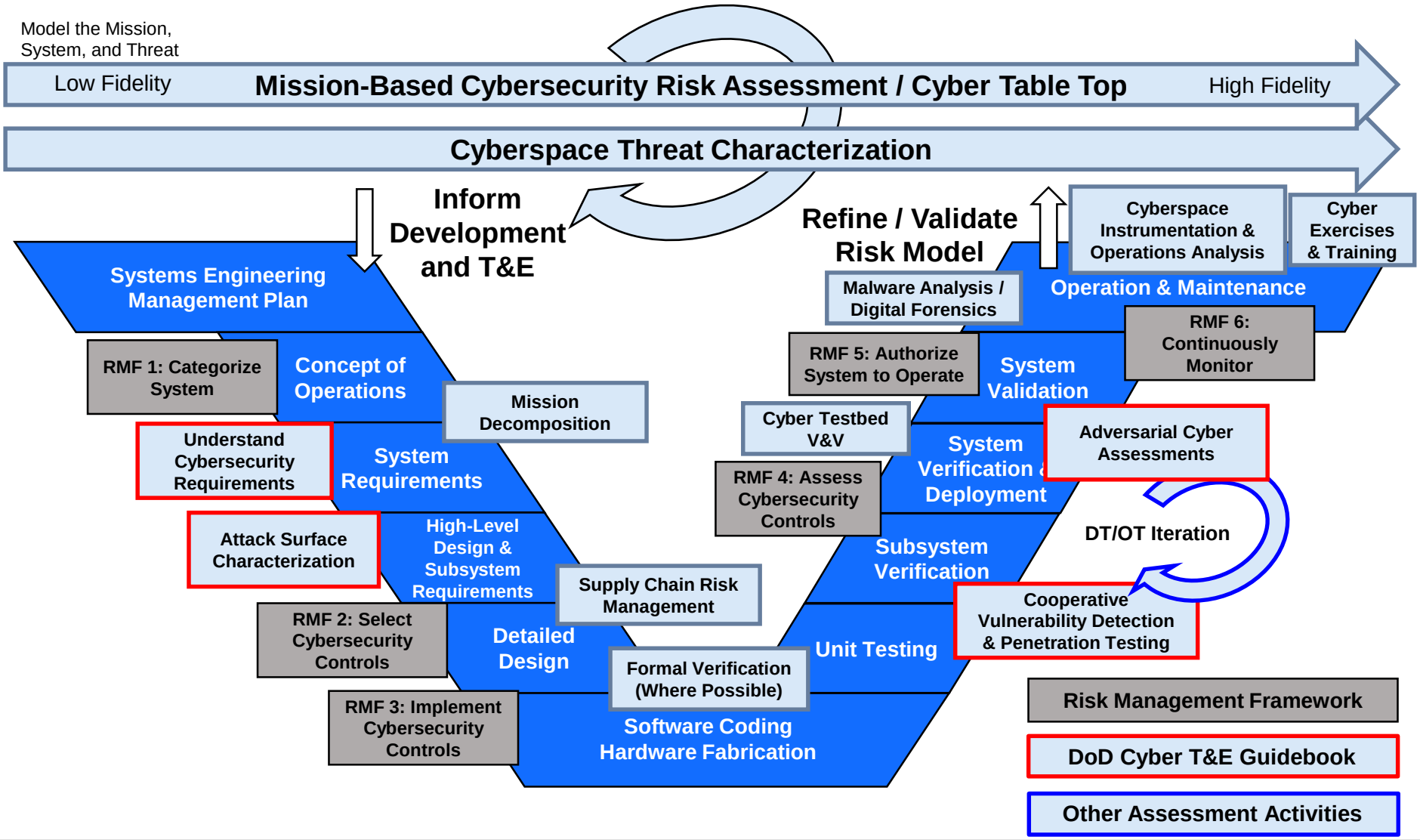
8 March 2018

Paul Dailey, PhD
Paul.Dailey@jhuapl.edu
(443) 778-8684

Agenda

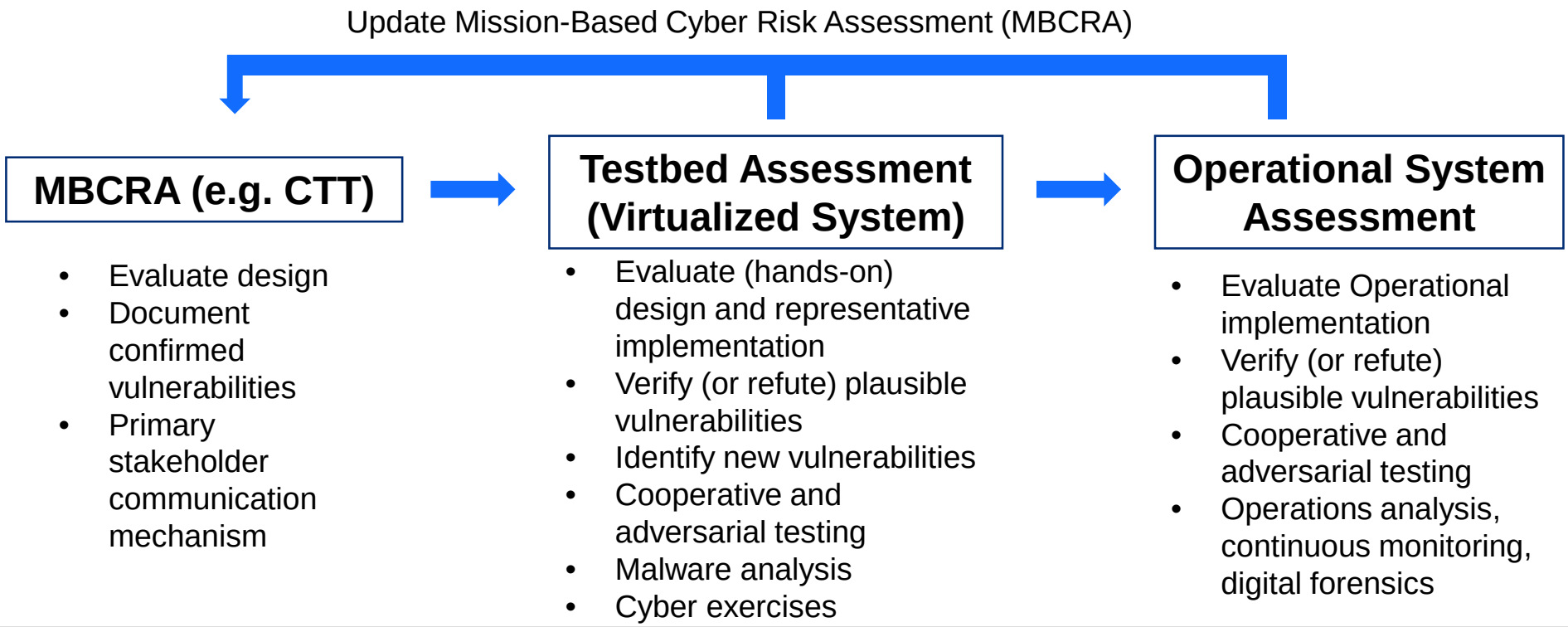
- Cybersecurity assessment and T&E activities overview
- Some cyber T&E process recommendations
- Attack surface characterization example
- Cybersecurity vs. resiliency
- Discussion: Requirements verification vs. vulnerability discovery

Cybersecurity Assessment & T&E Activities



Recommendations for Cyber T&E Practitioners

- Start early, iterate during concept definition and preliminary design w/ SE
- Leverage mission-based cyber risk assessments to guide follow-on activities
- Mission decomposition -> criticality analysis -> attack surface prioritization
- Identify your test infrastructure early and integrate with model-based systems engineering (MBSE) efforts



Attack Surface Characterization Approach

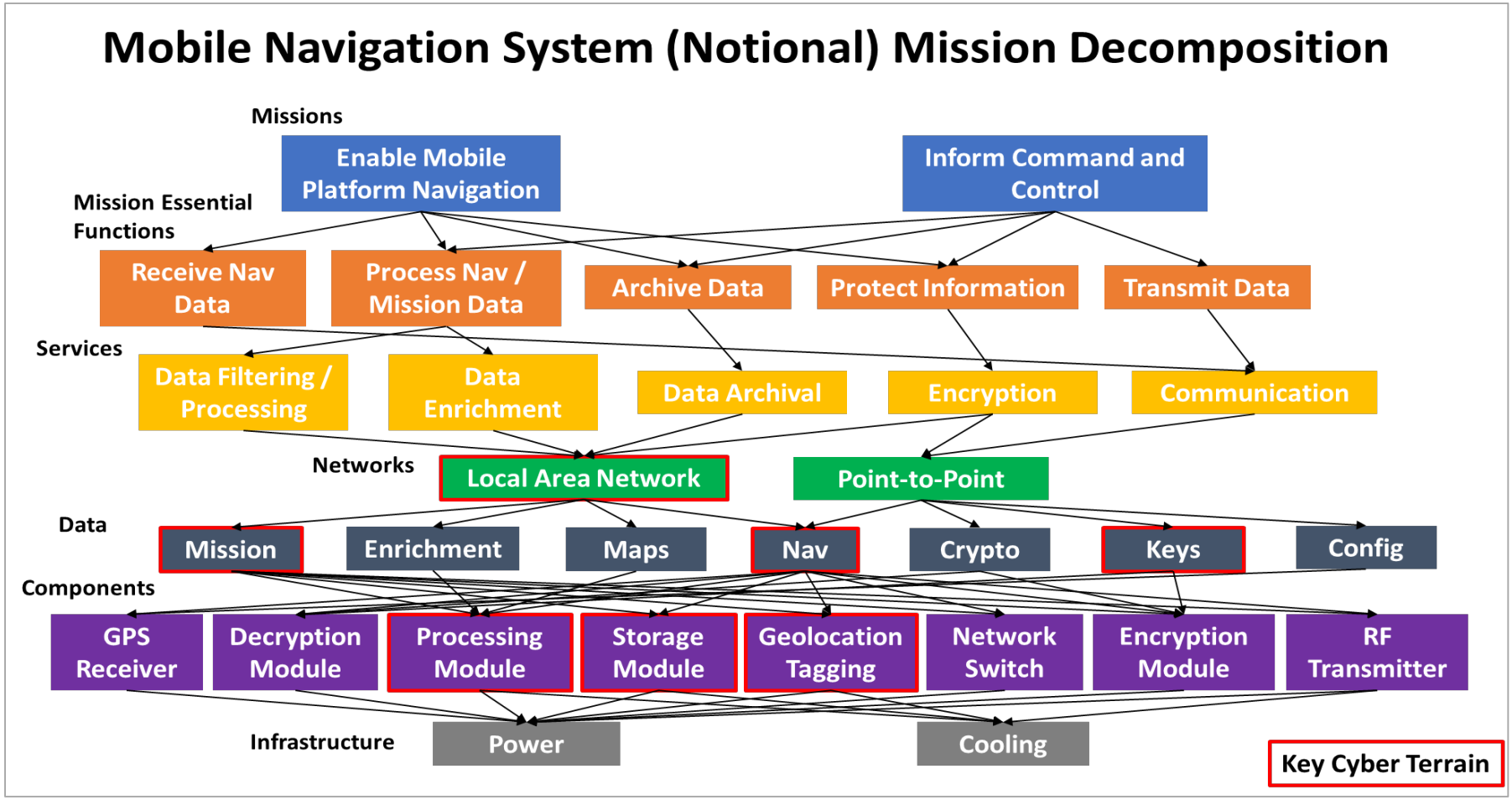
Develop an Attack Surface List – Map to Key Terrain

System Component	Interfaces	Information Exchanges	Data
GPS Receiver	• GPS antenna • Fiber interface • Serial port	• GPS navigation messages (GPS antenna) • Navigation messages (Decryption module) • Configuration updates (factory)	• Navigation data (encrypted, in transit) • Configuration data (at rest)
Decryption Module	• Fiber interface • Ethernet interface • Serial interface	• Navigation messages (GPS receiver) • Navigation messages (Processing module) • Key management information (Key custodian) • System administration commands (Admin)	• Navigation data (decrypted, in transit) • Cryptographic algorithm (at rest) • Cryptographic keys (at rest)
Processing Module	• Ethernet interface • Serial interface	• Navigation messages (Decryption module) • Enriched mission information (Geolocation tagging unit) • Navigation messages (Geolocation tagging unit) • Storage information (Storage module)	• Navigation data (at rest) • Maps (at rest) • Enrichment data (at rest) • Mission data (at rest)
Storage Module	• Ethernet interface • Removable media drive	• Storage information (Processing module) • Archive download (Analyst) • Maintenance commands (Database manager)	• Navigation data (at rest) • Mission data (at rest)

A notional example from DASD(DT&E)

Attack Surface Characterization Approach

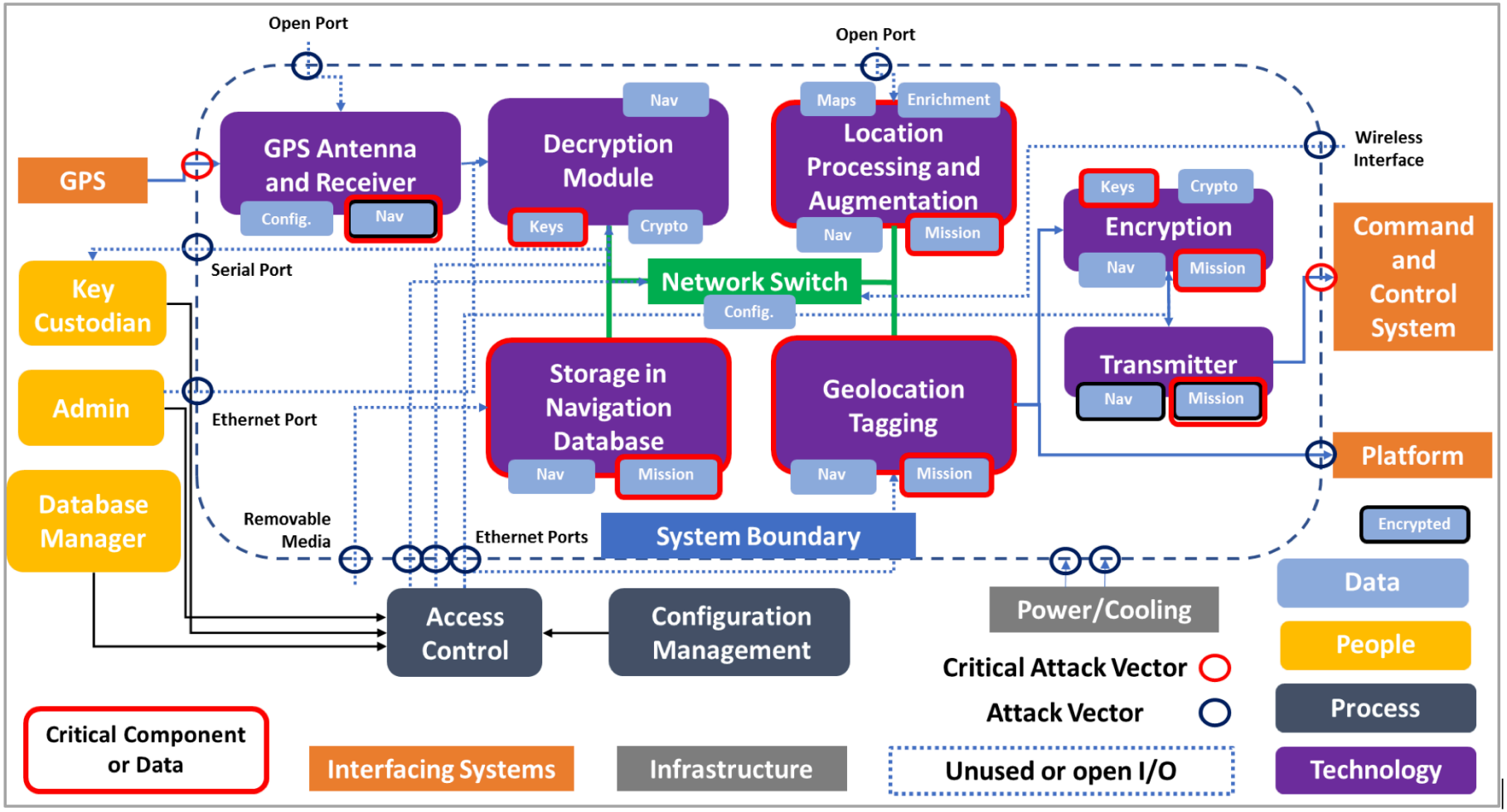
Decompose the mission, conduct dependency analysis, ID key terrain



A notional example from DASD(DT&E)

Attack Surface Characterization Approach

Analyze the attack surface – Ways to access key terrain

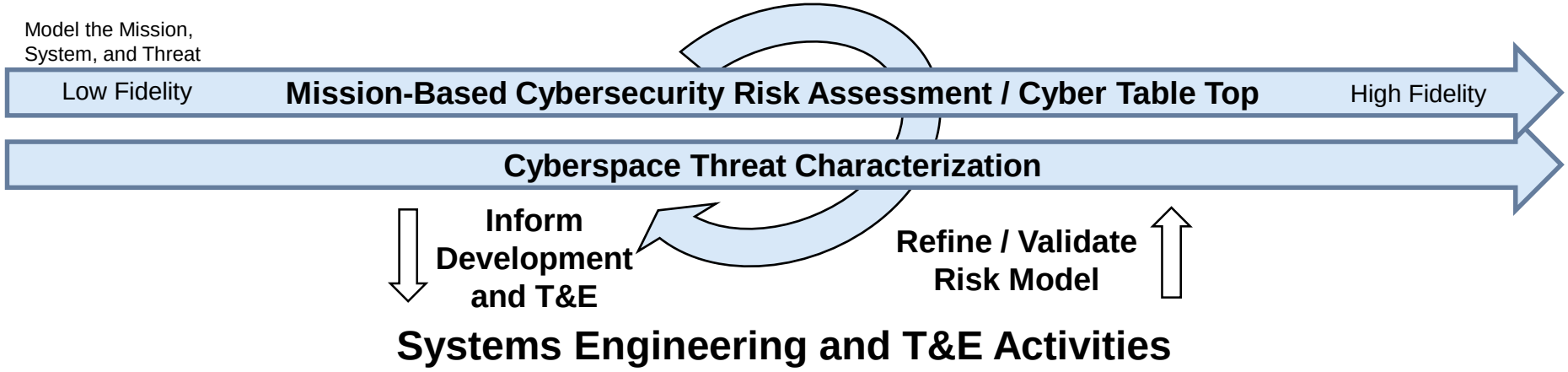


A Notional Example from DASD(DT&E)

Attack Surface Characterization Approach

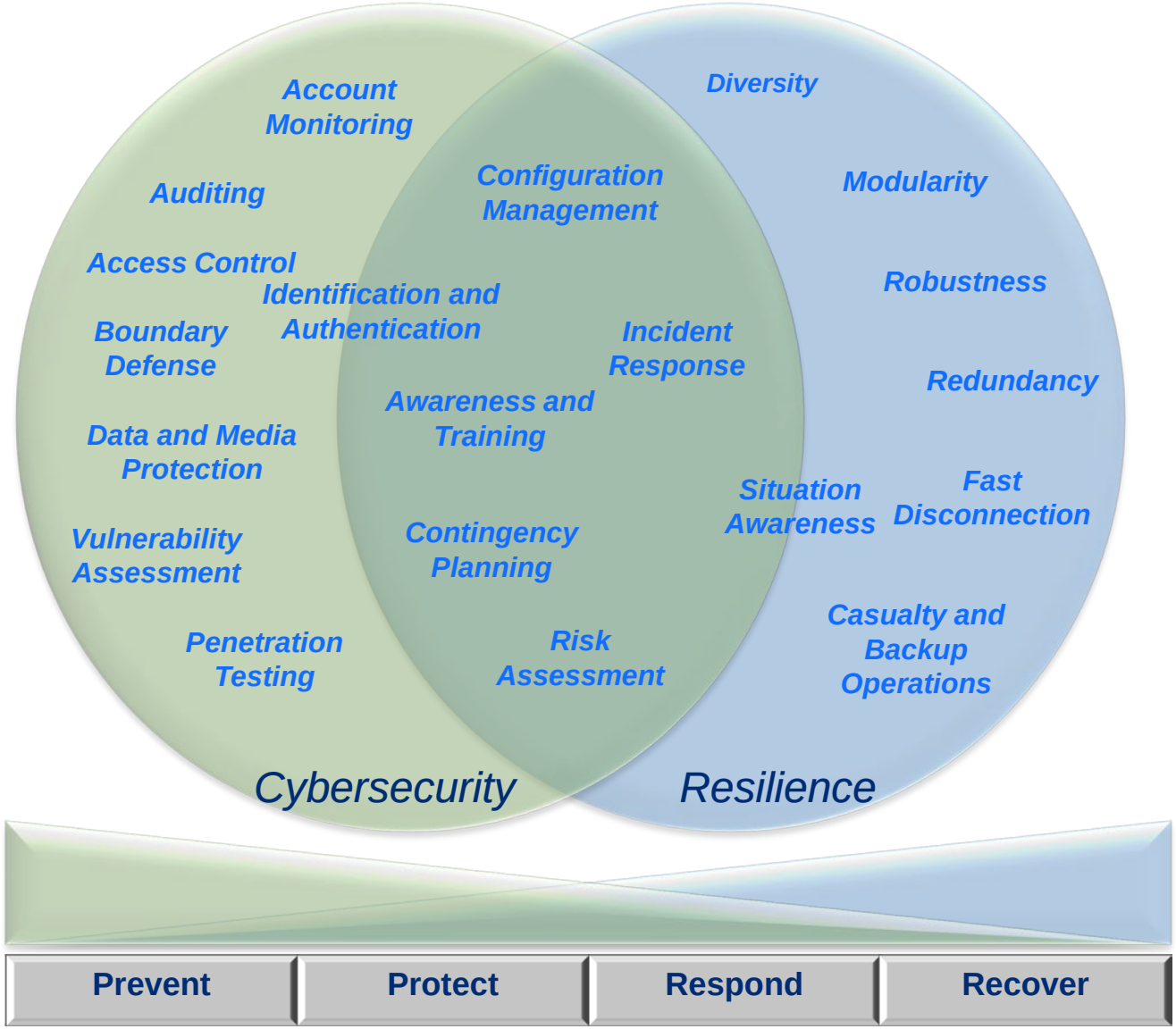
Complete the Attack Surface Analysis

- Complete (or update) your MBCRA
  - Characterize the threat
    - Understand your mission and what the adversaries' objectives would be
    - Consider the "art of the possible"
  - Characterize the mission (from mission decomposition)
  - Characterize the system
  - Characterize cyber risk
- Inform development (e.g. validate cybersecurity requirements)
- Inform cybersecurity T&E planning



Cybersecurity and Resilience

- Similar concerns, different emphasis
- Potential to interfere with or inhibit each other
- Awareness, evaluation, and careful trade-off



Resilient Capabilities

How will you continue to operate when you're compromised?

Feature	Description	Implications for Cyber Resilience
Diversity	Differently designed or implemented modules with (nearly) the same functionality.*	Multiple techniques required to degrade a particular function; can reduce scope of an intended attack.
Modularity	Functions are cleanly encapsulated and dependencies between functional modules are minimized.	Helps contain system failures and negative effects to a single or just a few modules.*
Robustness	System is effective in all or most situations and conditions.	Better able to recover from cyber attacks designed to cause failures; can also be robust against cyberspace-specific conditions like malware propagation and system re-infection.*
Redundancy	Duplicate components provide replacement capability when a primary component fails.*	Minimal if the redundant components are identical; if source of compromise can be removed prior to switchover, can provide rapid reconstitution and recovery.
Fast Disconnection	Ability to rapidly isolate subsystems, modules, or components while they continue to operate. Ideally, to also easily reconnect when the danger has passed.	Ability to continue operating in compromised environments, can also reduce the spread of malware and assist in diagnosing sources of infection.
Situation Awareness	Insight into the current state of the system to operators and to the system itself; includes an awareness of current threats and risks to the system.	Increases the ability to maintain and reconstitute system functions when compromised.
Casualty and Backup Operations	Ensure essential functions are still performed when the system fails or is compromised.	Appearance of a failure may prompt system-degrading actions; operator-performed casualty or backup operations may be isolated from cyber compromise.

*K.J. Hole, Anti-fragile ICT Systems, Springer, 2016, [online] Available: http://link.springer.com/book/10.1007/978-3-319-30070-2.

Discussion

Cyber T&E: Requirements Verification vs. Vulnerability Discovery

JOHNS HOPKINS

APPLIED PHYSICS LABORATORY