Resilience for Weapon System Cyber Defense

30 March 2017

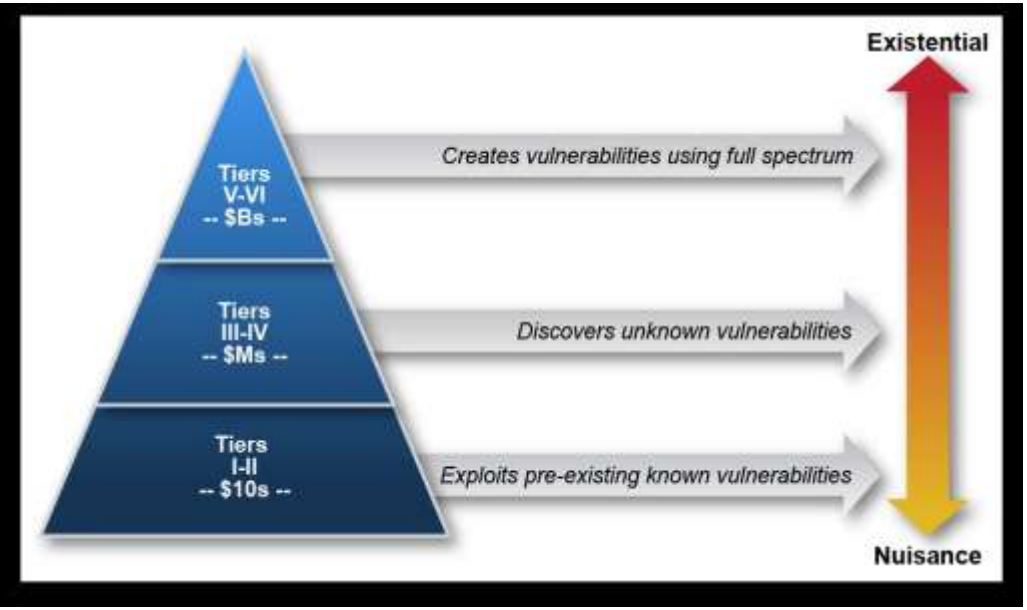
Rose Daley
JHU/APL
Rose.Daley@jhuapl.edu

JOHNS HOPKINS
APPLIED PHYSICS LABORATORY

Topics

- Cyber Environment
- Resilience and Cyber Resilience
- System and Program Resilience
- Implications for Test and Evaluation

Cyber Threat in a Nutshell



- **Tiers I and II attackers primarily *exploit known* vulnerabilities**
- **Tiers III and IV attackers are better funded and have a level of expertise and sophistication sufficient to *discover new* vulnerabilities in systems and to exploit them**
- **Tiers V and VI attackers can invest large amounts of money (billions) and time (years) to *actually create* vulnerabilities in systems, including systems that are otherwise strongly protected.**

Tier	Description
I	Practitioners who rely on others to develop the malicious code, delivery mechanisms, and execution strategy (use known exploits).
II	Practitioners with a greater depth of experience, with the ability to develop their own tools (from publically known vulnerabilities).
III	Practitioners who focus on the discovery and use of unknown malicious code, are adept at installing user and kernel mode root kits[10], frequently use data mining tools, target corporate executives and key users (government and industry) for the purpose of stealing personal and corporate data with the expressed purpose of selling the information to other criminal elements.
IV	Criminal or state actors who are organized, highly technical, proficient, well funded professionals working in teams to discover new vulnerabilities and develop exploits.
V	State actors who create vulnerabilities through an active program to “influence” commercial products and services during design, development or manufacturing, or with the ability to impact products while in the supply chain to enable exploitation of networks and systems of interest.
VI	States with the ability to successfully execute full spectrum (cyber capabilities in combination with all of their military and intelligence capabilities) operations to achieve a specific outcome in political, military, economic, etc. domains and apply at scale.

DSB TASK FORCE REPORT, Resilient Military Systems and the Advanced Cyber Threat, 2011

Cyber Threat in a Nutshell

Weapons systems are intentionally targeted by well-provisioned, sophisticated adversaries

- **Tiers I and II attackers primarily *exploit known* vulnerabilities**
- **Tiers III and IV attackers are better funded and have a level of expertise and sophistication sufficient to *discover new* vulnerabilities in systems and to exploit them**
- **Tiers V and VI attackers can invest large amounts of money (billions) and time (years) to *actually create* vulnerabilities in systems, including systems that are otherwise strongly protected.**

Tier	Description
I	Practitioners who rely on others to develop the malicious code, delivery mechanisms, and execution strategy (use known exploits).
II	Practitioners with a greater depth of experience, with the ability to develop their own tools (from publically known vulnerabilities).
III	Practitioners who focus on the discovery and use of unknown malicious code, are adept at installing user and kernel mode root kits[10], frequently use data mining tools, target corporate executives and key users (government and industry) for the purpose of stealing personal and corporate data with the expressed purpose of selling the information to other criminal elements.
IV	Criminal or state actors who are organized, highly technical, proficient, well funded professionals working in teams to discover new vulnerabilities and develop exploits.
V	State actors who create vulnerabilities through an active program to “influence” commercial products and services during design, development or manufacturing, or with the ability to impact products while in the supply chain to enable exploitation of networks and systems of interest.
VI	States with the ability to successfully execute full spectrum (cyber capabilities in combination with all of their military and intelligence capabilities) operations to achieve a specific outcome in political, military, economic, etc. domains and apply at scale.

DSB TASK FORCE REPORT, Resilient Military Systems and the Advanced Cyber Threat, 2011

Essentials of a Cyber Attack

- **Successful cyber attackers must:**
  - **Perform reconnaissance, gain access, maintain presence, take action**
  - **Operate covertly**

Gain Access	Maintain presence	Take action

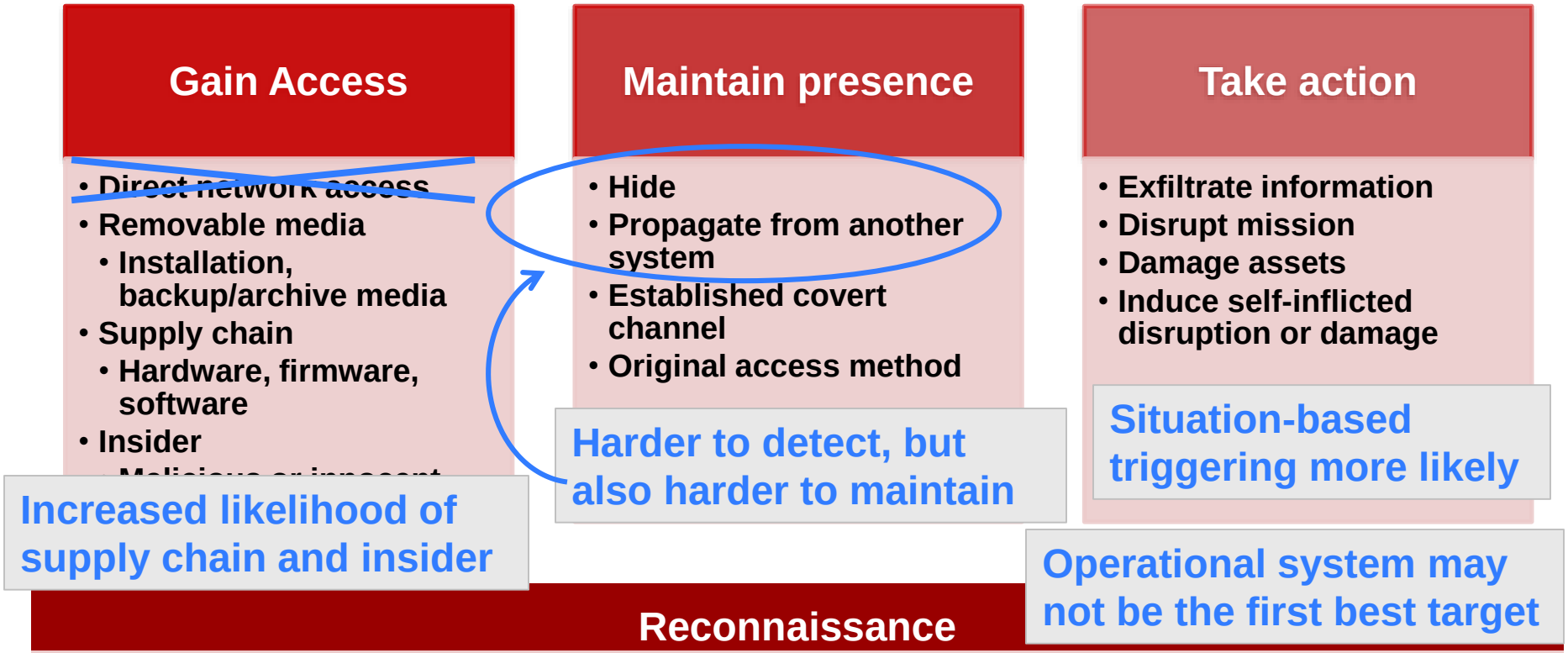
• Direct network access
• Removable media
  • Installation, backup/archive media
• Supply chain
  • Hardware, firmware, software
• Insider
  • Malicious or innocent
	• Hide
	• Propagate from another system
	• Established covert channel
	• Original access method
		• Exfiltrate information
		• Disrupt mission
		• Damage assets
		• Induce self-inflicted disruption or damage

Reconnaissance

- For intelligence gathering, status monitoring, effectiveness assessment
- Externally available information, remote scanning, internal scanning/mapping/exfil, beaconing

Essentials of a Cyber Attack for Protected Systems

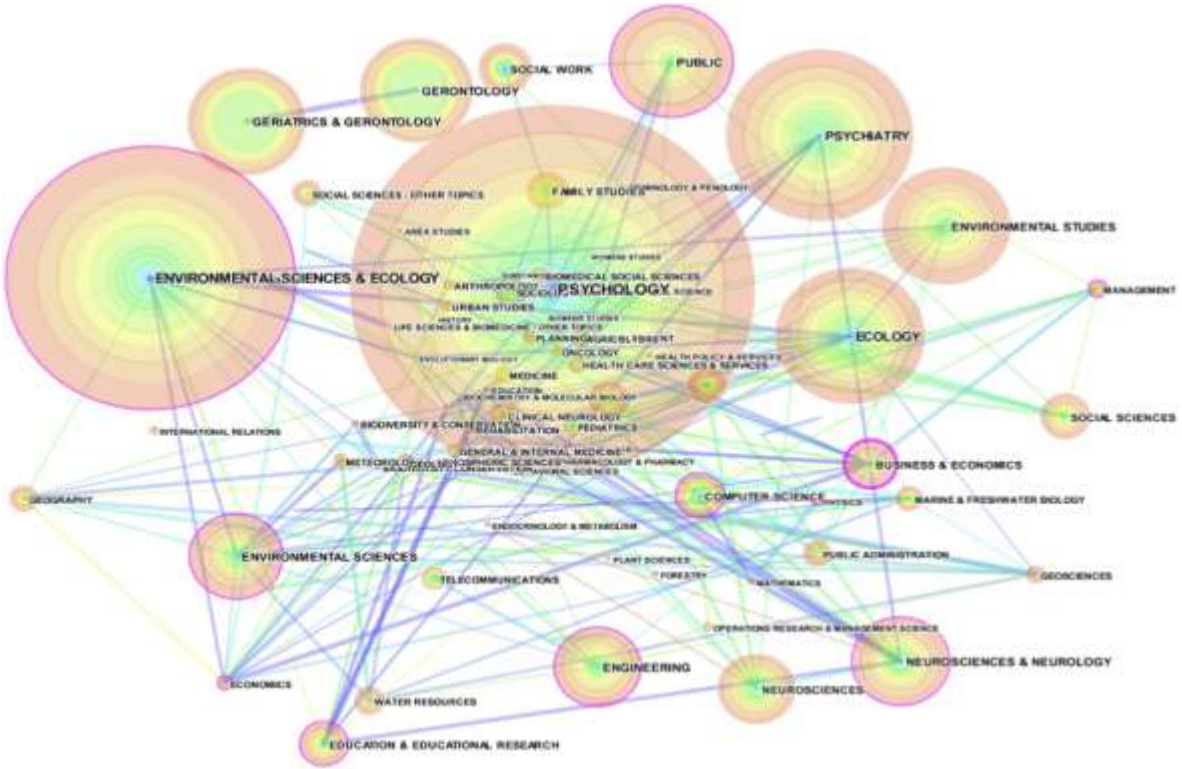
- Systems on secure networks or isolated via an air-gap reduce adversary's capability for direct manipulation
- Change the profile of malicious activities, but do not eliminate them



Resiliency Provides Options

- **Resiliency**
  - Achieve mission in the face of disturbances
  - "Fight through" an event that cannot be prevented and then recover
- **Attributes:**
  - Anticipate and mitigate potential attacks and failures
  - Withstand unanticipated attacks and failures
  - Recover from impactful attacks and failures
  - Evolve based on changing attacks and capabilities
- **Cyber Considerations:**
  - Intentional, covert, remote action
  - Virtual domain, not governed by physical laws
  - Mostly what didn't happen

Resiliency is NOT New



Hosseini, S., Barker, K., & Ramirez-Marquez, J. E. (2016). A review of definitions and measures of system resilience. Reliability Engineering & System Safety, 145, 47–61cc

Resilience Papers by Domain, 2000-2015, CiteSpace

Features ….

Good Engineering

- **Anticipate**
- **Withstand**
- **Recover**
- **Evolve**

Through:

- **Diversity**
- **Modularity**
- **Robustness**
- **Redundancy**
- **Fast Disconnection**
- **Situation Awareness**
- **Casualty/Backups**

System Resiliency and Cyber Resiliency

Traditional System Resiliency

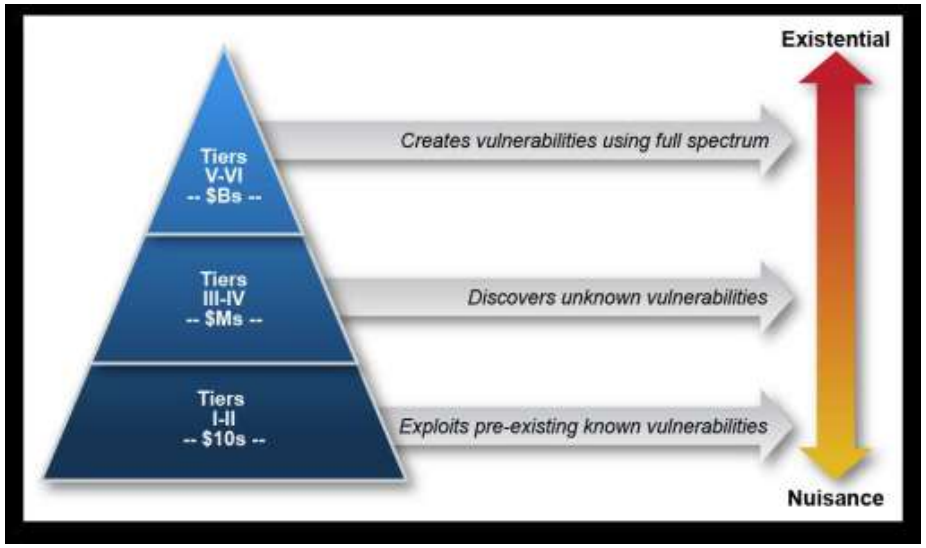
- Focused on resilience to unexpected events
  - Faults/failures and battle damage
  - Data corruption (integrity) and system availability
  - Safety
  - Graceful degradation outside designed performance envelope
- Kinetic weapons arsenals and physical faults/failures relatively well-understood
- Confidentiality, if considered, handled separately

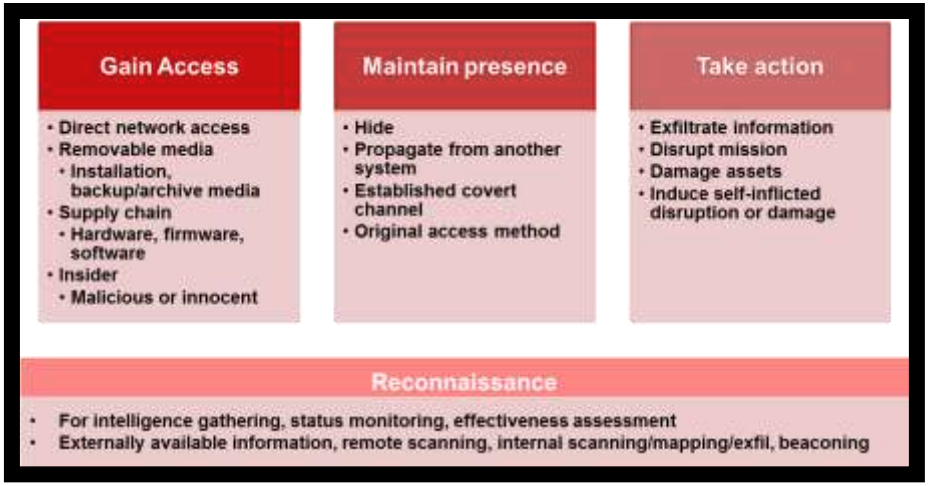
Cyber Resiliency

- Existing resilience features not always effective in cyberspace
  - Physical redundancy is not cyber redundancy
  - Adversary can trigger casualty modes/procedures to reduce capability
- Cyber weapons "one and done" and evolve rapidly
  - Hard to predict adversary capability
  - Hard to predict all of the effects
- Confidentiality is always a concern

Cyber Resiliency Extends Beyond the System

- **System Resiliency**
  - Persistence of designed functions and performance
  - In the face of disturbances both known and unknown (mission survivability)
- **Program Resiliency**
  - Persistence of capabilities throughout the complete program lifecycle supporting the system
  - In the face of uncertainty at the program level (threats and failures to system and support structure)





What is a Resilient Program?

A Resilient Program Provides Overarching Support and Coordination

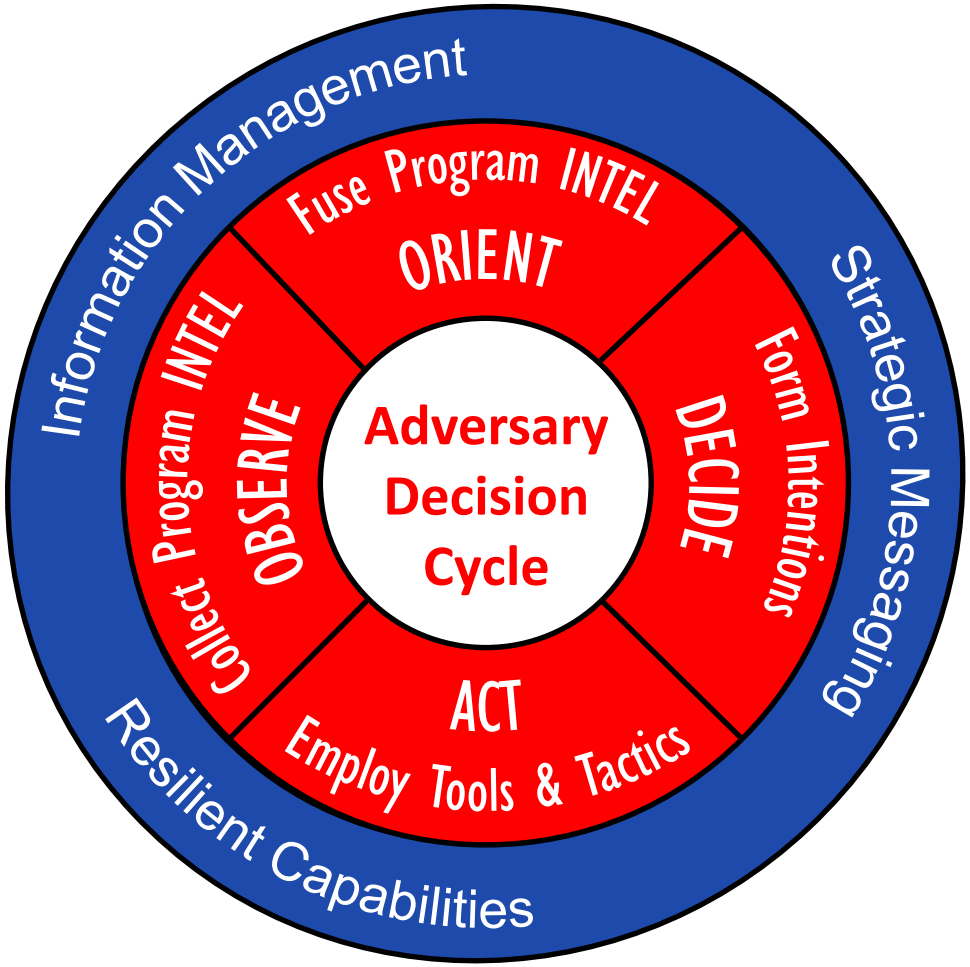
A Program of Record (POR) with:

- ***resilient capabilities*** **exhibiting robust, agile, and responsive elements**
- **actively addressing rapidly evolving adversary kill chains**
- **proactively managing all-source risk**
- **and intentionally influencing all internal and external program information flow.**

- ***Know System and Program Details***
  - ***Identify and Define System Interdependencies***
  - ***Comprehensively Understand Program Information and Implications***
- ***Shape Information for Defender's Advantage***
  - ***Information Management (Control Our Information)***
  - ***Strategic Messaging (Influence Adversary Understanding)***
- ***Define Solutions for Rapid Evolution and Improvement***
  - ***Resilient System Capabilities***
  - ***Aggressive Testing***

Cyber Decision Cycle Defeat

Continuous, Integrated Disruption of the Adversary's Decision Process Throughout Our Program Lifecycle

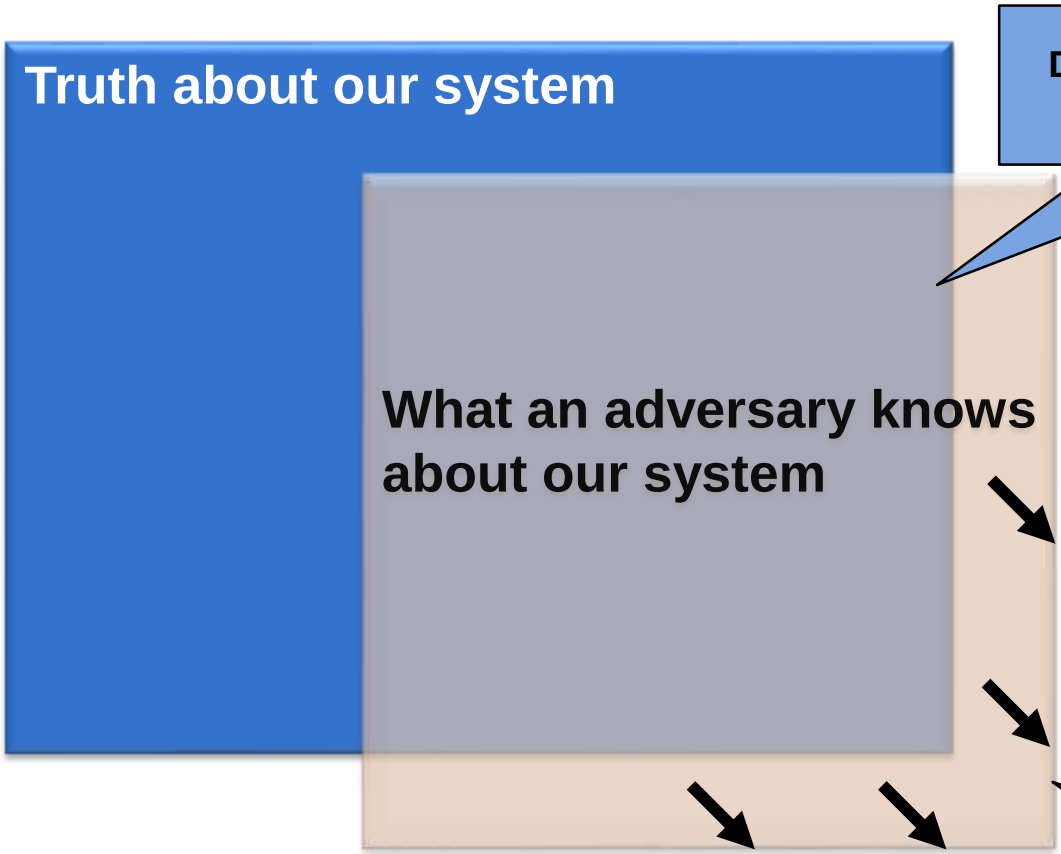


Strategic Messaging
Disrupt Adversary Decision-making

Resilient Capabilities
Disrupt Adversary Measures and Counter Measures

Information Management
Actively Control Data and Disrupt Adversary Data Collection

Obscure System Knowledge for Adversary



Decrease their knowledge or increase their uncertainty

Increasing the difference:

- ***Successful protection***
- ***Incomplete adversary collection***
- ***Successful deception***

Increase their errant knowledge

Obscuring Adversary Knowledge Requires Intelligence Collection and Understanding of the Adversary

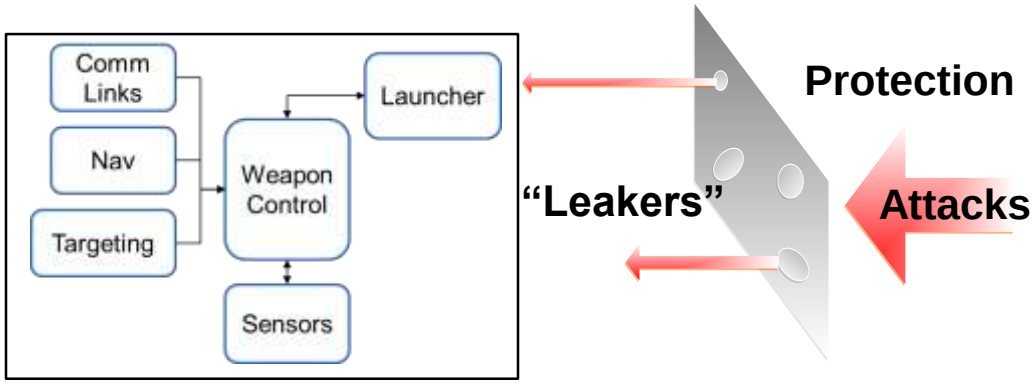
Threat Intelligence is Critical

- **Intelligence needs for *acquisition* and *engineering*:**
  - **What do our adversaries know about our systems?**
  - **How do attackers use system features for attacks?**
  - **What do we expect the threat environment to look like after the system is deployed? Five years later?**
  - **What future attacks/exploits should our system be prepared to handle?**

- **Challenges:**
  - **Intelligence collection and analysis tends to be based on threat actors, vulnerabilities/exploits, or specific components**
  - **Typically, analysis is performed at highest classification levels, then declassified**
  - **Analysts are rarely assigned to or gain in-depth familiarity with programs**
  - **Threat evolution requires continuous monitoring, collection and analysis**
  - **Today's low confidence intel may be high confidence by the time the system is operational**

Construct for Solutions

Apply Capabilities Quickly and Efficiently within Program Structures



Defense Framework

Protection	Detection	Respond (in situ)	Recovery (on board)
Reduce COTS vulnerabilities	Data collection	Use available tools	Scanning and cleaning
Reduce system vulnerabilities	On-board diagnostics	Enclaves/ partitions	Rebooting/ Rebuilding
Smart software assurance	On-board detection & alerting	Isolation/ New capabilities	Casualty Procedures …
Reduce propagation ability	Shore-based analysis		

Cyber Defense = Protection + Detection + Response + Recovery

Programmatic Mapping

Near-Term (Onboard Now or Easily Incorporated)

- Technical
  - Software
  - Network
- Operational
  - Cyber Awareness
  - Casualty Procedures
  - Training
- Other

Mid-Term (Incremental Upgrades)

- System-level Cyber Resiliency
  - Backup
  - Redundancies
  - Isolations
  - Manual Backups
  - Recovery
- Other

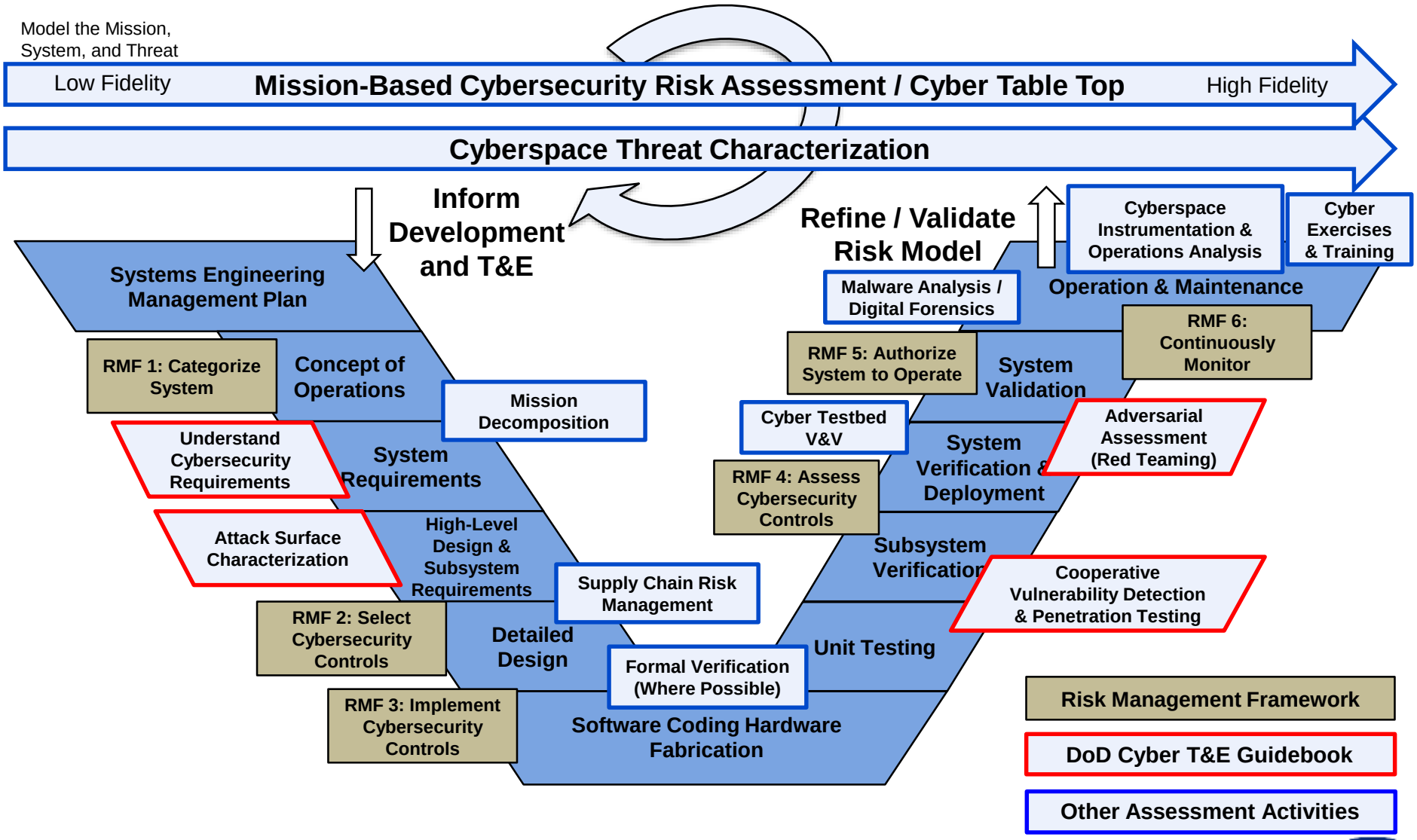
Long-Term (Major Upgrades)

- Cyber System/Network Architectures
  - Remove non-essential connections
  - Network
- Inherent Cyber Resiliency
  - Trust points to detect, recover, restore from events
- Next-Gen Trustworthy Platforms

System Engineering

- ***Requirements***
- Priorities/Criticalities,
- Architecture/Design,
- Data Analysis, Forensics,
- Test-beds, Test and Evaluation,
- … (Other Necessary Activities)

System Cybersecurity Assessment & T&E Activities



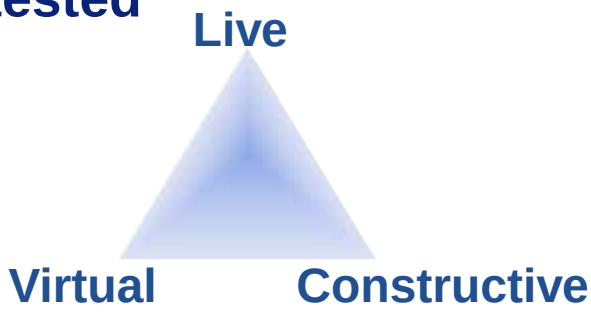
Implications for Test and Evaluation

Testbeds are Practice Targets

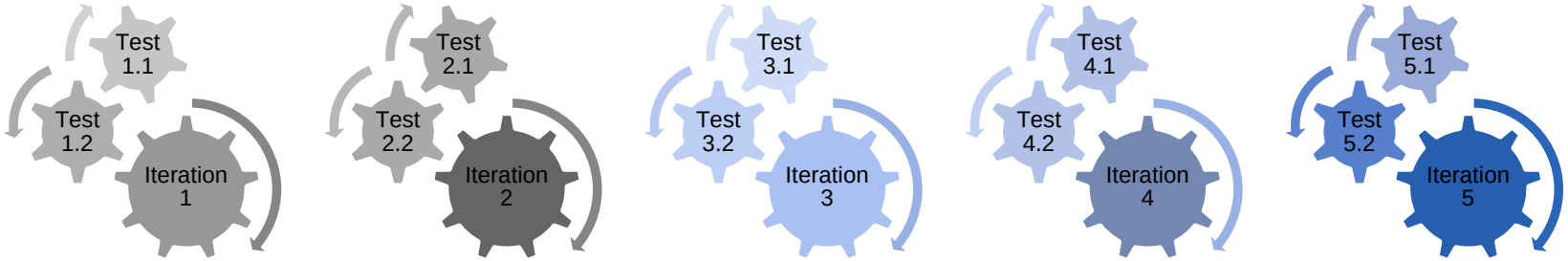
- Weapons systems are hard targets
- Testbeds can provide opportunities for adversaries
  - Reconnaissance, weaponization
  - More reliable remote access
  - Ability to “hide in the noise”
  - Unusual situations
  - Test equipment
- Can also provide opportunities for us
  - Monitor for adversary activity
  - Deception/disinformation

Cyber Attacks Can Be Destructive

- **Countermeasures and mitigations must be tested**
  - **Models with sufficient fidelity**
  - **Emulators**
  - **Live hardware**
    - **Life cycle support and spares**



- **Time to reconstitute/reconfigure is a factor**
  - **Drives achievable length and quantity of test runs**
    - **Significant number of test runs/configurations can be required**
    - **Higher degree of unpredictable results can occur**
- **Models used for development may be expanded**
  - **Evaluate for features relevant to cyber fidelity**



People Are Essential to the Solution

- **System Operators**
  - New and existing capabilities to:
    - Recognize potential cyber event
    - Diagnose potential cyber event
    - Respond (with platform capability)
    - Recover (with platform capability)
  - How to evaluate effectiveness?
  - How to evaluate mitigations with humans-in-the-loop?
  - Realistic representation of operator skillsets?
  - Realistic representation of cyber events?

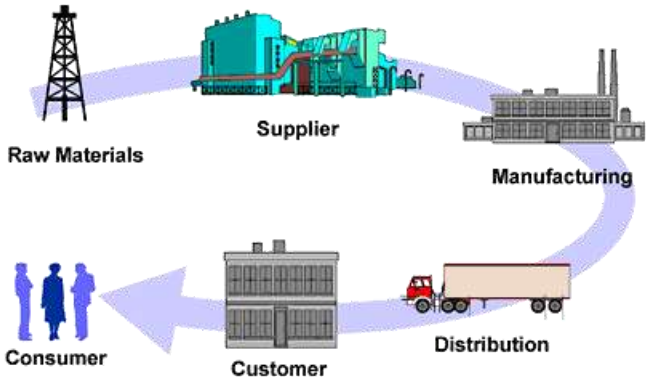
United States Navy, Wikipedia Commons ID 031227-N-7408M-001

- **Engineering/T&E Personnel**
  - Augment skillsets of current personnel
  - Existing domain knowledge + cybersecurity
    - Required training packages, team composition
  - Incorporate cyber specialists only where necessary
    - Red team, penetration testing, attack surface characterization
    - Integration/interaction with system's engineers

Evaluating Countermeasures for Supply Chain, Insider

Supply chain and insider attacks are a significant concern

- **Test and evaluate:**
  - **Response (system and personnel)**
  - **Mitigations and countermeasures**
  - **E.g., mitigations during system development—tested when?**
- **Targeted effects:**
  - **E.g., Situation-based triggering—before and after deployment**
- **Personnel are insiders**
  - **Vigilance against insider and supply chain**
  - **Anti-tamper in test facilities**
    - **Technology, processes and people**
  - **…**



Questions?