DHS SCIENCE AND TECHNOLOGY

Accelerating Cybersecurity Test

Mr. Alex Hoover
Associate Director for Cybersecurity Engineering
Office of Systems Engineering and Standards
Science and Technology Directorate

Homeland Security
Science and Technology

Cybersecurity Test and Evaluation Challenges

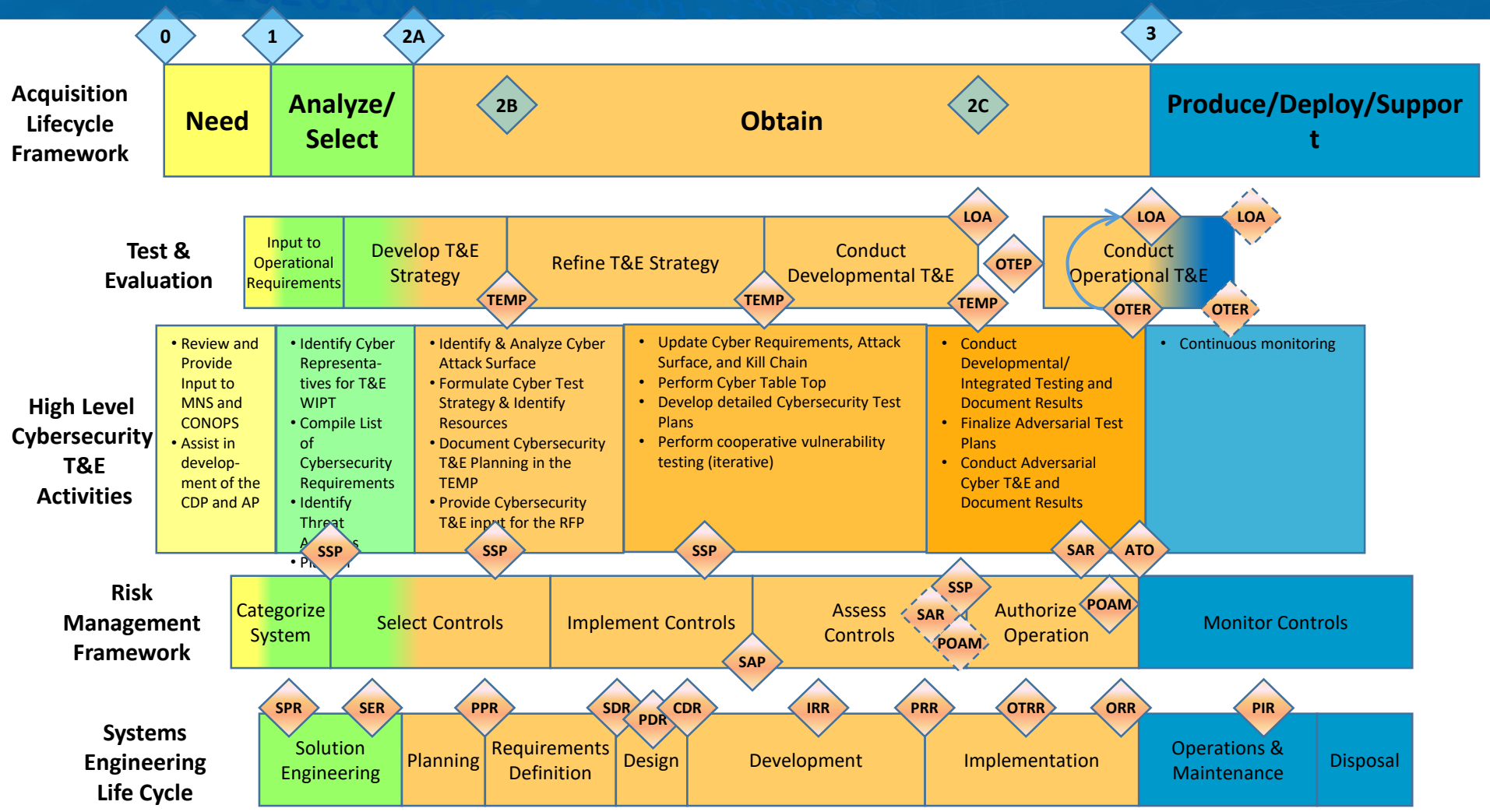
- Multidisciplinary Activity
- Many “Pigs at the Trough”
- Numerous Technical Standards
- No Mission-based Requirements
- Requires Operational Analysis
- Lack of Threat Focus
- No Adversary Stakeholders
- Volatile Parts of the Environment
- Recurring Limitations
- *Nie mój cyrk, Nie moje małpy*

Cybersecurity Test and Evaluation Imperatives

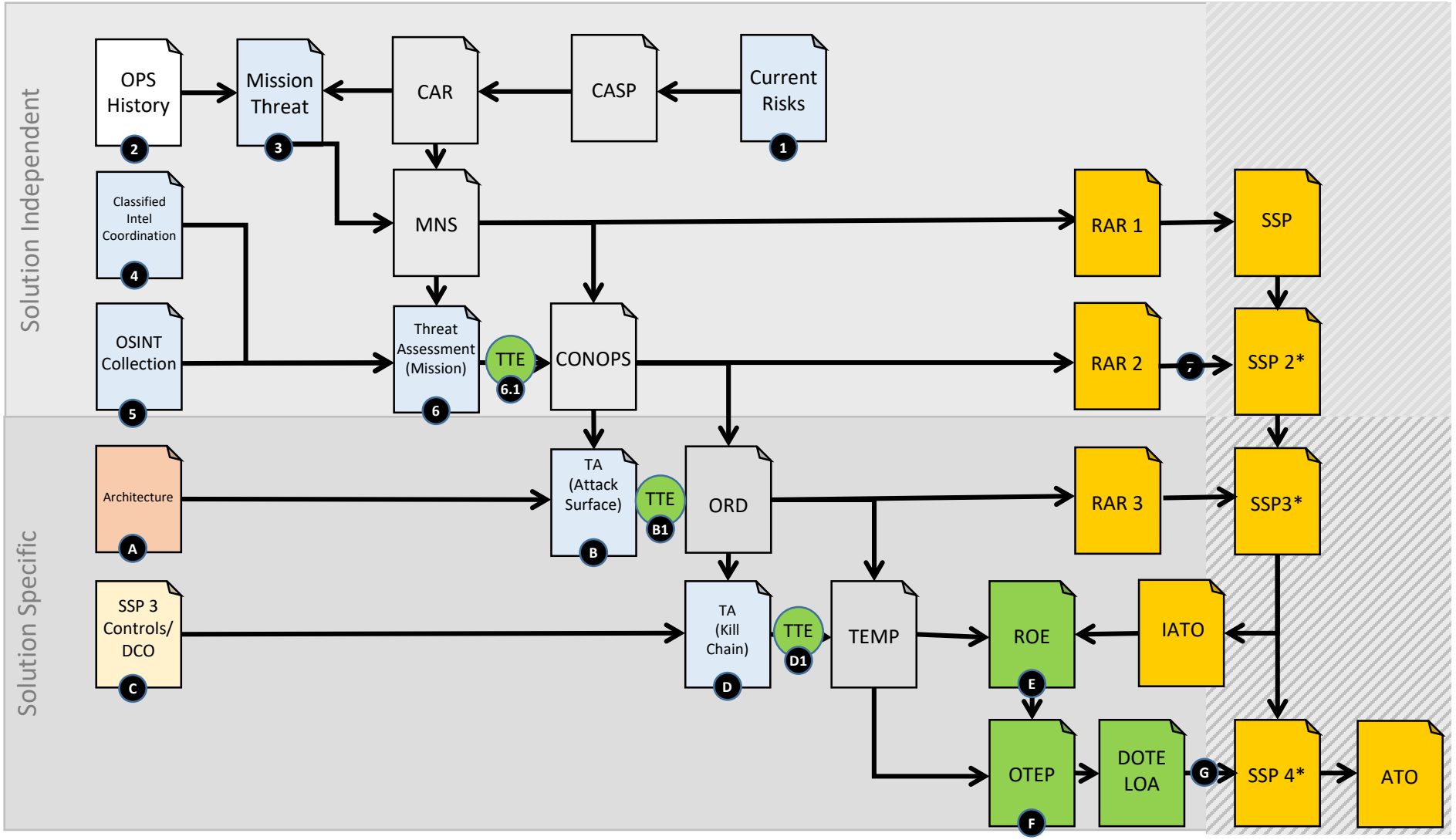
- Threat assessments provide context
- Performance modelling sets the foundation
- Operational requirements drive SE

- Operational requirements drive T&E
- RMF and T&E are mutually supportive
- Use of “ranges” can mitigate many recurring limitations
- Cybersecurity OT&E is more than penetration testing

Acquisition / SE / T&E / RMF



Implementation of Threat Assessment Information Flow



Acronyms

RAR – Risk Assessment Report

SSP-System Security Plan

CASP – Capability Analysis Study Plan

CAR – Capability Assessment Report

OSINT – Open Source Intelligence

DCO – Defensive Cyber Operations

OTEP – Operational Test and Evaluation Plan

DOTE LOA – Operational Test Letter of Assessment

Threat Assessment

Mission – What?

Attack Surface – Where?

Kill Chain
– When & How?

*SSP iterative updates

Why Are We Vulnerable?

Information technology is like any other tool. Any tool that has a legitimate use can be misused.

Why This Approach is Needed?

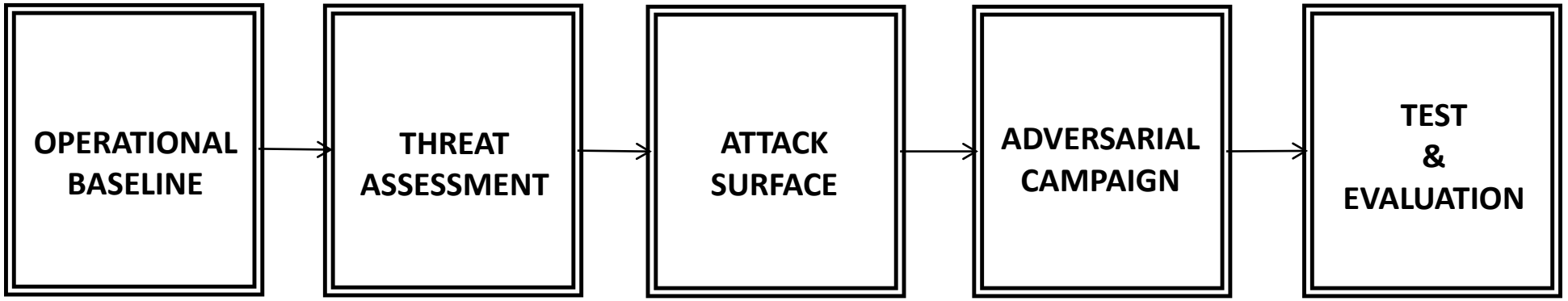
I've installed a lock on my front door

is different than

I can keep people out of my house

Operational Compromise Baseline

How to Approach Security



- Threat Assessment – Actors, Intent, Capabilities
- Attack Surface – Connecting Red and Blue Operations
- Adversarial Campaign – The Red CONOPS/TTP
- Resilience Performance Assessment - Feedback

Threat Assessment (1/3)

- Characterization of the Actors, their Intent and Capabilities seeking to subvert the IT supported mission
- Foundation is a series of process flows from the CONOPS for the capability being assessed
- Every security concern should tie back to a specific mission process from the CONOPS
  - Later, mapped to a specific part of the process based upon the solution

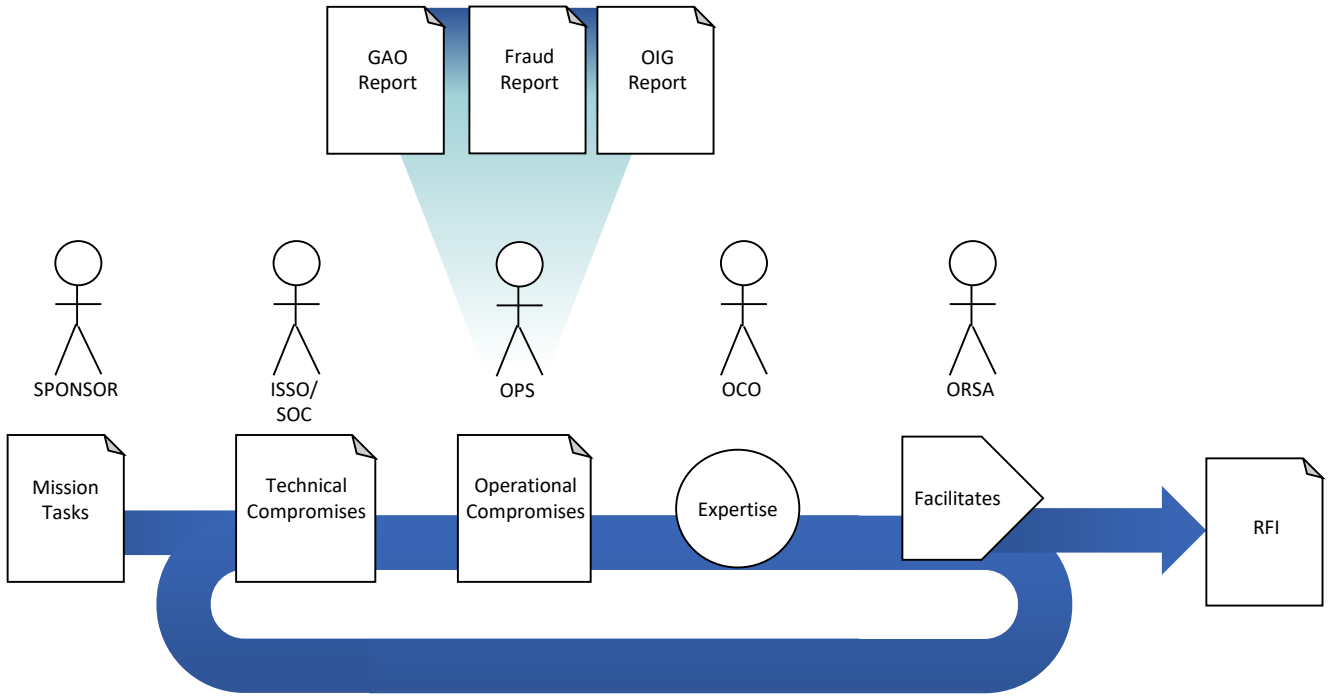
Threat Assessment (2/3)

- Key information comes from Open Source and Classified Intelligence
- Inputs are beholden to the operational process to have relevance
- Efforts need to be focused on the important lines of effort described in the CONOPS (and ensuing process documents)
- Known compromises are an important source of operational context for the Intelligence efforts
- Basic resources should include:
  - Security Operations Center
  - Inspector General, GAO, and other similar reports
  - Current operational fraud/inspection process

Threat Assessment (3/3)

- Must relate known compromises to the appropriate processes for consistency and completeness
  - A past IT technology may not exist in the new solution
  - A currently manual process may be automated
- Threat Actors' intent will remain relatively constant regardless of the changes in the IT mission support solution
- Threat will likely continue to attempt to compromise the mission process, independent of how it is implemented
- A best practice is to execute the Intelligence analyses sequentially and feed one from the other
  - Likely easiest to feed the Classified Intelligence analysis from the Open Source

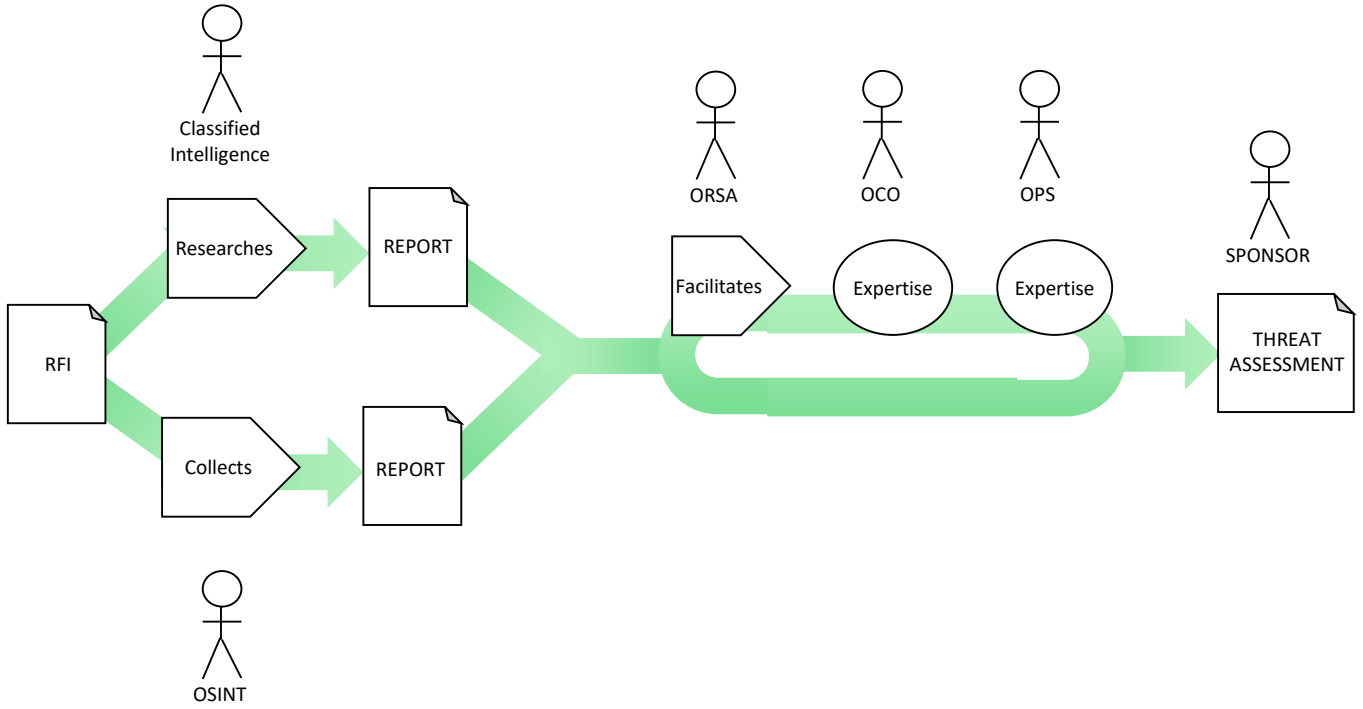
Establish Operational Baseline



Baseline KSA

- **Sponsor** – Provides an understanding of the mission context for the solution. The CAR and MNS should provide this information, possibly a P-CONOPS.
- **ISSO/SOC** – Provides an understanding of the environment for the current solution (if any) and the projected environment.
- **OPS** – The Operators provide knowledge about current known compromises to the *mission*. This knowledge should come from organic sources like audits, fraud reports, or Component counter intelligence organizations.
- **OCO** – Offensive Cyber Operations provides insight into known cyber operations techniques, tactics, and procedures. This facilitates a clear understanding of threat objectives.
- **ORSA** – An Operations Research/Systems Analyst facilitates the SME in developing a Request For Information that will describe the threat space from an operational, threat, and environmental perspective.

Conduct Threat Assessment



Threat Assessment KSA

- **Classified Intelligence** – The classified intelligence organization (I&A, a Component Intelligence Branch, an external partner) provides classified intelligence, with appropriate tearlines, that answers the RFI questions.
- **OSINT** – The Open Source Intelligence collection provides information from open source venues such as the open web, the deep web, and the dark web. This could be through an intelligence organization, an organic Component branch, or an external organization like a contractor, FFRDC, or UARC.
- **ORSA** – An Operations Research/Systems Analyst facilitates the SME in developing a Request For Information that will describe the threat space from an operational, threat, and environmental perspective.
- **OCO** – Offensive Cyber Operations provides insight into known cyber operations techniques, tactics, and procedures. This facilitates a clear understanding of key cyber terrain.
- **OPS** – The Operators provide context to the collected threat information, especially weighing the importance of different risks.
- **Sponsor** – The Program Sponsor synthesizes the results of the threat analysis so that it will support program documents like the CONOPS and ORD to inform developers of how the threat operates in the intended environment.

Threat Actor Intent

- Denial – Blocking completion of mission tasks.
- Degradation – Decreasing the speed, quality, or other performance characteristics for mission tasks.
- Manipulation – Altering the information available to decision makers.
- Exfiltration – Gaining information about mission details to be exploited against other assets.
- Pivot – Using access to one system/network to gain access to a partner system/network.

Threat Actor Capabilities – Knowledge

	Minimal	Limited	Moderate	Advanced
General Systems	Home market hardware, networks and, general-purpose languages. Basic user OS and applications. Public cryptography/ authentication. Public exploits of known vulnerabilities.	Common hardware, firmware, and defensive devices. Enterprise network and OS. Industry data protocols. 0-day exploits of less common/more vulnerable software, custom software.	Custom hardware, embedded systems, and less common network/protocols, specialized firmware. Biometric-based authentication. 0-day exploits of more common/less vulnerable software.	Classified systems, platforms, and software. Cross-domain devices, cryptography and associated hardware. 0-day exploits of restricted government systems and industrial control systems.
Target Network and Systems	Information found from commonly available open sources or from external reconnaissance of target organization.	Knowledge of network and system specifications and type/configuration of host-based defenses equivalent to an authorized user in the target environment.	Knowledge of network and system specifications and type/configuration of networked defenses equivalent to an authorized administrator in the target environment.	Knowledge of network and system specifications and defenses equivalent to an authorized domain administrator in the target environment.
Target Operations	Information found from commonly available open sources or from external reconnaissance of target organization.	Knowledge from more specialized literature or equivalent to prior experience with target operations, including key information or supporting systems.	Knowledge equivalent to substantial prior experience with target operations, including work flow and sub-task objectives.	Knowledge of current target operations equivalent to an experienced authorized operator.

Threat Actor Capabilities – Tools

	Minimal	Limited	Moderate	Advanced
Hardware	Inexpensive home market hardware.	Hard-ware, clusters, costing $10,000s or dozens of man hours.	Hardware costing $100,000s or hundreds of man hours.	Custom hardware costing $1,000,000s or thousands of man hours.
Software	Freeware and inexpensive commercial tools.	Commercial software.	Custom software, polymorphic malware, rootkits.	Custom software, firmware-resident malware.
Infrastructure	Access through publically available infrastructure.	Direct control of leveraged public infrastructure.	Covert remote access tools and loggers.	Covert close access.

Threat Actor Capabilities – Operations

	Minimal	Limited	Moderate	Advanced
Planning	Opportunistic actions, no planning.	Intent and short-range plans formed on-the-fly as needed.	Organizes one or more operations with specific target systems and associated effects on target organization	Organizes multiple operations against separate targets, synchronizing timing, accesses, and planned second-order effects
Procedures	No demonstrated stealth, non-attribution or efficient use of resources	Countermeasures for common defensive systems. Non-attribution. Efficiency in use of resources consistent with intent.	Advanced and custom non-attribution tools. Efficiency in use of resources consistent with intent	High degree of control of defensive infrastructure. Non-attribution, false flag operations. Efficiency in use of resources consistent with intent
Persistence	Intermittent, directed activity.	Gradual, low level passive operations.	Repeated active operations.	24/7 monitoring and control of offensive capabilities.

Threat Description Example (1/6)

Special Operations: Such a threat could consist of a DoS attack or RF jamming of one or more cell sites to bar WPS/GETS users in a limited geographic area or to only one of the WPS/GETS service providers. This action could be undertaken to potentially compliment a kinetic terrorist attack (e.g., bomb) with the goal of disabling NS/EP wireless (and potentially wireline) services in a given area on one or more service providers to enhance or increase the impact or disruption of the primary attack. However, NS/EP users in such an area of attack will most likely be subscribed to different WPS/GETS providers and therefore not all NS/EP users in the area of attack may be barred from WPS/GETS services or only WPS services on one service provider may be disrupted depending on their multiple frequency resources, area of attack (e.g., urban, suburban, rural), and deployment/density of infrastructure (e.g., small cells). As a result, such an event could be more moderate in frequency but only have the ability to congest a small area around the attack on the order of a mile or so.

Threat Description Example (2/6)

Special Operations: Such a threat could consist of a DoS attack or RF jamming of one or more cell sites to bar WPS/GETS users in a limited geographic area or to only one of the WPS/GETS service providers. This action could be undertaken to potentially compliment a kinetic terrorist attack (e.g., bomb) with the goal of disabling NS/EP wireless (and potentially wireline) services in a given area on one or more service providers to enhance or increase the impact or disruption of the primary attack. However, NS/EP users in such an area of attack will most likely be subscribed to different WPS/GETS providers and therefore not all NS/EP users in the area of attack may be barred from WPS/GETS services or only WPS services on one service provider may be disrupted depending on their multiple frequency resources, area of attack (e.g., urban, suburban, rural), and deployment/density of infrastructure (e.g., small cells). As a result, such an event could be more moderate in frequency but only have the ability to congest a small area around the attack on the order of a mile or so.

Threat Description Example (3/6)

Special Operations: Such a threat could consist of a DoS attack or RF jamming of one or more cell sites to bar WPS/GETS users in a limited geographic area or to only one of the WPS/GETS service providers. This action could be undertaken to potentially compliment a kinetic terrorist attack (e.g., bomb) with the goal of disabling NS/EP wireless (and potentially wireline) services in a given area on one or more service providers to enhance or increase the impact or disruption of the primary attack. However, NS/EP users in such an area of attack will most likely be subscribed to different WPS/GETS providers and therefore not all NS/EP users in the area of attack may be barred from WPS/GETS services or only WPS services on one service provider may be disrupted depending on their multiple frequency resources, area of attack (e.g., urban, suburban, rural), and deployment/density of infrastructure (e.g., small cells). As a result, such an event could be more moderate in frequency but only have the ability to congest a small area around the attack on the order of a mile or so.

Threat Description Example (4/6)

Special Operations: Such a threat could consist of a DoS attack or RF jamming of one or more cell sites to bar WPS/GETS users in a limited geographic area or to only one of the WPS/GETS service providers. This action could be undertaken to potentially compliment a kinetic terrorist attack (e.g., bomb) with the goal of disabling NS/EP wireless (and potentially wireline) services in a given area on one or more service providers to enhance or increase the impact or disruption of the primary attack. However, NS/EP users in such an area of attack will most likely be subscribed to different WPS/GETS providers and therefore not all NS/EP users in the area of attack may be barred from WPS/GETS services or only WPS services on one service provider may be disrupted depending on their multiple frequency resources, area of attack (e.g., urban, suburban, rural), and deployment/density of infrastructure (e.g., small cells). As a result, such an event could be more moderate in frequency but only have the ability to congest a small area around the attack on the order of a mile or so.

Threat Description Example (5/6)

Special Operations: Such a threat could consist of a DoS attack or RF jamming of one or more cell sites to bar WPS/GETS users in a limited geographic area or to only one of the WPS/GETS service providers. This action could be undertaken to potentially compliment a kinetic terrorist attack (e.g., bomb) with the goal of disabling NS/EP wireless (and potentially wireline) services in a given area on one or more service providers to enhance or increase the impact or disruption of the primary attack. However, NS/EP users in such an area of attack will most likely be subscribed to different WPS/GETS providers and therefore not all NS/EP users in the area of attack may be barred from WPS/GETS services or only WPS services on one service provider may be disrupted depending on their multiple frequency resources, area of attack (e.g., urban, suburban, rural), and deployment/density of infrastructure (e.g., small cells). As a result, such an event could be more moderate in frequency but only have the ability to congest a small area around the attack on the order of a mile or so.

Threat Description Example (6/6)

Special Operations: Such a threat could consist of a DoS attack or RF jamming of one or more cell sites to bar WPS/GETS users in a limited geographic area or to only one of the WPS/GETS service providers. This action could be undertaken to potentially compliment a kinetic terrorist attack (e.g., bomb) with the goal of disabling NS/EP wireless (and potentially wireline) services in a given area on one or more service providers to enhance or increase the impact or disruption of the primary attack. However, NS/EP users in such an area of attack will most likely be subscribed to different WPS/GETS providers and therefore not all NS/EP users in the area of attack may be barred from WPS/GETS services or only WPS services on one service provider may be disrupted depending on their multiple frequency resources, area of attack (e.g., urban, suburban, rural), and deployment/density of infrastructure (e.g., small cells). As a result, such an event could be more moderate in frequency but only have the ability to congest a small area around the attack on the order of a mile or so.

Operational Process Modelling

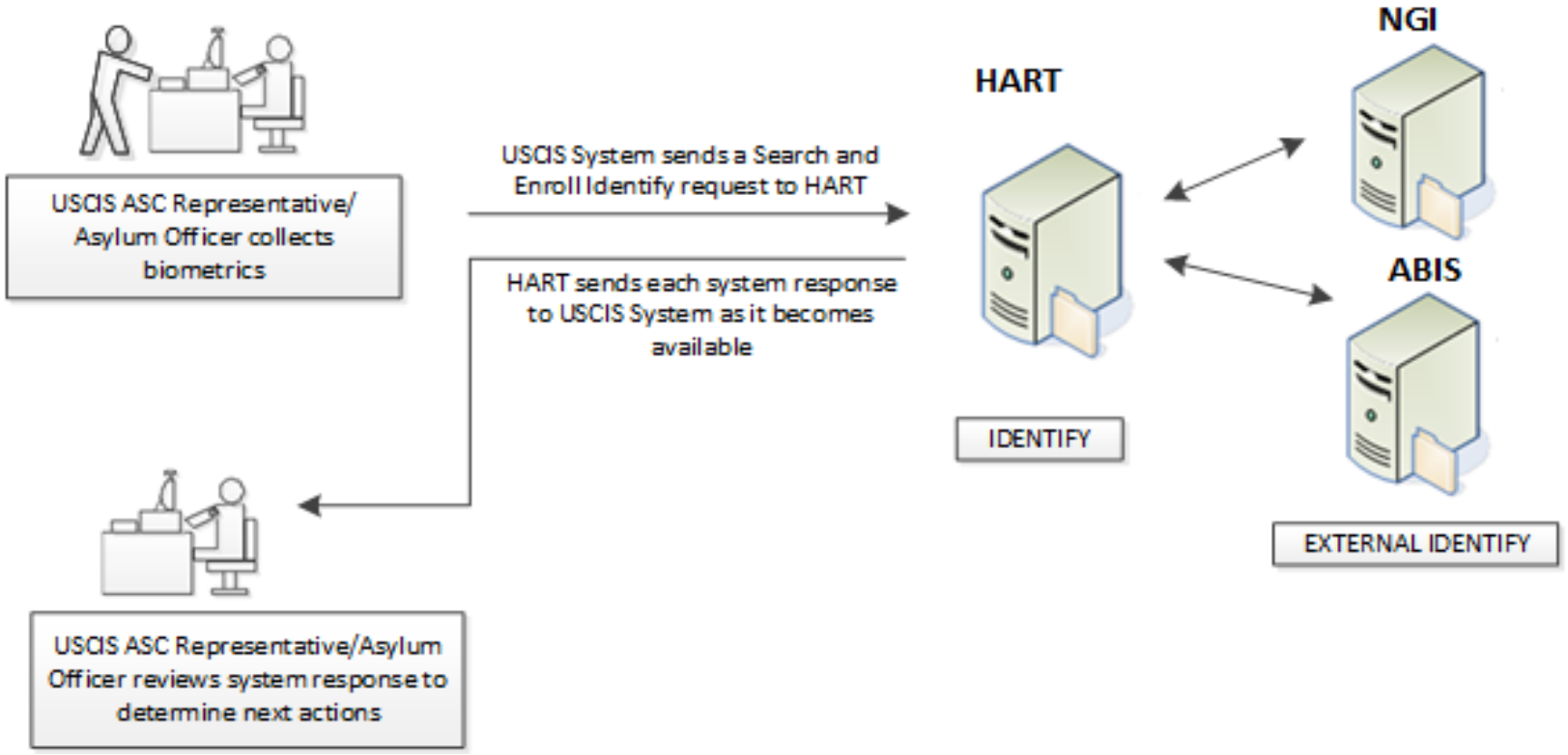
Customer Use Case Example

Homeland Advanced Recognition Technology

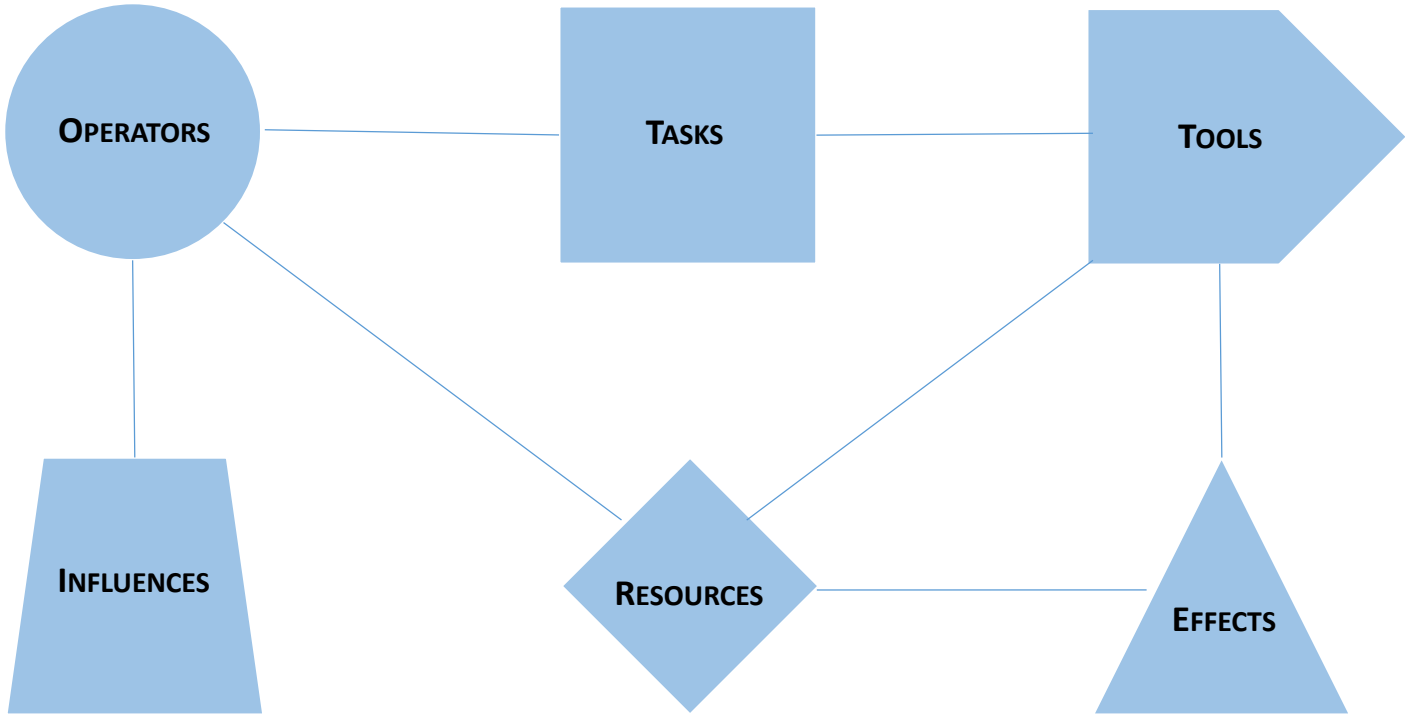
Use Case: USCIS Biometric Enrollment with External Search	
Primary Actor (Persons, Systems)	USCIS ASC Representative/Asylum Officer, USCIS System, OBIM HART System
Secondary Actor (Persons, Systems)	DOJ NGI, DoD ABIS
Goal	The goal is to successfully enroll an individual applying for a USCIS benefit at an Application Support Center (ASC).
Pre-Conditions	• Individual has fingers with readable prints. OR • Individual has readable irises (if fingerprints are not available). • The workstation device is available to the officer and is operational. • The mode of information transmission is operational.
Main Success Scenario Description	• Action 1: USCIS ASC Representative/Asylum Officer collects applicant's available biometrics (fingerprints, iris, and facial) at a workstation. • Action 2: USCIS System submits collected biometrics to OBIM HART with request to search and enroll in OBIM HART and search NGI and ABIS. • Action 3: OBIM HART executes an IDENTIFY with enrollment and generates an EXTERNAL IDENTIFY to NGI and ABIS. • Action 4: OBIM HART sends system responses to USCIS. • Action 5: If a match is not found in OBIM HART, the system creates a new identity with USCIS encounter. If a match is found to an existing identity, OBIM HART associates a USCIS encounter to that identity.
Alternate Scenario Description	• No alternate scenario.
Post-Conditions	• USCIS encounter with submitted biometrics is created in OBIM HART.

Customer Use Case Example (cont'd)

USCIS Biometric Enrollment with External Search (ASC and Asylum)

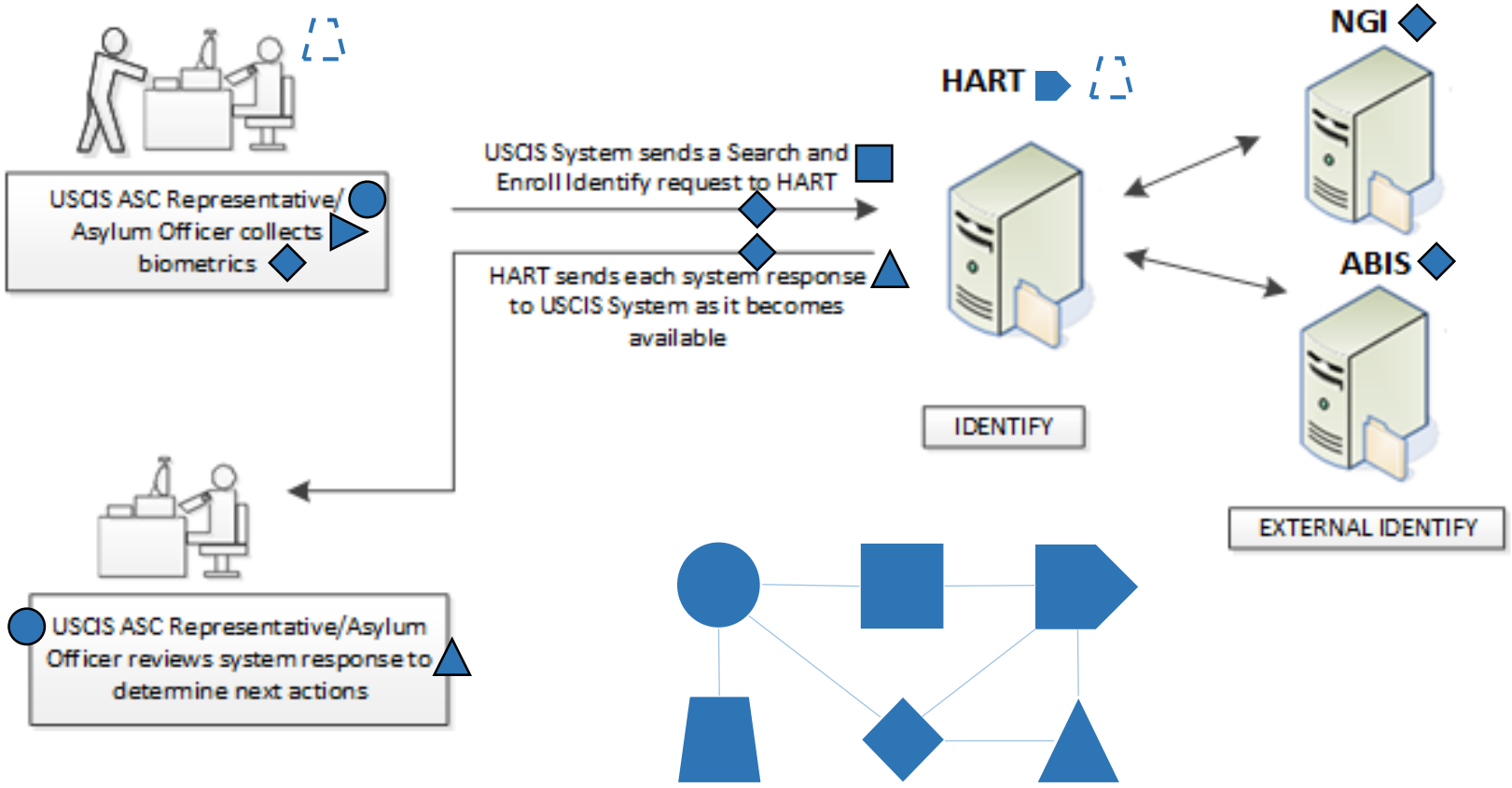


Six Components, Seven Relationships



Customer Use Case Example (cont'd)

USCIS Biometric Enrollment with External Search (ASC and Asylum)



Operational and Technical Attack Surface

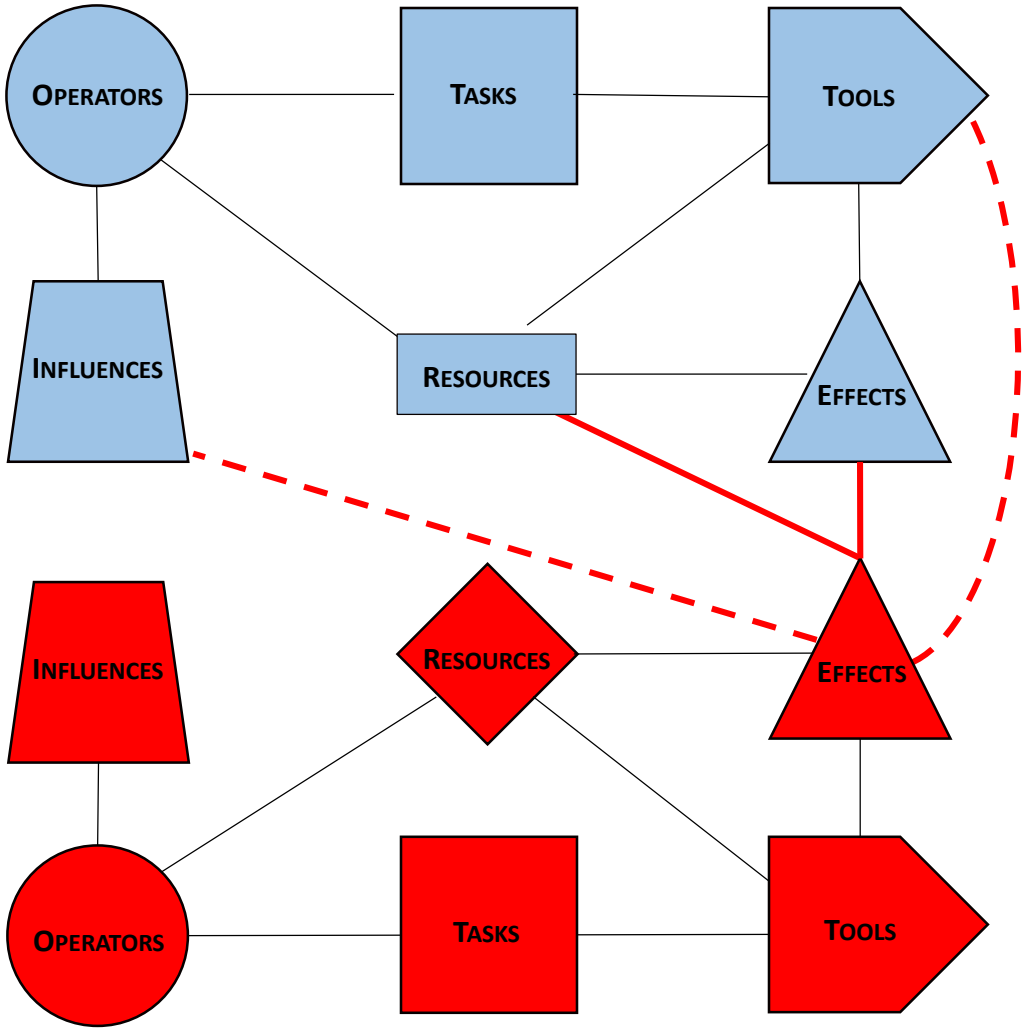
Attack Surface

- Mapping of the Actors' Intent to subvert a mission process on to the (initially notional) Solution Architecture
- Each mission process identified as a "target" in the Intent will map to solution technologies and procedures that support that mission process
- Linking the mission process and Intent to a subset of the Solution Architecture that supports that mission process creates a node in the Attack Surface
- From the adversarial view, Threat Capabilities link to Attack Surface nodes

Attack Surface (cont'd)

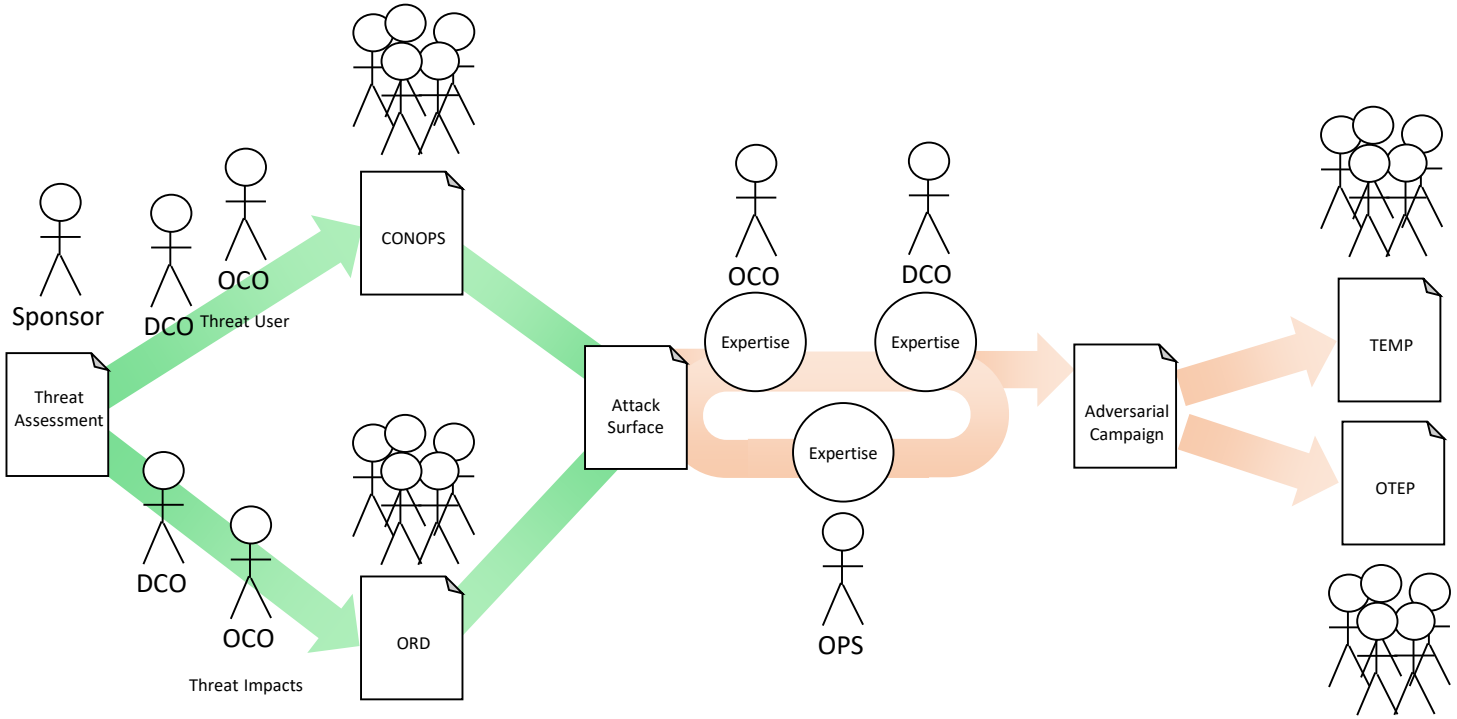
- From the solution view, procedures, behaviors, and later on, controls map to the Attack Surface nodes
- The Attack Surface helps in solution engineering by identifying additional operational conditions for the solution
  - Helps drive operational requirements for the solution
- Procedures, behaviors, system, and data architecture of the solution can be designed to limit exposure to the Threat Intent and Threat Capabilities
  - Long before identifying specific controls

Adversarial Operational Ontology



Integrate Threat Perspective

Integrate Threat Perspective



Threat Integration KSA

- **OCO** - Offensive Cyber Operations provides insight into known cyber operations techniques, tactics, and procedures.
  - CONOPS – Supports the CONOPS team to integrate potential threat behaviors into the description of the operational environment
  - ORD – Supports the ORD team to align identify threat approaches to key cyber terrain based on the CONOPS and notional technical and data architectures.
  - Attack Surface – Synthesizes the CONOPS and ORD perspectives into the description of the attack surface of the threat to the solution.
  - Adversarial Campaign – Supports the Operators in development of a time-sequenced TTP for the threat to be matched against Operator TTP and Defensive Cyber Operator TTP.
- **OPS** – Operators provide context on trade-offs for system performance (based on ORD requirements) for the interaction of OCO, DCO and operations.

Operational Evaluation Framework

Possible Evaluation Questions

Critical Operational Issue

Is this capability resilient to cyber attack?

Measures of Cybersecurity

How resilient is this mission to DOS attack of this capability?

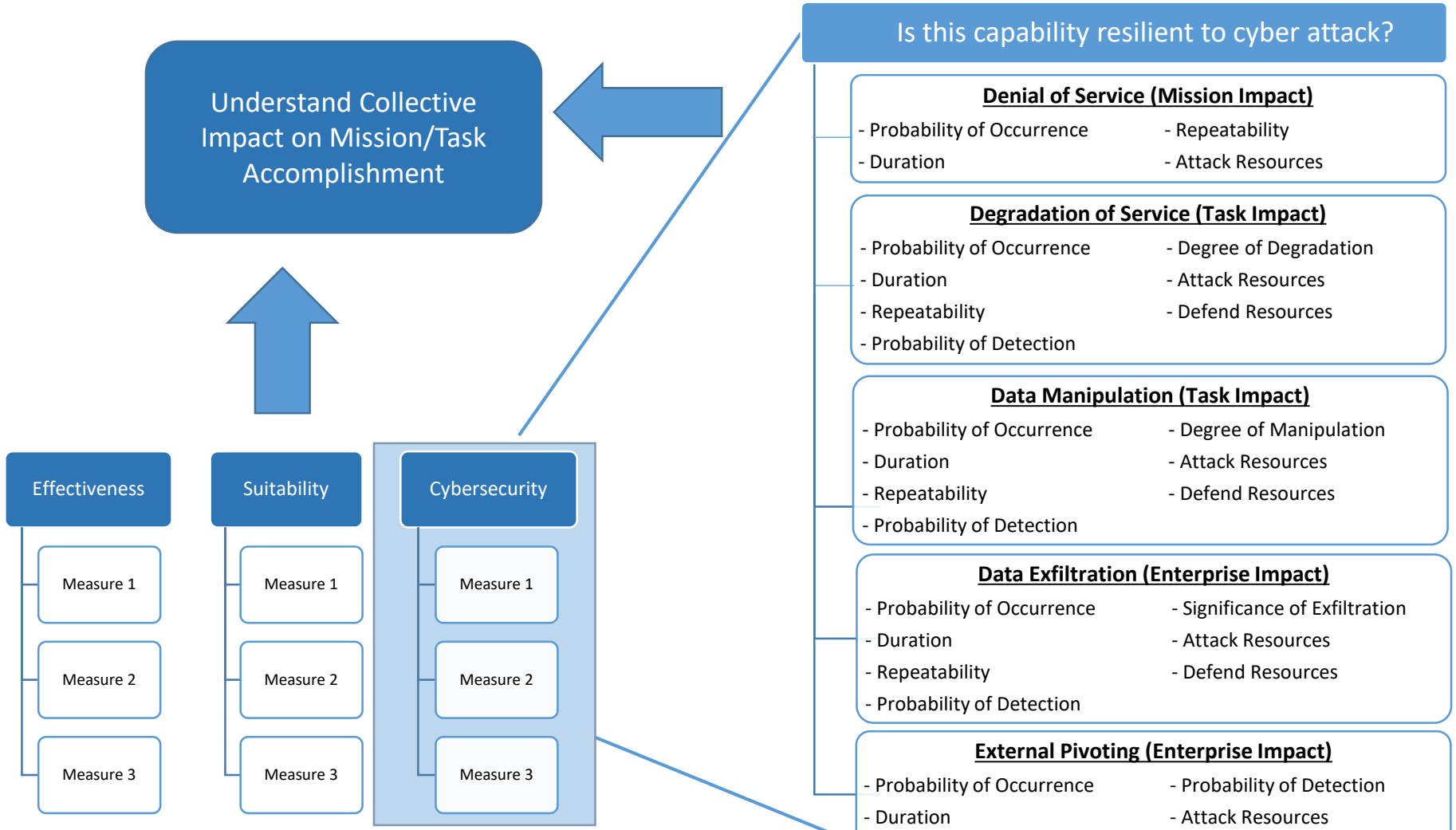
How resilient are the tasks to cyber degradation?

How resilient are the procedures to data manipulation?

How resilient is the mission to data exfiltration of the key cyber terrain?

How well does this system protect against attack from/to interfaced capabilities?

Sample Cybersecurity Evaluation Structure



Mapping MOC to Tasks

Cybersecurity
Is this capability resilient to cyber attack?

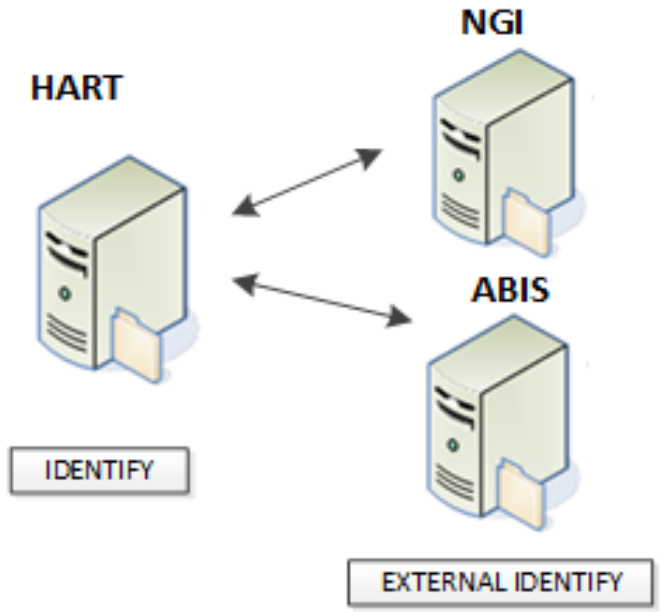
- **Denial of Service**
- **Degradation of Service**
- **Data Manipulation**
- **Data Exfiltration**
- **External Pivoting**

USCIS ASC Representative/ Asylum Officer collects biometrics

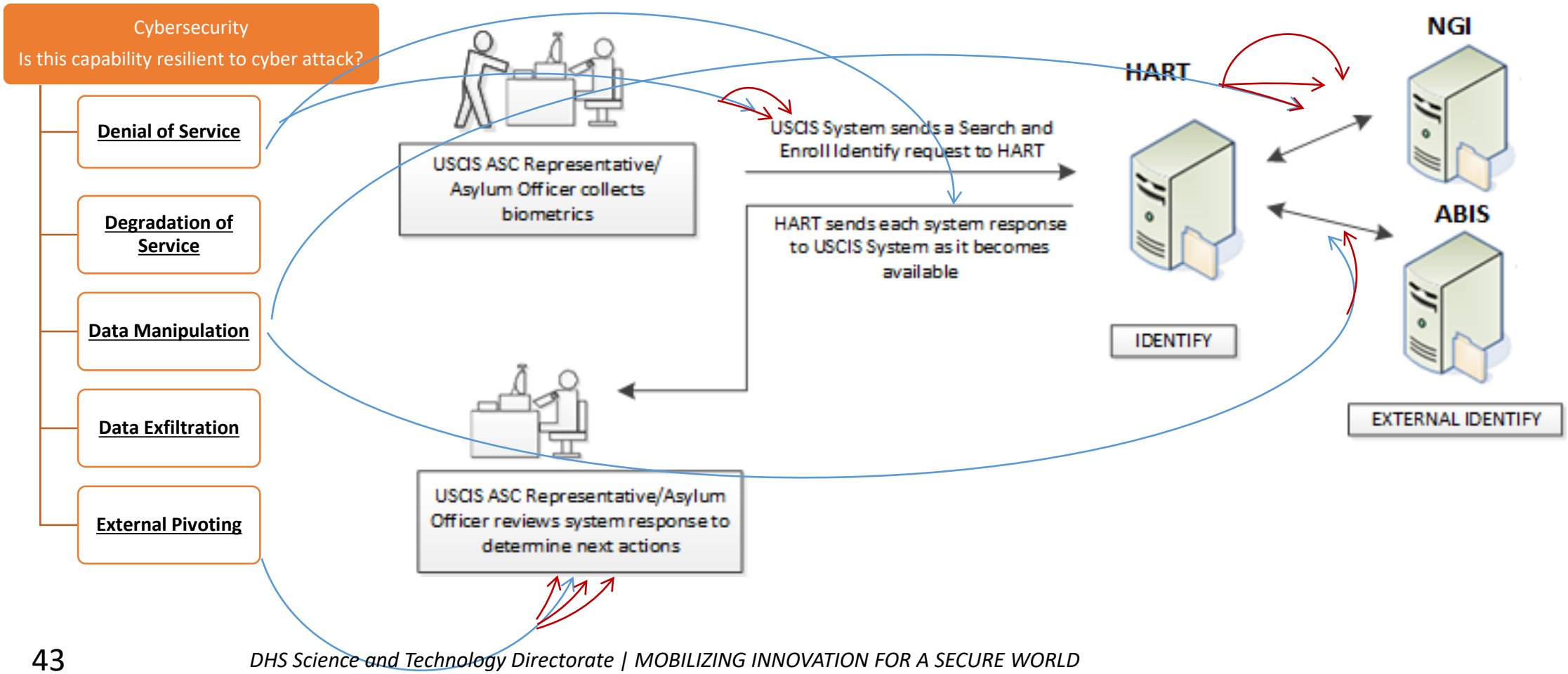
USCIS System sends a Search and Enroll Identify request to HART

HART sends each system response to USCIS System as it becomes available

USCIS ASC Representative/Asylum Officer reviews system response to determine next actions



Mapping MOC to Tasks



Design of Experiments

Mapping

		Operational Tasks					
		Mission Area 1			Mission Area 2		
		Task A	Task B1	Task B2	Task A	Task B	Task C
Threat Actor A	Denial		MD				
	Degradation				X		
	Manipulation	X					
	Exfiltration				X	ML	X
	Pivoting						
Threat Actor B	Denial						
	Degradation						
	Manipulation						
	Exfiltration	ML		X	X		
	Pivoting				X	X	X

Conditions

		Operational Tasks					
		Mission Area 1			Mission Area 2		
		Task A	Task B1	Task B2	Task A	Task B	Task C
Effectiveness	Performance						
	Interoperability						
Suitability	Availability						
	Throughput						
	Usability						
Security	Denial						
	Degradation						
	Manipulation						
	Exfiltration						
	Pivoting						

Conditions

		Operational Tasks									
		Mission Area 1						Mission Area 2			
		Task A		Task B1	Task B2			Task A	Task B		Task C	
		α	β		α	β	γ		δ	ε	β	γ
Effectiveness	Performance											
	Interoperability											
Suitability	Availability											
	Throughput											
	Usability											
Security	Denial											
	Degradation											
	Manipulation											
	Exfiltration											
	Pivoting											

Modes

		Operational Tasks										
		Mission Area 1						Mission Area 2				
		Task A		Task B1	Task B2			Task A	Task B		Task C	
		α	β		α	β	γ		δ	ε	β	γ
Effectiveness	Performance ?											
	Interoperability ?											
Suitability	Availability											
	Throughput											
	Usability											
Security	Denial											
	Degradation											
	Manipulation											
	Exfiltration											
	Pivoting											

Modes

			Operational Tasks										
			Mission Area 1						Mission Area 2				
			Task A		Task B1	Task B2			Task A	Task B		Task C	
			α	β		α	β	γ		δ	ε	β	γ
Effectiveness	Performance	2											
		1											
	Interoperability	C											
		B											
		A											
Suitability	Availability												
	Throughput												
	Usability												
Security	Denial												
	Degradation												
	Manipulation												
	Exfiltration												
	Pivoting												

Full Factorial Product

			Operational Tasks										
			Mission Area 1						Mission Area 2				
			Task A		Task B1	Task B2			Task A	Task B		Task C	
			α	β		α	β	γ		δ	ε	β	γ
Effectiveness	Performance	C2											
		B2											
		A2											
		C1											
		B1											
		A1											
	Interoperability	C2											
		C1											
		B2											
		B1											
		A2											
		A1											
Suitability	Availability												
	Throughput												
	Usability												
Security	Denial												
	Degradation												
	Manipulation												
	Exfiltration												
	Pivoting												

Collection

			Operational Tasks										
			Mission Area 1						Mission Area 2				
			Task A		Task B1	Task B2			Task A	Task B		Task C	
			α	β		α	β	γ		δ	ε	β	γ
Effectiveness	Performance	B2											
		A2											
		C1											
		B1											
	Interoperability	C1											
		B2											
		B1											
		A2											
Suitability	Availability												
	Throughput												
	Usability												
Security	Denial												
	Degradation												
	Manipulation												
	Exfiltration												
	Pivoting												

Assignment

			Operational Tasks										
			Mission Area 1						Mission Area 2				
			Task A		Task B1	Task B2			Task A	Task B		Task C	
			α	β		α	β	γ		δ	ε	β	γ
Effectiveness	Performance	B2											
		A2											
		C1											
		B1											
	Interoperability	C1											
		B2											
		B1											
		A2											
Suitability	Availability												
	Throughput	2											
		1											
	Usability	C1											
		B1											
		2											
Security	Denial												
	Degradation												
	Manipulation												
	Exfiltration												
	Pivoting												

Collapsing

			Operational Tasks											
			Mission Area 1							Mission Area 2				
			Task A		Task B1	Task B2				Task A	Task B		Task C	
			α	β		α	β	γ			δ	ε	β	γ
Effectiveness	Performance	B2												
		A2												
		C1												
		B1												
	Interoperability	C1												
		B2												
		B1												
		A2												
Suitability	Availability													
	Throughput	2												
		1												
	Usability	C1												
		B1												
		2												
Security	Denial													
	Degradation													
	Manipulation													
	Exfiltration													
	Pivoting													

Cybersecurity Operational T&E

Cybersecurity OT&E ≠ Penetration Testing

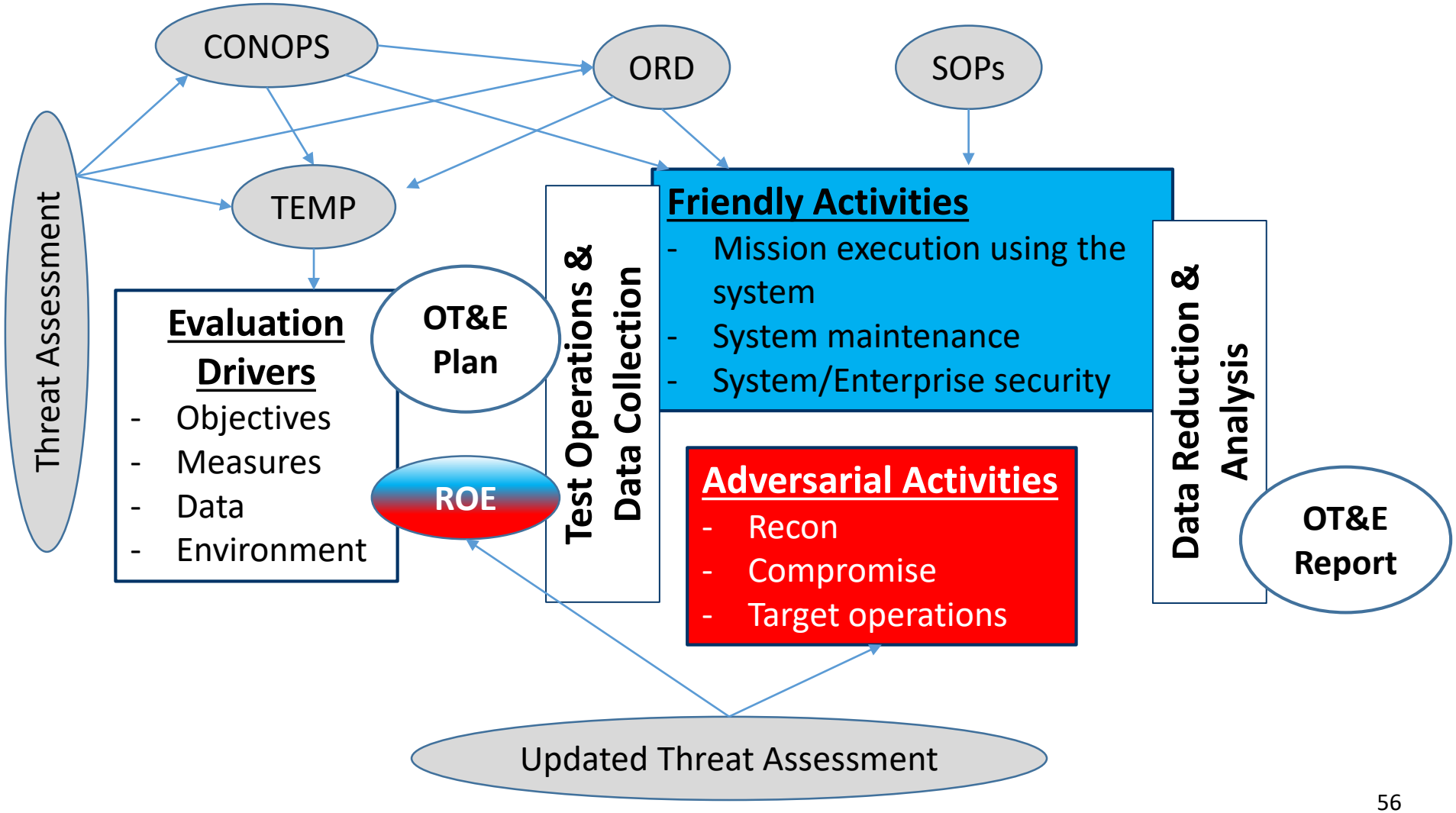
Cybersecurity OT&E

- Why: evaluate operational cybersecurity resilience
  - Understand mission effects
- When: TEMP-driven
- Who: OTA-led
- What: White cell manages friendly and adversary activities
  - Data collection on system use, defensive cyber operations, and adversary activities

Penetration Testing

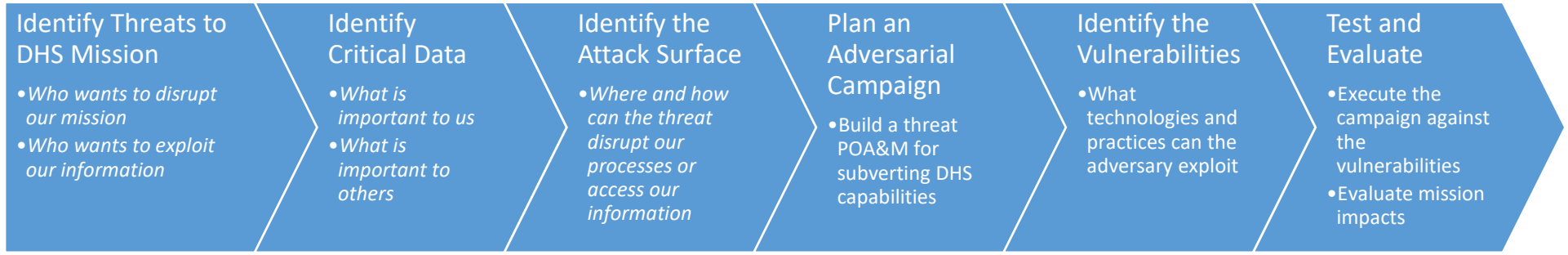
- Why: validate security controls & identify system security risks
  - Find vulnerabilities
- When: enterprise-driven
- Who: Penetration Test Team
- What: Pen Test Tm finds exploitable vulnerabilities
  - Data collection on Pen Test Tm activities

Elements of Cybersecurity OT&E



Vignettes and Kills Chains

How Adversarial Testing Works



Adversarial Campaign Planning (1/3)

- Characterize the Threat Actor CONOPS → then Tactics, Techniques, and Procedures
- Begin with goals and objectives → shape processes → lead to interactions along the Attack Surface
- Contains measures of effectiveness for the adversarial team , who will represent the Threat Actors, and alternative courses of action
- Free of constraints with respect to the safety and security of the targeted capability

Adversarial Campaign Planning (2/3)

- Prior to executing the Adversarial Campaign all affected parties will agree to a Rules of Engagement
  - Constrain the activities of the adversarial team with respect to the safety and security of the targeted capability
  - Establish relevant time and resource constraints
- Constraints need to be addressed by mitigations
  - Acceptance of risk, or
  - Surrogating the Tactics, Techniques, and Procedures with analysis or simulation

Adversarial Campaign Planning (3/3)

- Time and resource constraints are commonly addressed through assumption of risk
- An example is the designation of a “starting position” (physical, logical, access, state) for the adversarial team
  - Avoids expending the resources to achieve that state (often a long time of surveillance, exfiltration, and positioning)
- Commonly, the adversarial team will achieve this “starting position” once and then be allowed to restart at this position without expending the resources again later in the campaign

Rules of Engagement

Rules of Engagement

Purpose – Support evaluation of ...

Threat Assessment

Actors	(FIS, Terrorist, Criminal, Activist, Mercenary, Hackers)
Intent	
Capabilities	(Historical, Projected, Surrogates)

Strategic Goals

Definition of Capability Under Test
System Boundary
Included Systems
Excluded Systems
Mission Impacts (DOS, DEG, DMAN, EXFIL, PIVOT)

Operational Objectives

Targeted Data (leads to ...)	Deliberate
Targeted Systems (leads to ...)	Deliberate
Targeted Networks (leads to ...)	Deliberate 80 / Exploratory 20
Targeted Interfaces (leads to ...)	Deliberate 50 / Exploratory 50
Relevant Vulnerabilities	Deliberate 20 / Exploratory 80

Rules of Engagement (cont'd)

Tactical Plan

Schedule

Operational Objective, Capability (Surrogate) Start, End

Initial Access

TTP by Scheduled Event (planned and contingency)

OCO Actions
Limits of Action
Prohibited Actions
Termination Conditions/Notification
DCO Posture

Active Events – Events the DCO will carry out

Stop Events – Events where the DCO will report detection to the red team and the event will stop

Passthrough Actions – Events where the DCO will report detection and the event will proceed

Data Handling

Ranges, Simulations, and Tools

Cyber Ranges

- Persistent, continuously maintained environment reduces timeline and costs between planning and event execution
- Operationally realistic environment with repeatable processes
- Access to enterprise tools and services not typically available in smaller scale test labs
- Threat scenario development and threat automation capabilities
- TTP development and capabilities validation prior to fielding
- Coordinate with other Lab/Range Environments to support large scale interoperable test/training/exercise
- Ability to support multiple environments / configurations (STIG'd, non-STIG'd, HBSS, non-HBSS, etc.)

DOD Ranges

- National Cyber Range (NCR)
- Joint Information Operations Range (JIOR)
- DoD Cybersecurity Range
- JMETC

Cyber Table Top Exercises – DASD(DT&E)

Examples of CTT Benefits

Socialize the concept of cybersecurity for program office and operators, bridging the gaps between the cybersecurity, systems engineering, testing and operational mission viewpoints

Look beyond a single test system to the cyber vulnerabilities of System of Systems and Family of Systems within the disciplined context of a specific test

Define the first steps to collect empirical data in order to answer key questions aimed at the most critical unknowns

Enable knowledge and action that lead to more secure and resilient Developmental Test (DT) and Operational Test (OT) events

28

More CTT Benefits

Provide opportunities for risk reduction throughout the life cycle to the Program Manager's engineering and test team

Reduce the likelihood and cost of cyber vulnerability discovery during operational testing and deployment

Pragmatic affordable method to implement elements of the DT/OT six cybersecurity phases

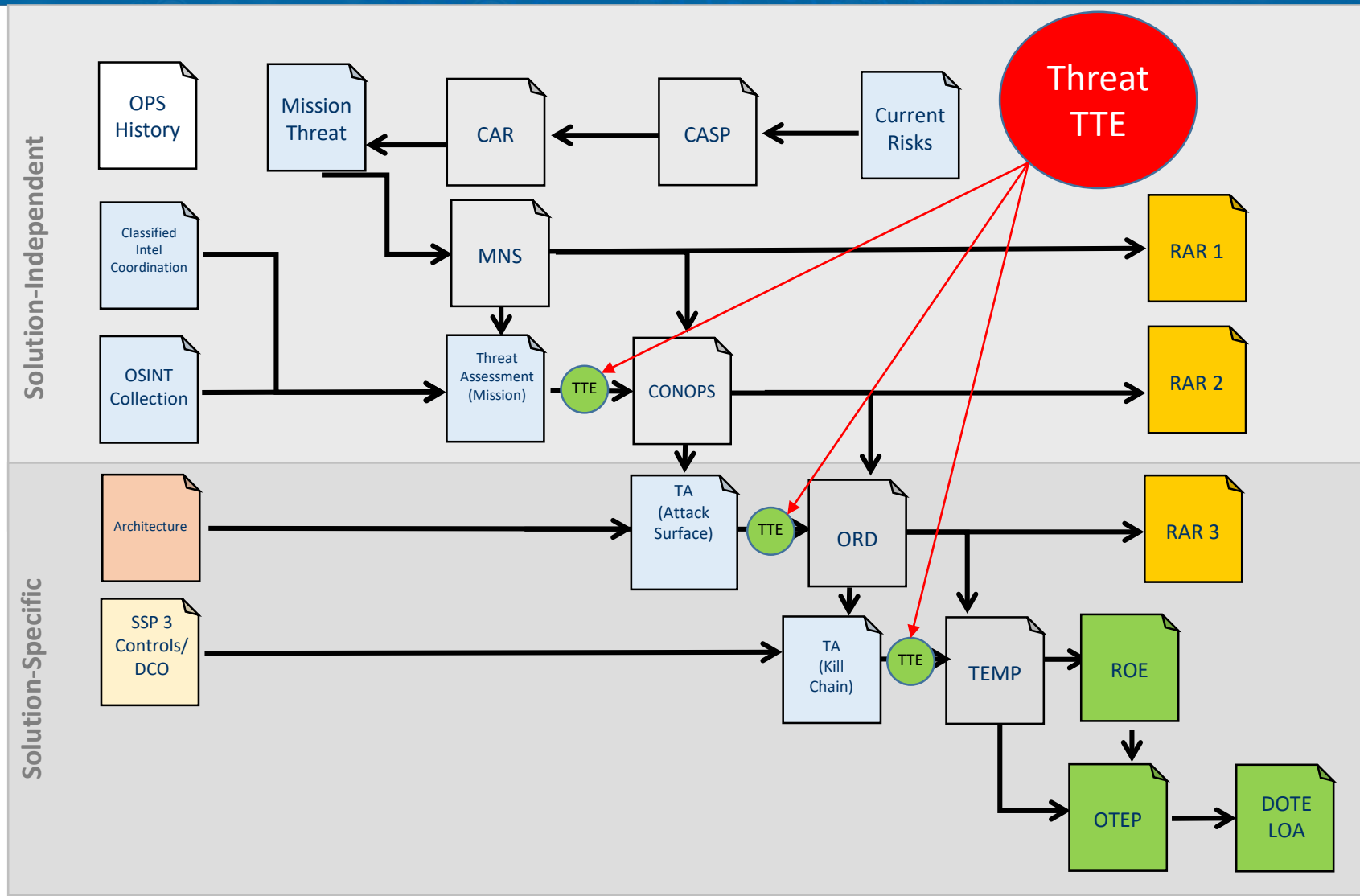
Inform analysis for the system survivability Key Performance Parameter (KPP)

CTTs address aspects that the Risk Management Framework (RMF), or Defense Information Assurance Certification and Accreditation Process (DIACAP) do not account for

29

Slides pulled from "Cyber Table Top Overview" briefing dated Jan 2018; Sarah Standard, DASD(DT&E)

Threat Table Top Exercises



Acronyms

RAR – Risk Assessment Report

SSP-System Security Plan

CASP – Capability Analysis Study Plan

CAR – Capability Assessment Report

OSINT – Open Source Intelligence

DCO – Defensive Cyber Operations

OTEP – Operational Test and Evaluation Plan

DOTE LOA – Operational Test Letter of Assessment

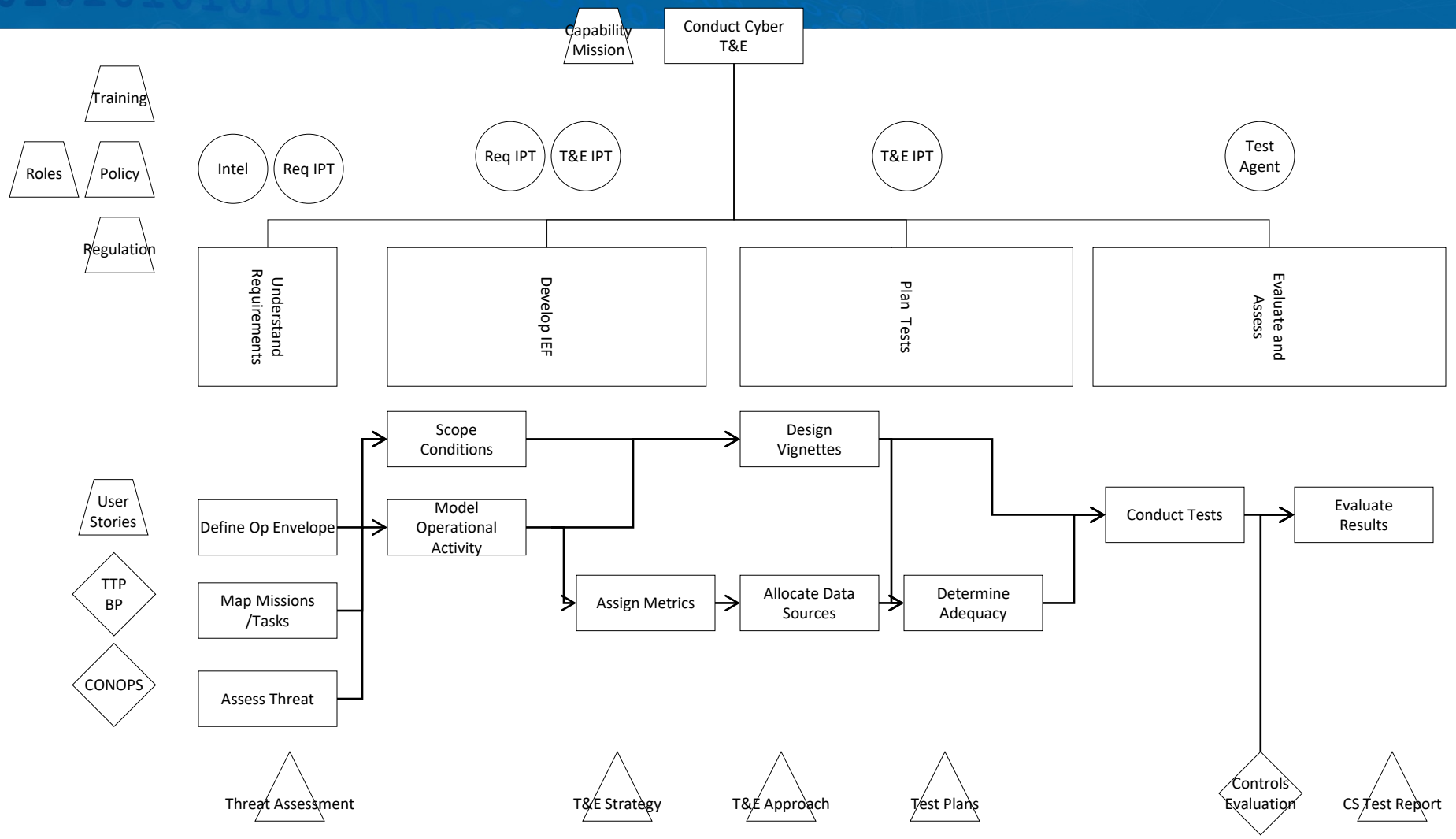
Threat Assessment

Mission – What?

Attack Surface – Where?

Kill Chain – When & How?

Cyber T&E Activity Model



Cybersecurity Test and Evaluation Imperatives

- Threat assessments provide context
- Performance modelling sets the foundation
- Operational requirements drive SE

- Operational requirements drive T&E
- RMF and T&E are mutually supportive
- Use of “ranges” can mitigate many recurring limitations
- Cybersecurity OT&E is more than penetration testing

Questions?

Homeland Security

Science and Technology

Contact Info

Alex Hoover
DHS Office of Systems Engineering
Alex.Hoover@hq.dhs.gov
202 254-5615

James Wells
DHS Office of Test & Evaluation
James.wells@hq.dhs.gov
202-254-6103

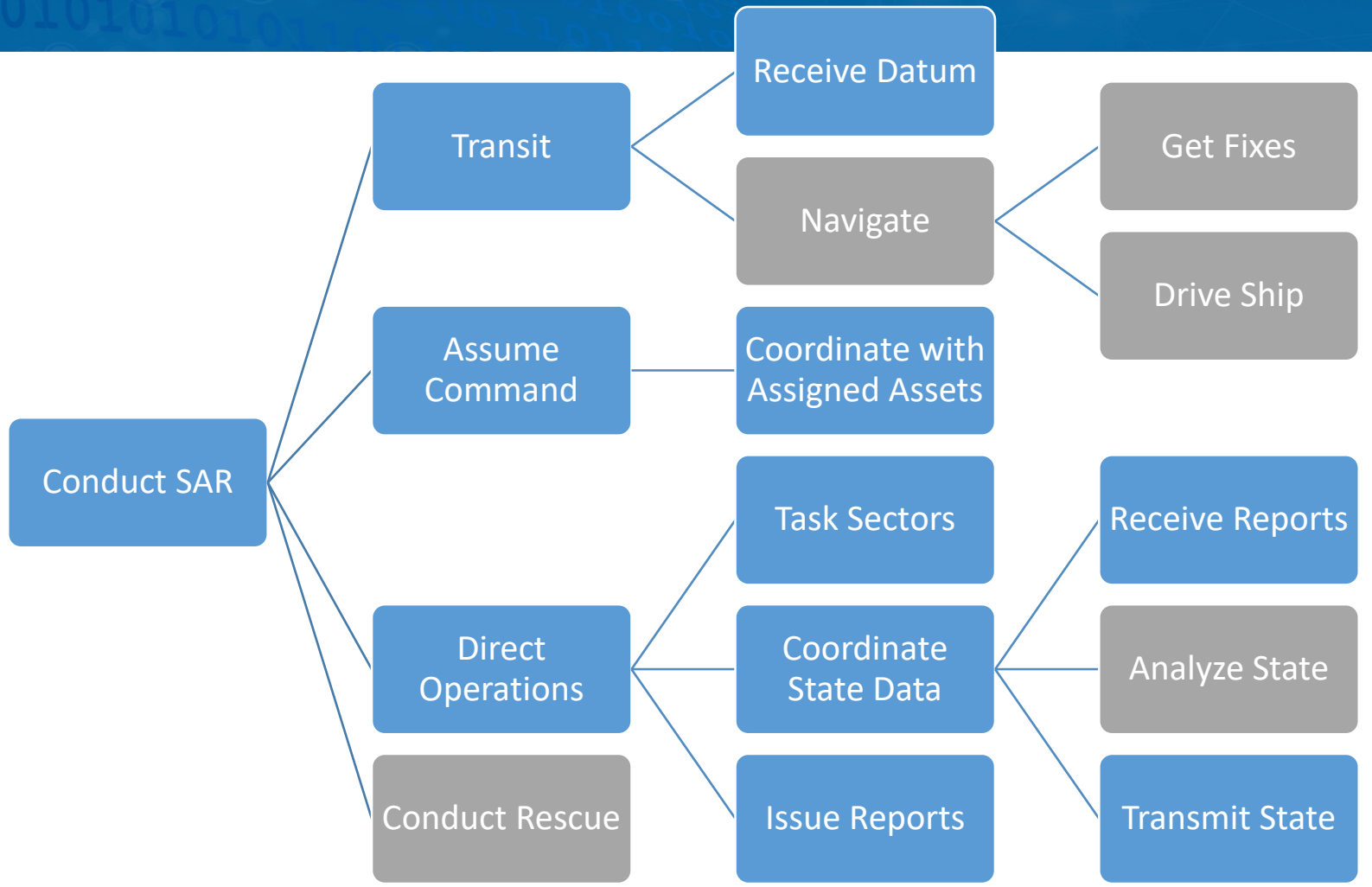
Backup – Process Mapping

National Security Cutter (WMSL) SAR Task

2.2.2.7 Search and Rescue: While conducting training off the Northern California coast, a WMSL is diverted by the D11 Rescue Coordination Center to investigate an Emergency Position-Indicating Radio Beacon (EPIRB), registered to a sailboat sailing from Honolulu to San Francisco. Additional SAR assets are mobilized to support the effort, including USCG HC-130s and USN P-3s. The first fixed wing asset on scene reports debris in the water, but no presence of survivors.

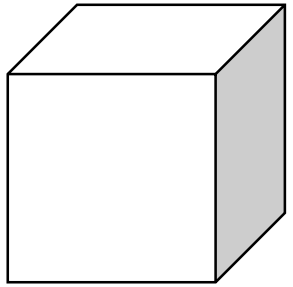
When the WMSL reaches the search area it assumes duties as OSC and begins to coordinate the search effort. The WMSL arrives at the beacon position and confirms debris in the water, but no presence of survivors. The search area is expanded and additional Coast Guard, U.S. Navy, and Automated Mutual-assistance Vessel Rescue system assets are diverted. Eventually, a USN P-3C locates a life raft with 3 passengers 16 miles south of the initial beacon report and the WMSL vectors its helicopter to the area. The helicopter uses the hoist and basket to recover all 3 passengers. The helicopter lands on the WMSL and the passengers are carried to the ship's sick bay, where they are examined by the ship's corpsman who determines that one of the passengers needs to be evacuated as soon as possible. WMSL proceeds at maximum speed to shore, and when within range, the ship's helicopter transports the patient to a nearby hospital. The WMSL then proceeds to enter port and delivers the other passengers to another hospital for care.

Tasks – Partitioning

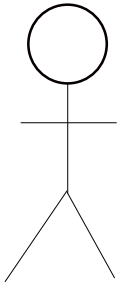


Backup – Security

Asset



Actor

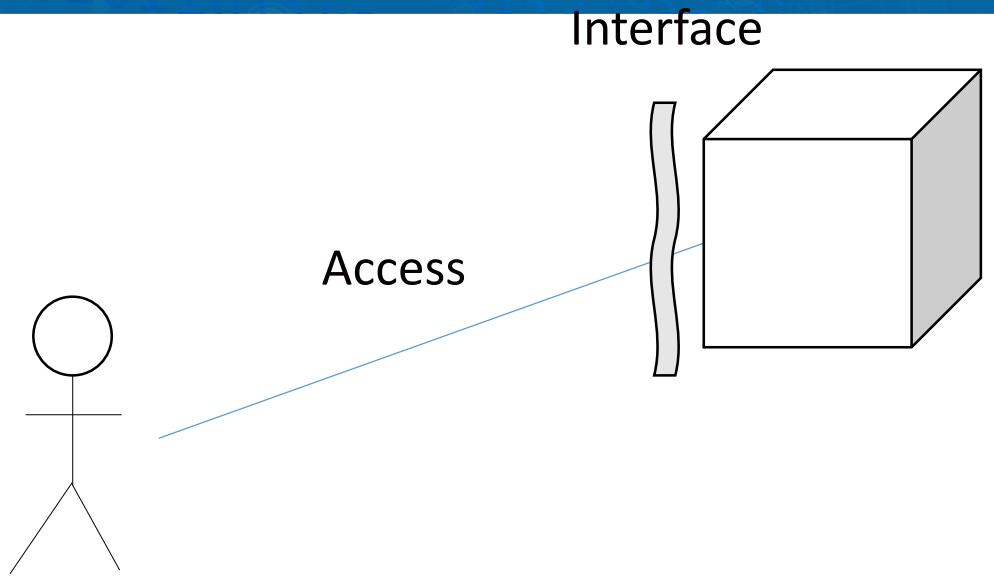


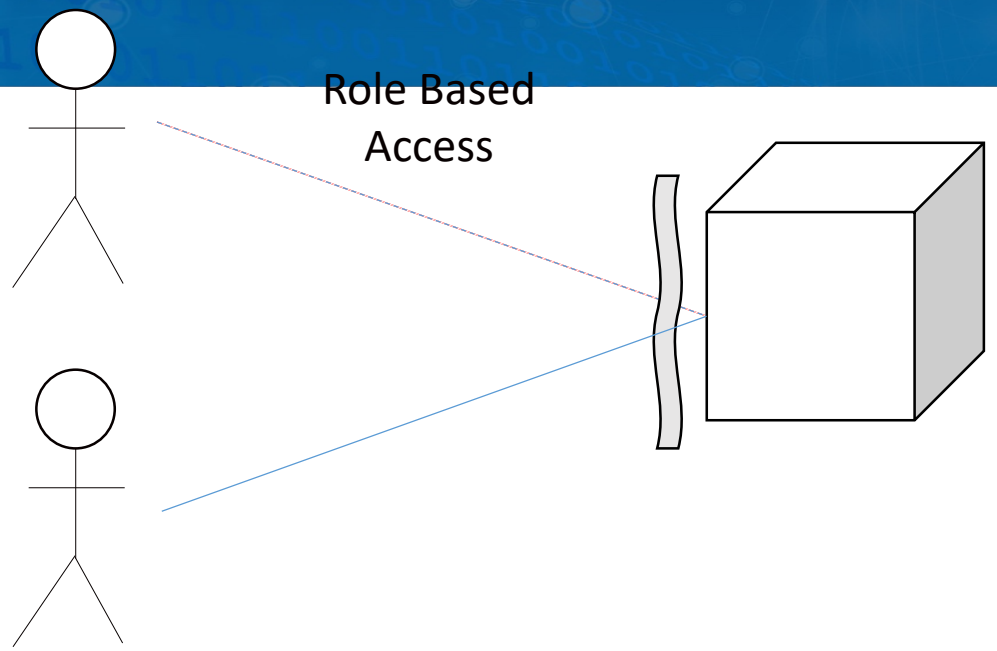
Ranges, Simulations, and Tools

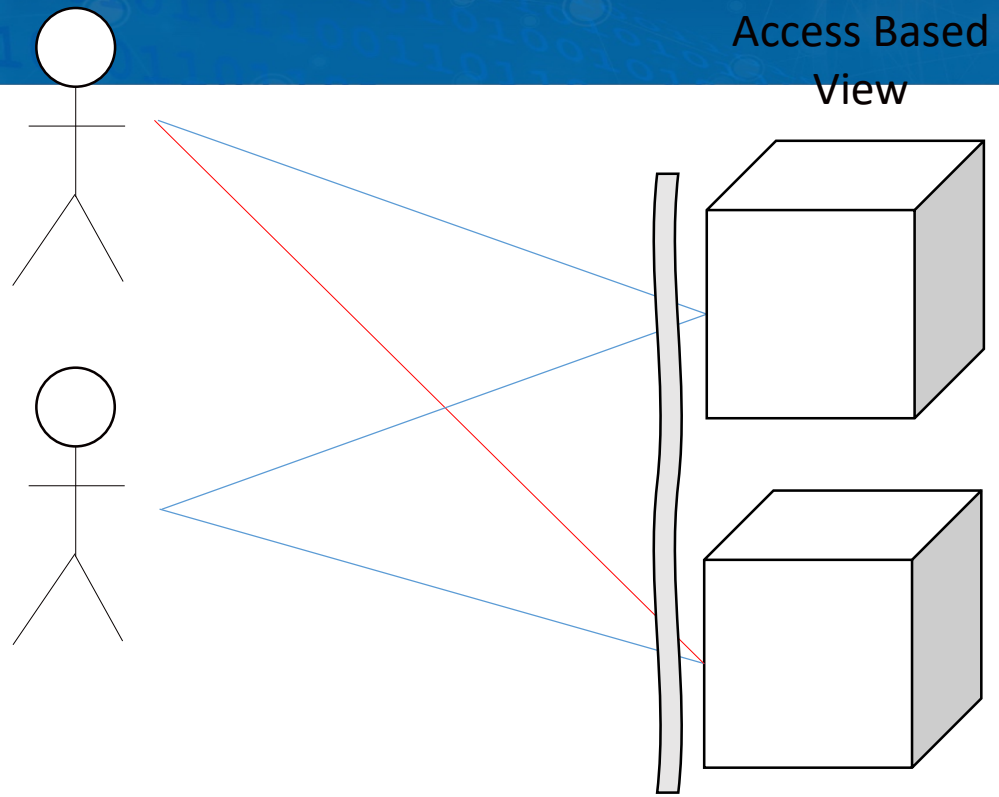
DOD Ranges

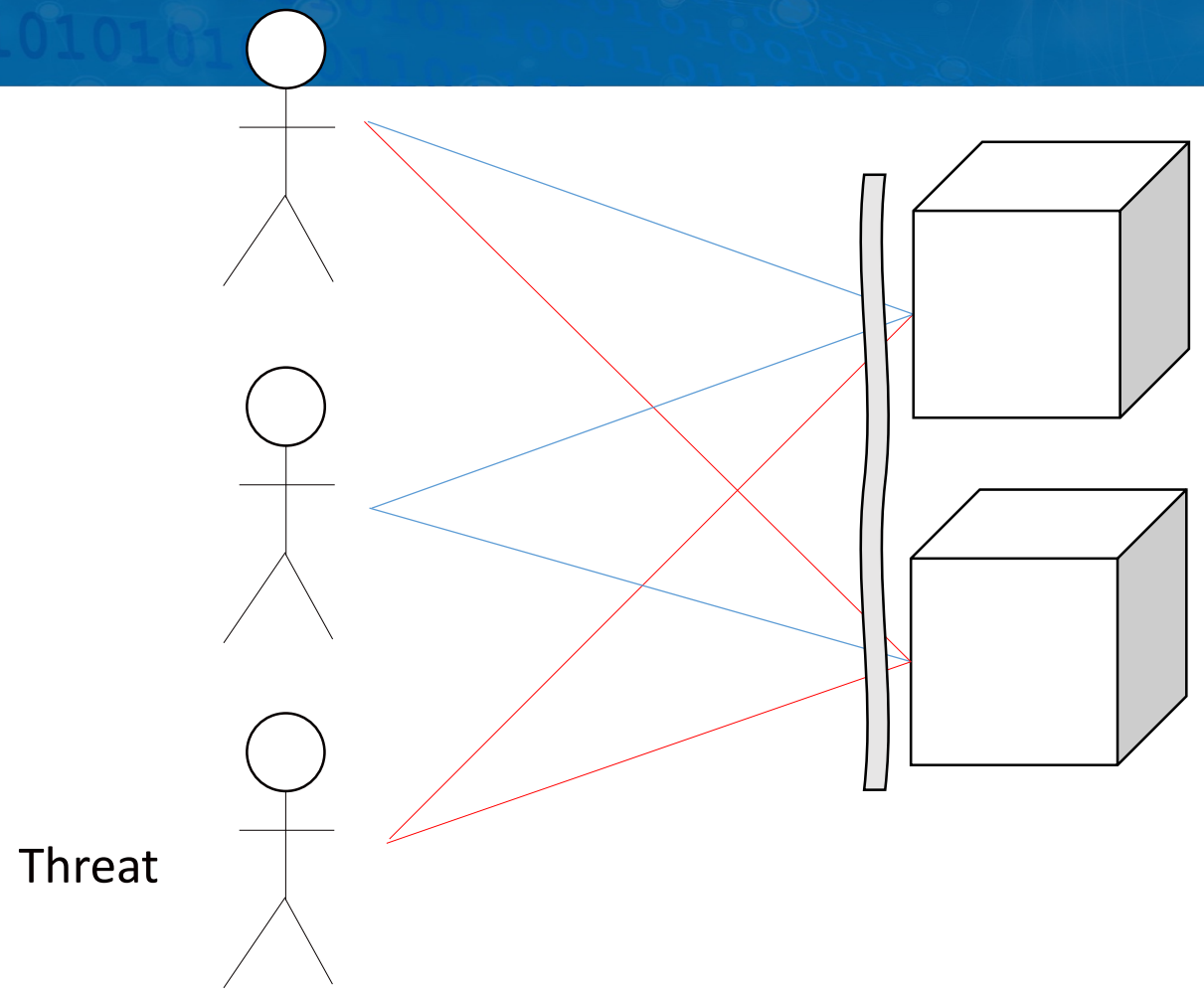
- National Cyber Range (NCR)
- Joint Information Operations Range (JIOR)
- DoD Cybersecurity Range
- JMETC

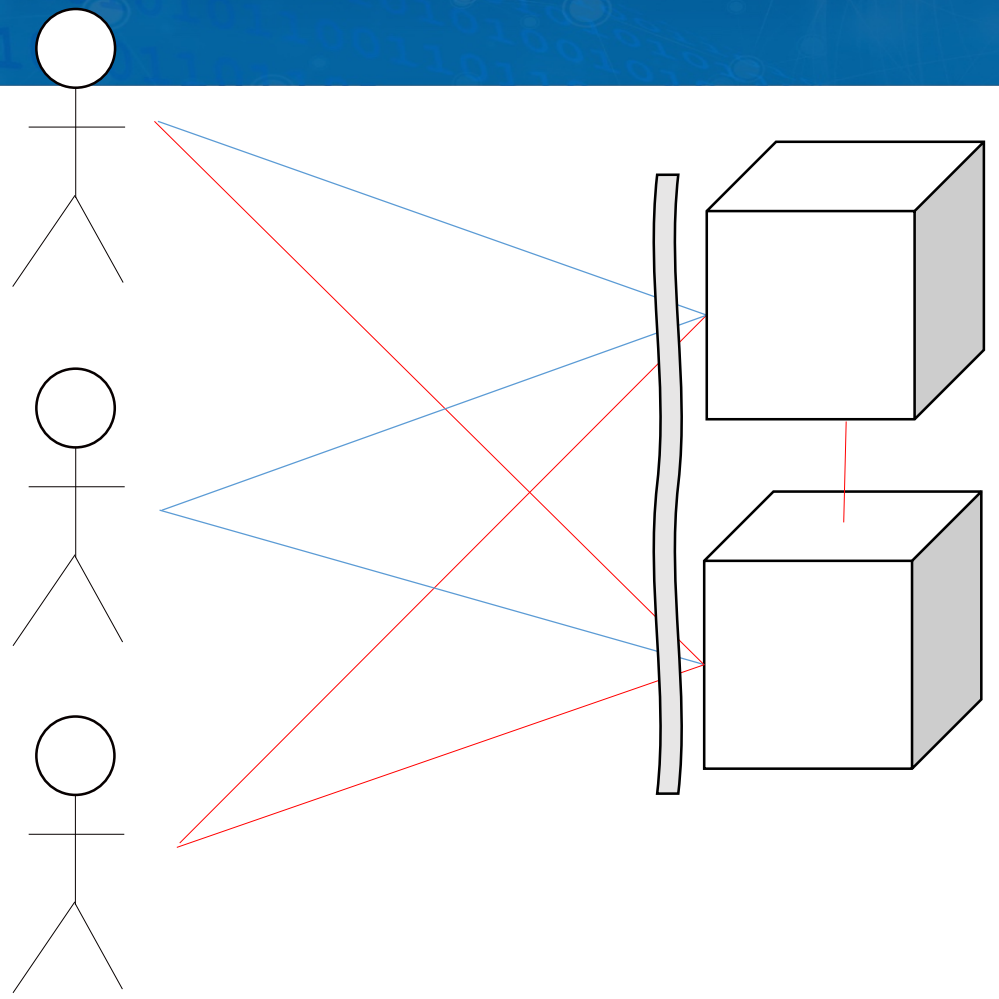
Table Top Exercises


Interface
Access

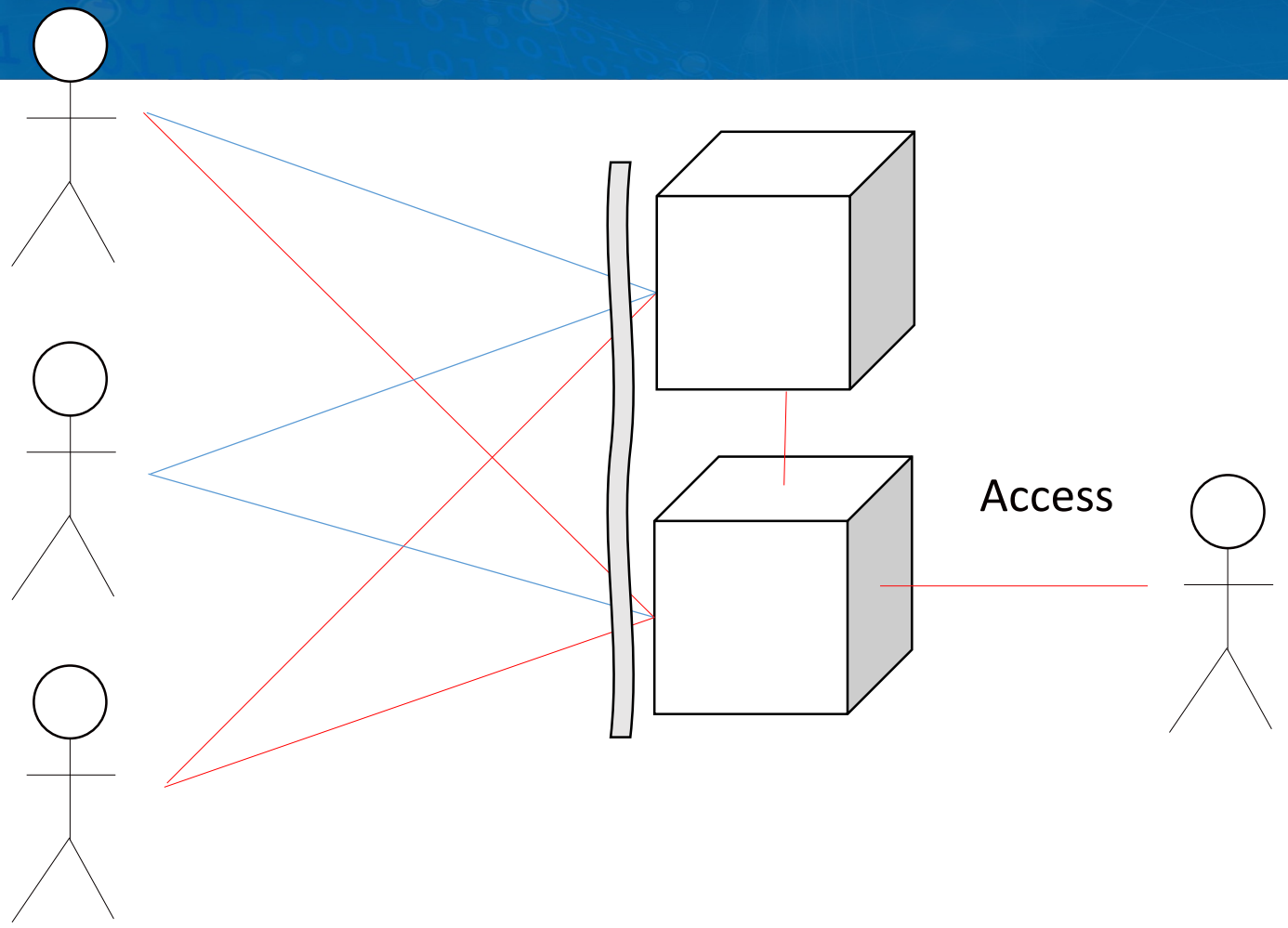

Role Based
Access

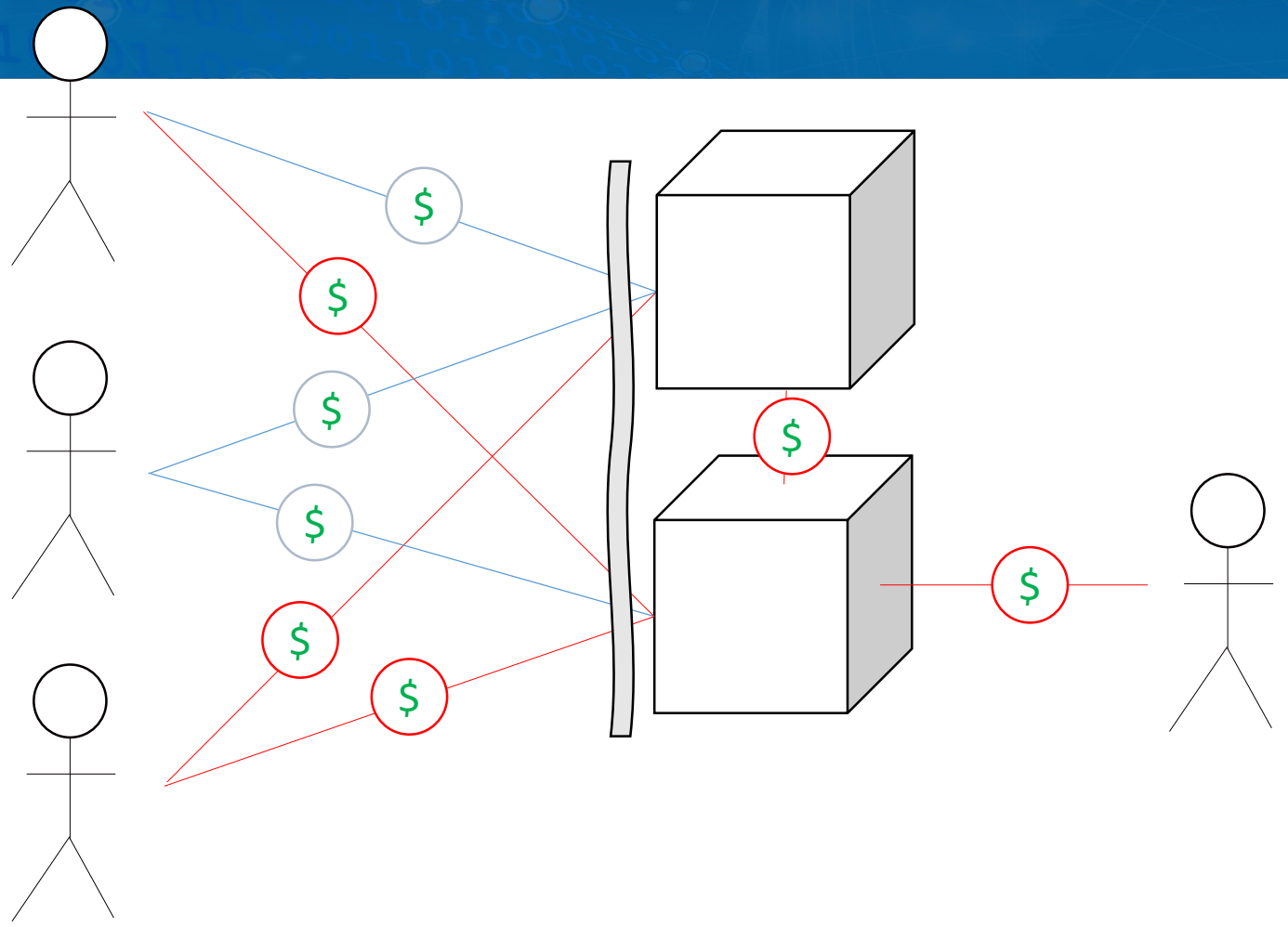

Access Based
View

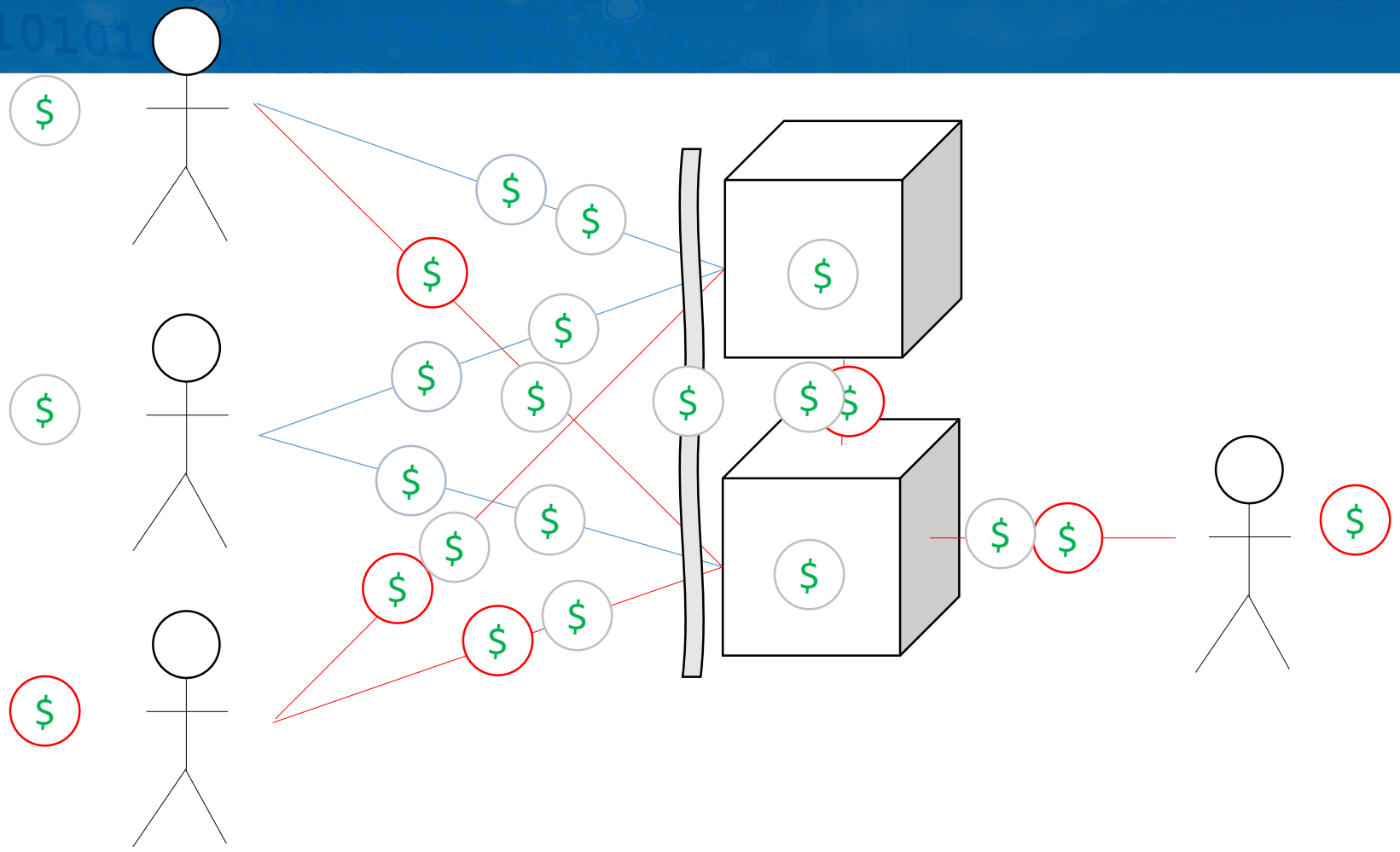

Threat



Pivot


Access





Backup – Process Mapping

The Holon

- Holon
  - Both a whole and a part
- Individual Holon
  - Composition
  - Agency
  - “i-ness” (dominant monad)
- Social Holon
  - No dominant monad
  - Collective agency
  - Temporality

Cyberspace

- IT systems are artifacts
  - Produced by holons
  - No agency

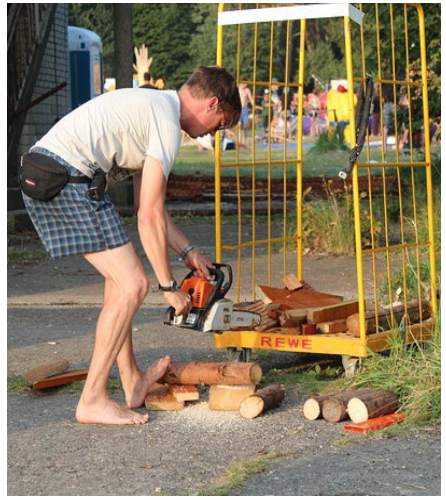
- Cyberspace is a social holon
  - Its agency is collective
  - Many monads contribute in different ways

Who Cares?

We Care

- Key Information Terrain
- Critical, not just supplemental, processes
- More and more distribution
- Rapidly evolving tech environment
- Rapidly emerging missions

Tools or Agency?



extracted from www.pixabay.com 21 APR 17

What can HFE do for us?

- Establish knowledge norms
- Provide true situational awareness
- Operationalize the IT crowd
- Challenge NRT-24/7
- Actually evaluate COTS

The Last Word

Don’t make this thing so specialized, so unique, so different that it just gets pushed to the side. That will sub-optimize our ability to execute cyber operations, and quite frankly it will minimize or at least negatively impact, in my view, the operational outcomes, which is the whole reason we’re doing this in the first place. We have got to focus on generating operational outcomes. If it doesn't generate operational outcomes, whether it be offensive or defensive application of cyber, it is a waste of time and a waste of investment.

Adm. Mike Rogers, Commander, U.S. Cyber Command

extracted from www.defense.gov 21 APR 17

Backup – Meaninglessness

日本語を話しますか

We're going to teach you to "speak computer" by using Japanese. By the way, that question on the last slide asked who here speaks Japanese.

If you do speak Japanese, what we go over will seem strange, until you get to the end point. The lesson will make the same point, just in a different way.

Instead of teaching in terms of words and grammar, we need to teach you in terms of "axioms" (stuff) and "rules of inference" (things to do with stuff).

Don't worry about taking notes, just follow along. There is a test, but we keep all the material on the screen for you during the test.

Axioms

1 aka

2 kiiro

3 honoiro

4 ao

5 murasaki

So, Here's your first stuff. Numbers. Numbers are a basic thing that computers "understand" and use.

This is a pretty small set, but it is big enough to do what we want. That is a key thing we don't realize about computers – because they work so fast, we think they have infinite capacity. In reality, each computer is designed to only have as much capacity as the user needs. Changes in the environment that change that need, we get "upgrades".

Axioms

1	aka	+	to
2	kiiro	-	nashi
3	honoiro	=	desu
4	ao		
5	murasaki		

Just a little more stuff, some mathematical operators.

As humans, we think of “numbers” and “operators” as different kinds of things. Computers don’t. Each thing it deals with is just a string of bits, so it doesn’t differentiate among different “types” of things.

If you saw, “+ 2 3 =“, you would probably think, “Oh, typo. They want 2+3, which is five. A computer would treat the “+” (or really, its bit string) like a number and the “2” as an operator. Who knows what that would lead to?

Axioms

1	aka	+	to
2	kiiro	-	nashi
3	honoiro	=	desu
4	ao		
5	murasaki		

Rules of Inference

aka to kiiro desu honoiro

murasaki nashi ao desu aka

Here are two of the things you can do with the stuff we gave you. Like the axioms, as a human being you see the rules of inference as incomplete. You know things and can apply outside information into the context. But the computer only knows and does exactly what it is told to do.

Since we often have multiple people (programmers, administrators, users) who never see each other telling one computer what to do, we superimpose behavior on computer processing. After all, I didn't tell it to do that. But someone did …

Axioms

1	aka	+	to
2	kiiro	-	nashi
3	honoiro	=	desu
4	ao		
5	murasaki		

Rules of Inference

aka to kiiro desu honoiro

murasaki nashi ao desu aka

OK, here's your test. Just click a box for each statement, then hit submit. (A computer would need a lot more instructions to do this.)

Application	aka	kiiro	honoiro	ao	murasaki	don't know
aka to kiiro desu	☐	☐	☐	☐	☐	☐
kiiro to aka desu	☐	☐	☐	☐	☐	☐
murasaki nashi ao desu	☐	☐	☐	☐	☐	☐
murasaki nashi ao desu to kiiro desu	☐	☐	☐	☐	☐	☐

Axioms

1	aka	+	to
2	kiiro	-	nashi
3	honoiro	=	desu
4	ao		
5	murasaki		

Rules of Inference

aka to kiiro desu honoiro

murasaki nashi ao desu aka

The first one is pretty easy. It's just repeat the first rule of inference.

Application	aka	kiiro	honoiro	ao	murasaki	don't know
aka to kiiro desu	☐	☐	☐	☐	☐	☐
kiiro to aka desu	☐	☐	☐	☐	☐	☐
murasaki nashi ao desu	☐	☐	☐	☐	☐	☐
murasaki nashi ao desu to kiiro desu	☐	☐	☐	☐	☐	☐

Axioms

1	aka	+	to
2	kiiro	-	nashi
3	honoiro	=	desu
4	ao		
5	murasaki		

Rules of Inference

aka to kiiro desu honoiro

murasaki nashi ao desu aka

Even though you know that 1+2 = 2+1, a computer doesn't unless you tell it so.

Application	aka	kiiro	honoiro	ao	murasaki	don't know
aka to kiiro desu	☐	☐	☐	☐	☐	☐
kiiro to aka desu	☐	☐	☐	☐	☐	☐
murasaki nashi ao desu	☐	☐	☐	☐	☐	☐
murasaki nashi ao desu to kiiro desu	☐	☐	☐	☐	☐	☐

Axioms

1	aka	+	to
2	kiiro	-	nashi
3	honoiro	=	desu
4	ao		
5	murasaki		

Rules of Inference

aka to kiiro desu honoiro

murasaki nashi ao desu aka

And this one is just repeating the second rule.

Application	aka	kiiro	honoiro	ao	murasaki	don't know
aka to kiiro desu	☐	☐	☐	☐	☐	☐
kiiro to aka desu	☐	☐	☐	☐	☐	☐
murasaki nashi ao desu	☐	☐	☐	☐	☐	☐
murasaki nashi ao desu to kiiro desu	☐	☐	☐	☐	☐	☐

Axioms

1	aka	+	to
2	kiiro	-	nashi
3	honoiro	=	desu
4	ao		
5	murasaki		

Rules of Inference

aka to kiiro desu honoiro

murasaki nashi ao desu aka

This one was a bit tricky. But since the computer has a way to process each group of stuff, it can produce this answer by working in series.

Application	aka	kiiro	honoiro	ao	murasaki	don't know
aka to kiiro desu	☐	☐	☐	☐	☐	☐
kiiro to aka desu	☐	☐	☐	☐	☐	☐
murasaki nashi ao desu	☐	☐	☐	☐	☐	☐
murasaki nashi ao desu to kiiro desu	☐	☐	☐	☐	☐	☐

Axioms

1	aka	+	to
2	kiiro	-	nashi
3	honoiro	=	desu
4	ao		
5	murasaki		

Rules of Inference

aka to kiiro desu honoiro

murasaki nashi ao desu aka

But the interesting thing about this example is that everything in it is a lie…

Application	aka	kiiro	honoiro	ao	murasaki	don't know
aka to kiiro desu	☐	☐	☐	☐	☐	☐
kiiro to aka desu	☐	☐	☐	☐	☐	☐
murasaki nashi ao desu	☐	☐	☐	☐	☐	☐
murasaki nashi ao desu to kiiro desu	☐	☐	☐	☐	☐	☐

Axioms

1	aka	+	to
2	kiiro	-	nashi
3	honoiro	=	desu
4	ao		
5	murasaki		

Rules of Inference

aka to kiiro desu honoiro

murasaki nashi ao desu kiiro

Your “numbers” weren’t numbers, they were colors. But still you got the right answers. Just like a computer, you didn’t really know what you were doing, you just plugged ahead according to instruction.

Application	aka	kiiro	honoiro	ao	murasaki	don’t know
aka to kiiro desu	☐	☐	☐	☐	☐	☐
kiiro to aka desu	☐	☐	☐	☐	☐	☐
murasaki nashi ao desu	☐	☐	☐	☐	☐	☐
murasaki nashi ao desu to kiiro desu	☐	☐	☐	☐	☐	☐

Axioms

1	aka	+	to
2	kiiro	-	nashi
3	honoiro	=	desu
4	ao		
5	murasaki		

Rules of Inference

aka to kiiro desu honoiro

murasaki nashi ao desu kiiro

Within the bounds of what you did, the answers were right, independent of what concepts we superimposed over the symbols you were manipulating.

Application	aka	kiiro	honoiro	ao	murasaki	don't know
aka to kiiro desu	☐	☐	☐	☐	☐	☐
kiiro to aka desu	☐	☐	☐	☐	☐	☐
murasaki nashi ao desu	☐	☐	☐	☐	☐	☐
murasaki nashi ao desu to kiiro desu	☐	☐	☐	☐	☐	☐

Axioms

1	aka	+	to
2	kiiro	-	nashi
3	honoiro	=	desu
4	ao		
5	murasaki		

Rules of Inference

aka to kiiro desu honoiro

murasaki nashi ao desu kiiro

Thinking about other possibilities in this example like “kiiro to kiiro” illustrates another thing that can go very wrong when we assume a computer “understands” things instead of just processes data.

Application	aka	kiiro	honoiro	ao	murasaki	don’t know
aka to kiiro desu	☐	☐	☐	☐	☐	☐
kiiro to aka desu	☐	☐	☐	☐	☐	☐
murasaki nashi ao desu	☐	☐	☐	☐	☐	☐
murasaki nashi ao desu to kiiro desu	☐	☐	☐	☐	☐	☐

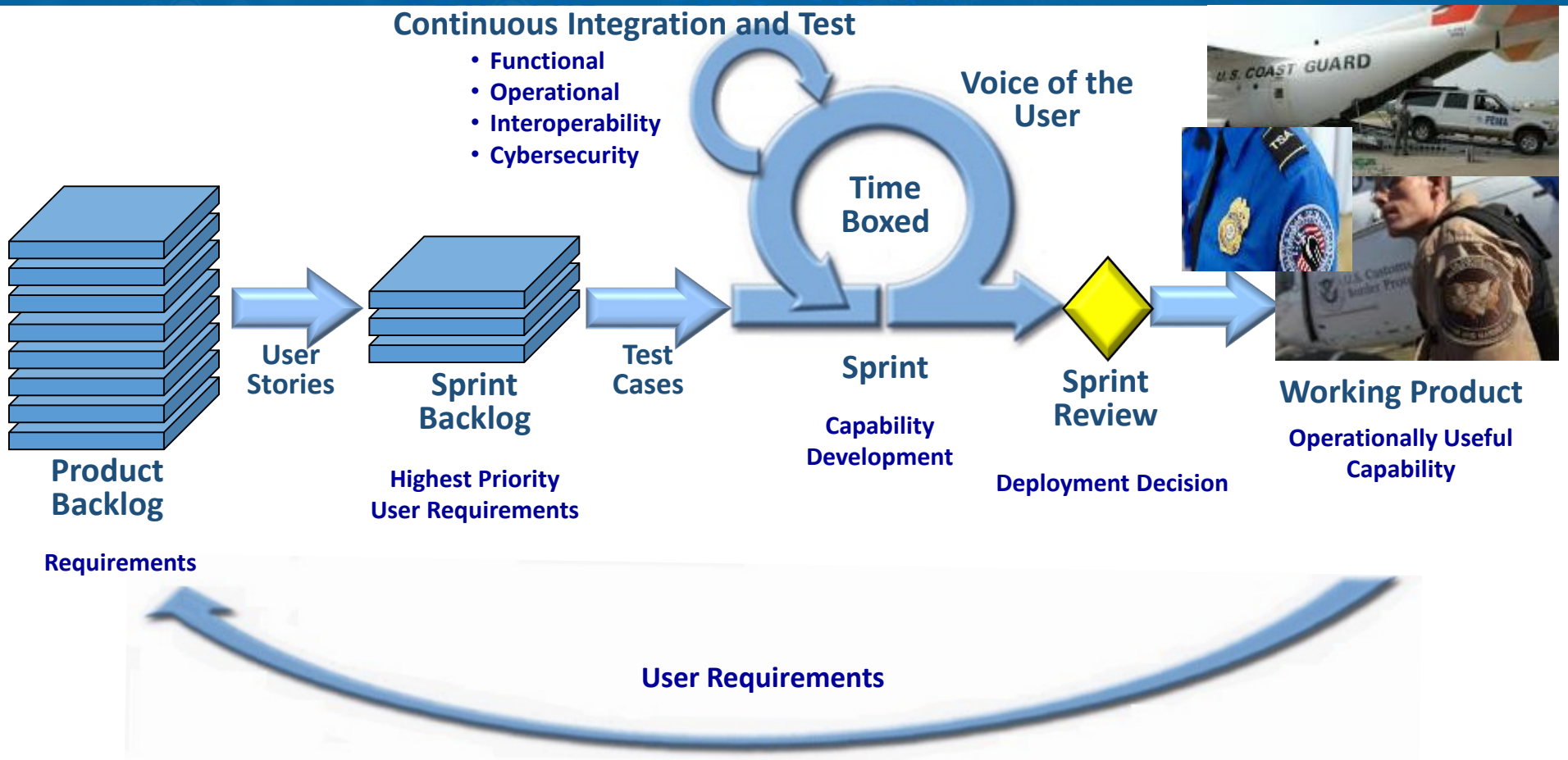
Backup – Agile

Agile Philosophy

Manifesto for Agile Software Development

- We are uncovering better ways of developing software by doing it and helping others do it. Through this work we have come to value:
  - Individuals and interactions over processes and tools
  - Working software over comprehensive documentation
  - Customer collaboration over contract negotiation
  - Responding to change over following a plan

- That is, while there is value in the items on the right, we value the items on the left more.

http://agilemanifesto.org/principles.html

T&E for Agile IT