www.DAU.mil

Title: Cybersecurity as it Applies to the Survivability Key Performance Parameter

Defense Acquisition University

Certification Training | Knowledge Sharing | Continuous Learning | Mission Assistance

Date: 6 June 2018

Presenters: Vincent Lamolinara, Professors of Acquisition Cybersecurity, Defense Acquisition University, Mid-Atlantic Region

Moderator: Jim Davis, Logistics Department Chair, Defense Acquisition University, Mid-Atlantic Region

Background

DepSecDef (DSD) directed Joint Staff to develop Cybersecurity KPP

- DOT&E Cybersecurity Report … *"Highlighted multiple weapon systems with vulnerabilities that should have been known and fixed prior to DT&E."*

- JCS Guidance from JROC Memo 009-17, 27 Jan 2017:
  - Cyber Survivability Endorsement (CSE) Implementation Guide (now v1.01a)
  - 10 Cyber Survivability Attributes (CSAs)

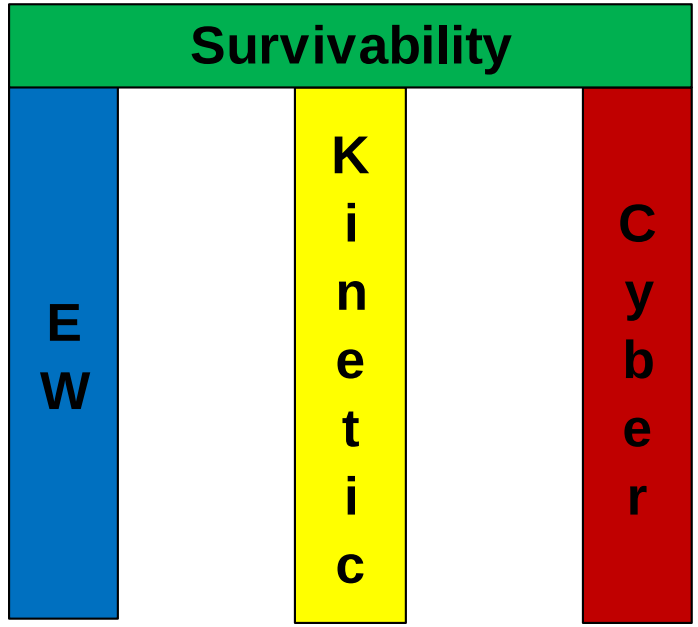
- CSE Implementation Guide helps sponsors articulate cyber survivability requirements in the ICD, AoA, CDD (KPP starts here), & CPD entered in the Knowledge Management / Decision Support (KM/DS) tool for programs with Joint Requirements Oversight Council (JROC) interest, Joint Capabilities Board (JCB) Interest, or qualify as Joint Integration.

- Although the CSE is only required for these levels of Joint interest, the Services are encouraged to use this guide for requirement documents that are validated by the DoD Component sponsor.

2

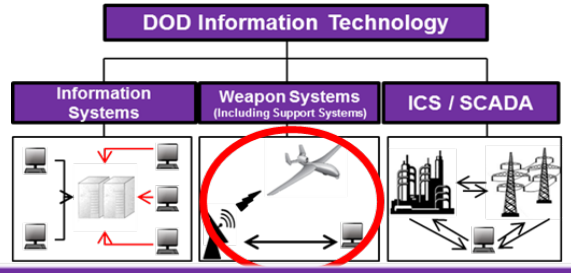
Cyber Survivability Requirement

- **System Survivability Key Performance Parameter (KPP)**
  - SS KPP = Kinetic, EW & Cyber
  - Cyber Survivability Endorsement (CSE) From Joint Staff
    - Three pillars:

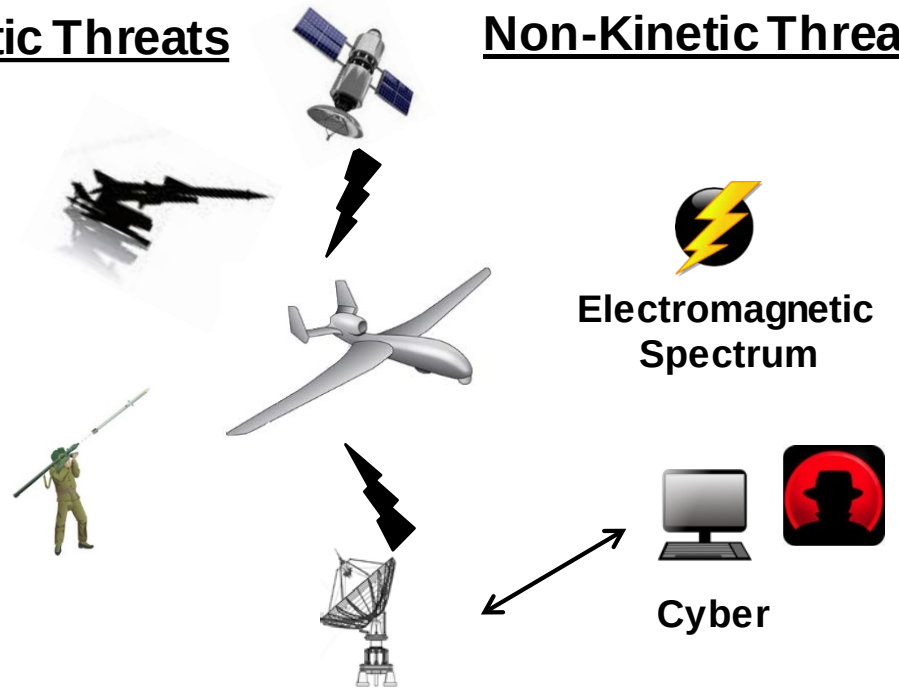


Prevent – design principles that protect system's mission functions from most likely cyber threats	***Mitigate –*** design principles to detect and respond to cyber-attacks; enable the mission system to survive attacks and complete the mission	***Recover –*** design principles to enable recovery from cyber-attacks and prepare mission systems for the next fight

Cyber Survivability Endorsement (CSE)

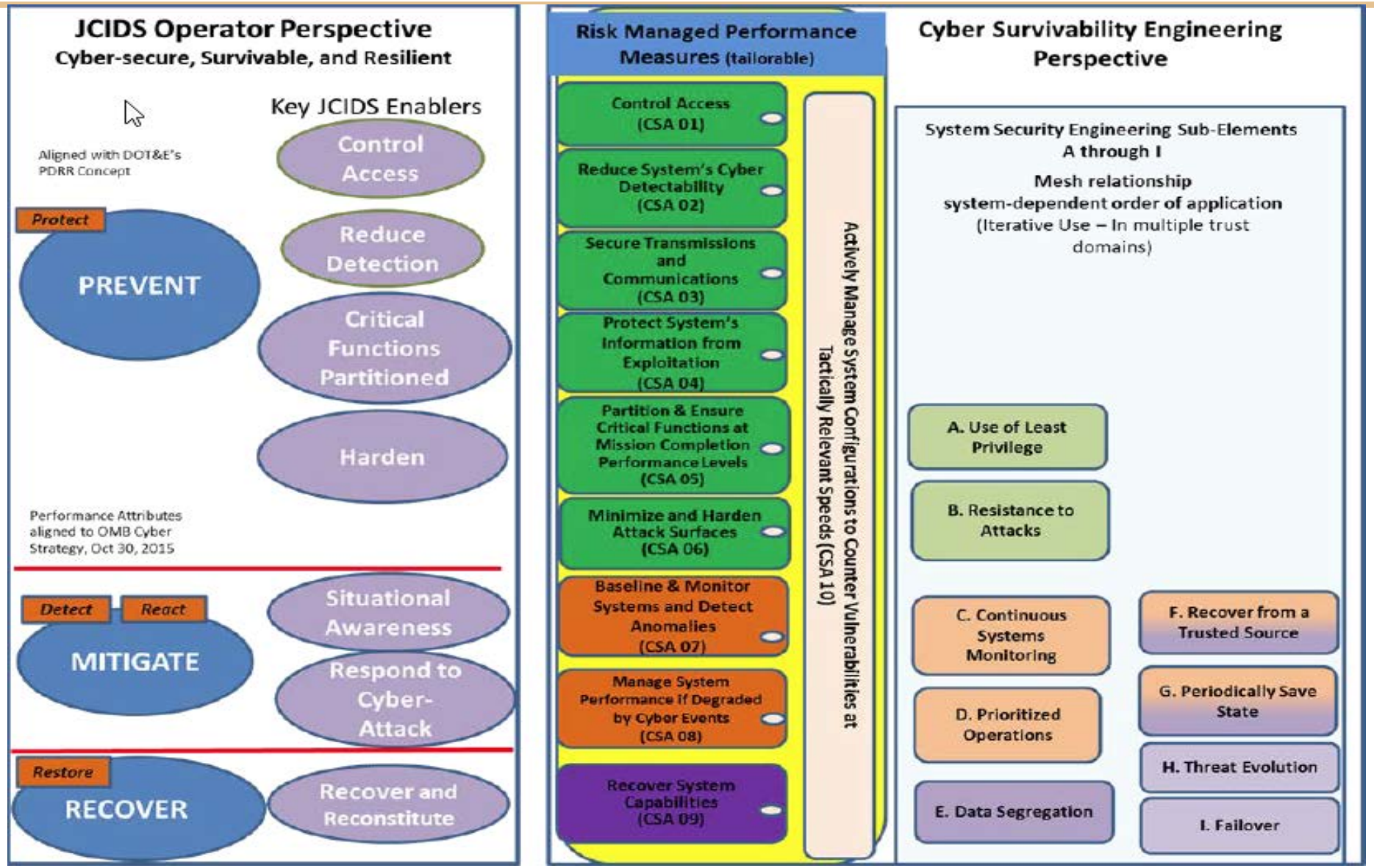


SS KPP Pillars	Cyber Survivability Attributes (CSA)	
Prevent	CSA 01 - Control Access	CSA 10 - Actively Manage System's Configuration to Counter Vulnerabilities at Tactically Relevant Speeds
	CSA 02 - Reduce Cyber Detectability	
	CSA 03 - Secure Transmissions and Communications	
	CSA 04 - Protect Information from Exploitation	
	CSA 05 - Partition and Ensure Critical Functions at Mission Completion Performance Levels	
	CSA 06 - Minimize and Harden Cyber Attack Surfaces	
Mitigate	CSA 07 – Baseline & Monitor Systems, and Detect Anomalies	
	CSA 08 - Manage System Performance if Degraded by Cyber Events	
Recover / Resiliency	CSA 09 - Recover System Capabilities	



Must address Cyber Survivability Attributes (CSA) as part of the System Survivability KPP

Systems Security Engineering (SSE) Sub-Elements



Cyber System Survivability Risk

Step 1: Select Mission Type
- MT1 – Organization Support
- MT2 – Mission Support
- MT3 – Operational / Tactical
- MT4 – Strategic / National

Criticality Analysis

Mission Functions
Type1 – Required
Type 2 – Supporting
Type 3 – Not Required

Step 2: Select Cyber Dependence Level
- DL1 – Sustain Ops / Maneuver
- DL2 – Maintain Communications
- DL3 – Offensive / Defensive Activities

Step 3: Select Adversary Tier Threat
AT1 – Nascent
AT2 – Limited
AT3 – Moderate
AT4 – Advanced

Step 4: Select Impact Level
IL1 – Acceptable
IL2 – Limited
IL3 – Serious
IL4 – Severe

Step 5: Cyber Survivability Risk Category
CSRC1 – Low
CSRC2 – Moderate
CSRC3 – High
CSRC4 – Very High

CSRC aggregates Mission, Cyber Dependence & Threat to inform ICD/CDD/CPD language & SSE Sub-elements / Security Controls applied

Cyber Survivability Attributes (CSA) & the Risk Management Framework (RMF)

- **~800 NIST 800-53 Cybersecurity Technical Controls**
  - Supports the Risk Management Framework (RMF)
  - Consist of 18 Control Families

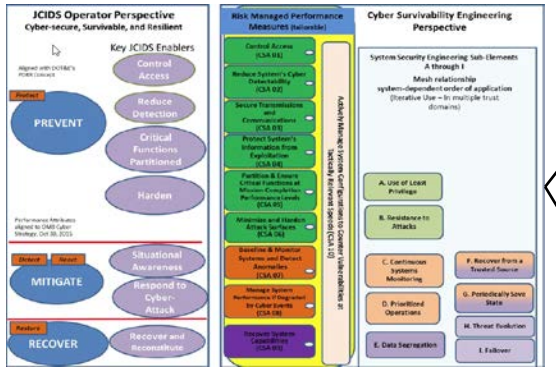
ID	FAMILY	ID	FAMILY
AC	Access Control	MP	Media Protection
AT	Awareness and Training	PE	Physical and Environmental Protection
AU	Audit and Accountability	PL	Planning
CA	Security Assessment and Authorization	PS	Personnel Security
CM	Configuration Management	RA	Risk Assessment
CP	Contingency Planning	SA	System and Services Acquisition
IA	Identification and Authentication	SC	System and Communications Protection
IR	Incident Response	SI	System and Information Integrity
MA	Maintenance	PM	Program Management

- **239 Identified NIST controls potentially applicable to CSAs**
  - 98 Highly Applicable
  - 86 Somewhat Applicable
  - 55 Require Interpretation

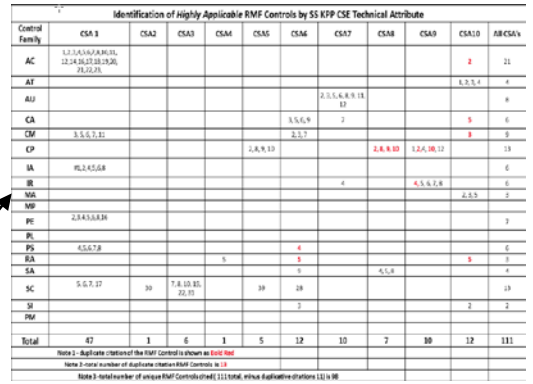
CSA to RMF to System Security Engineering (SSE) Mapping

- SS KPP to CSA to RMF (NIST Security Controls) to ***SSE Mapping***
  - Least Privilege
  - Resistance to Attack
  - Continuous Monitoring
  - Prioritized Operations
  - Data Segregation
  - Recover from a Trusted Source
  - Periodically Save State
  - Threat Evolution
  - Failover
- "Mesh" Interrelation
- Focus on ***Weapon System*** germane controls
- Adapt controls for SSE which is ***more relevant to Weapon Systems***
- ***Exemplar SSE Requirements Language*** for:
  - ICD / CDD / CPD
  - RFP
  - SOW

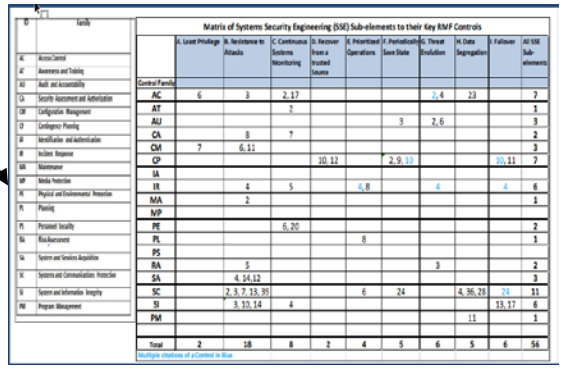
CSA to SSE



RMF - CSA



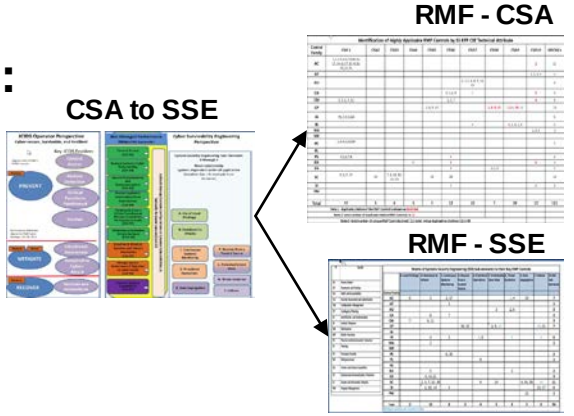
RMF - SSE



Mesh Interrelation Example

Implementation of **CSA 9 Recover System Capabilities** might require **SSE sub-elements:**

- **"prioritized operations**" to shed lower priority tasks,
- **"periodically save state"** to establish the restart point, and
- **"recover from a trusted source"** to ensure return to normal operations.



NIST SP 800-53 Control CP-10 "Information System Recovery and Reconstitution":

- Specifically, the control CP-10 (4) "Restore Within Time Period" would be germane
- **Language from NIST SP 800-53** for use in **ICD/CDD** could include:
  - "Restoration of information system components includes reimaging which restores components to known, operational states".

SSE RFP Language for **CSA 9** might include:

- "In the event of cyber attack, compromises, or events, the system must be capable of being restored to an effective operational state in which the system's software, configuration and operational information, security protections, and mission systems information are at pre-attack assured levels".

CSA 9 clearly is interrelated to **CSA 7** Baseline and Monitor System And Detect Anomalies & **CSA 8** Manage System Performance if Degraded by Cyber Events

System Security Engineering Analytical Sequence

Architecture

1) CSA 5 Partition and Ensure Critical Functions at Mission Completion Performance Levels
2) CSA 6 Minimize and Harden Attack Surfaces

Mitigation

3) CSA 7 Baseline and Monitor System And Detect Anomalies
4) CSA 8 Manage System Performance if Degraded by Cyber Events

Protection

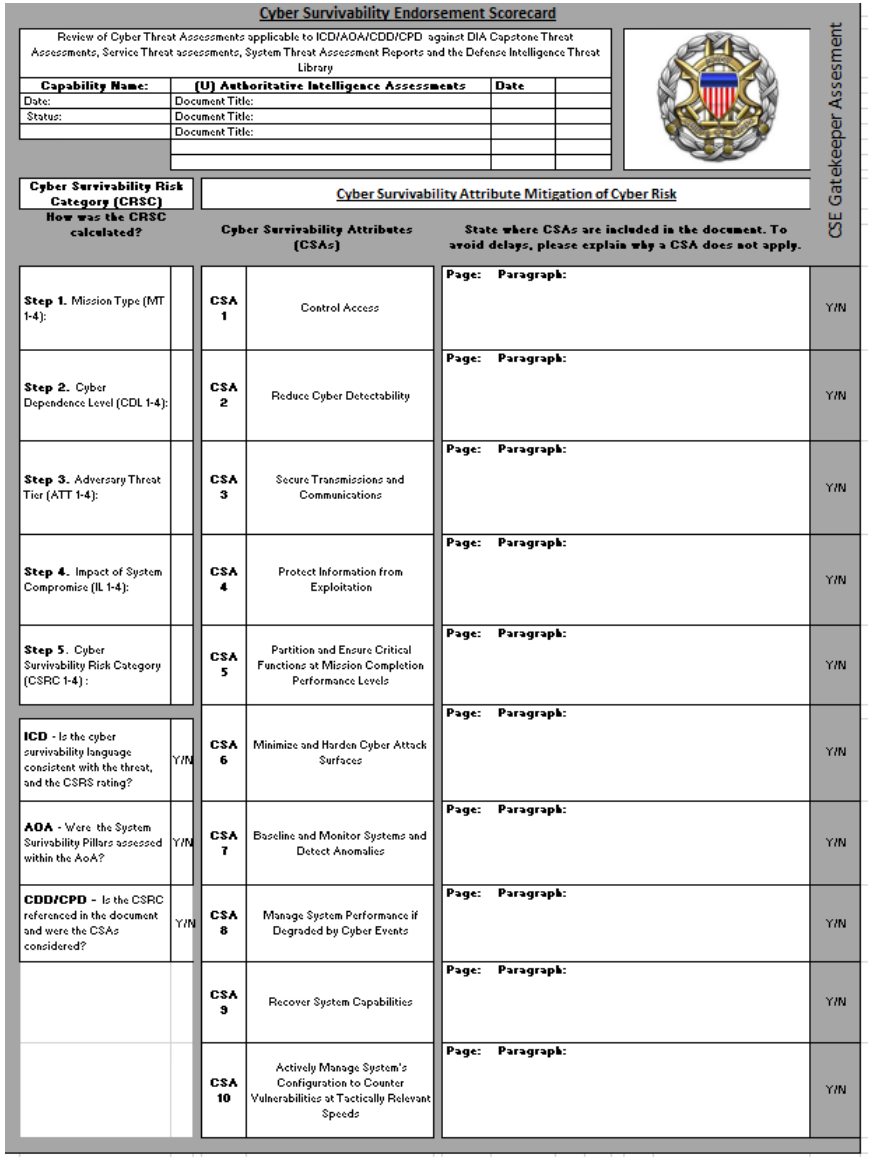
5) CSA 1 Control Access
6) CSA 2 Reduce System Cyber Detectability
7) CSA 3 Secure Transmissions and Communications
8) CSA 4 Protect System Information from Exploitation

Recovering

9) CSA 9 Recover System Capabilities
10) CSA 10 Actively Manage System Configurations to Counter Vulnerabilities At Tactically Relevant Speeds

CSE Scorecard Assessment Process

- **CSE assessment** occurs during the 21 day Document Review and commenting stage within the JCIDS Deliberate process.
- **Requirements Sponsors** use the CSE Scorecard to document that appropriate CSAs are in requirement's documents.
- **CSE analysts** use the CSE Scorecard to assess ICD,CDDs & CPDs with Joint interest.



Cyber Survivability Endorsement Scorecard

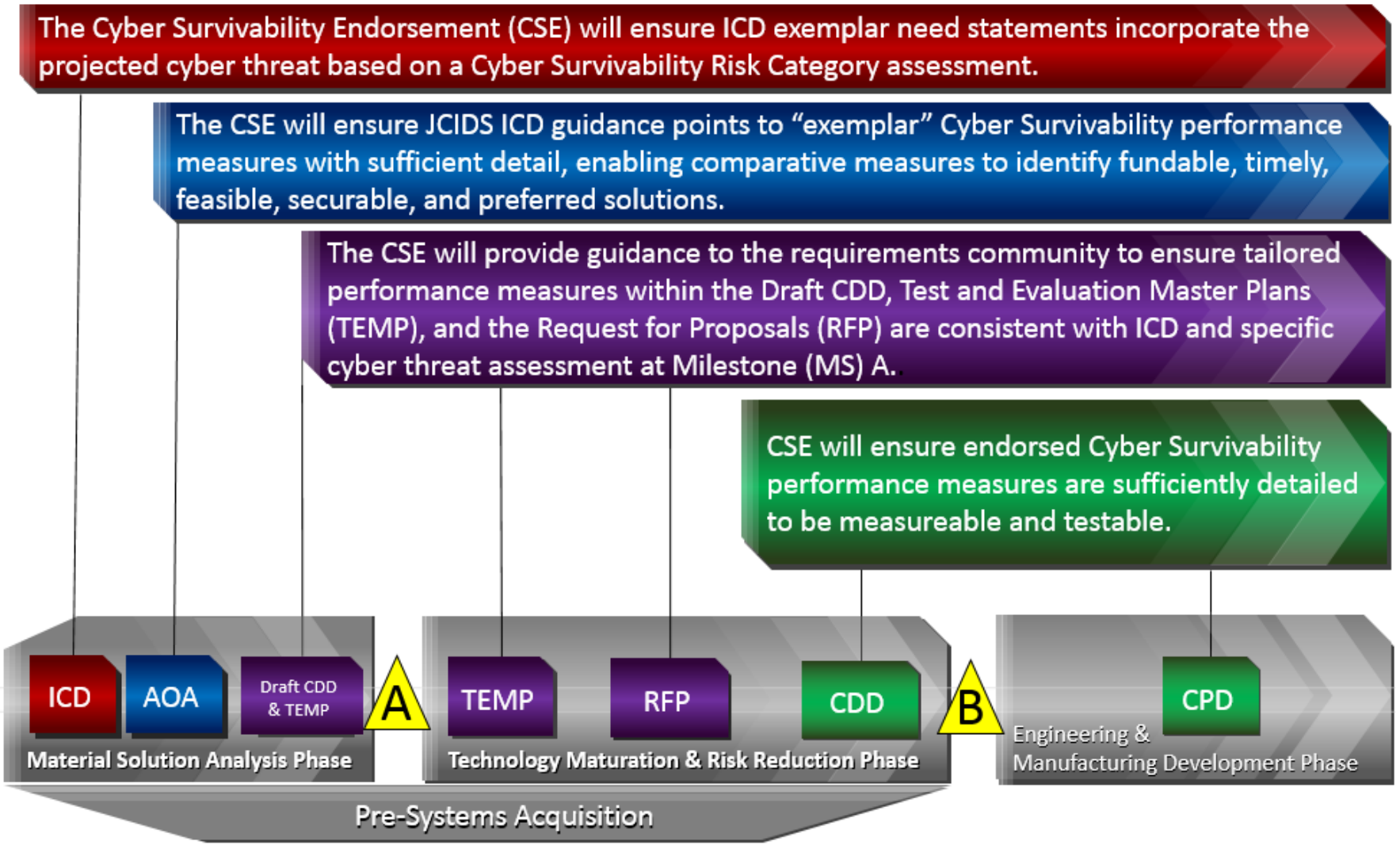
Review of Cyber Threat Assessments applicable to ICD/AOA/CDD/CPD against DIA Capstone Threat Assessments, Service Threat assessments, System Threat Assessment Reports and the Defense Intelligence Threat Library

Capability Name:	(U) Authoritative Intelligence Assessments	Date	
Date:	Document Title:		
Status:	Document Title:		
	Document Title:		

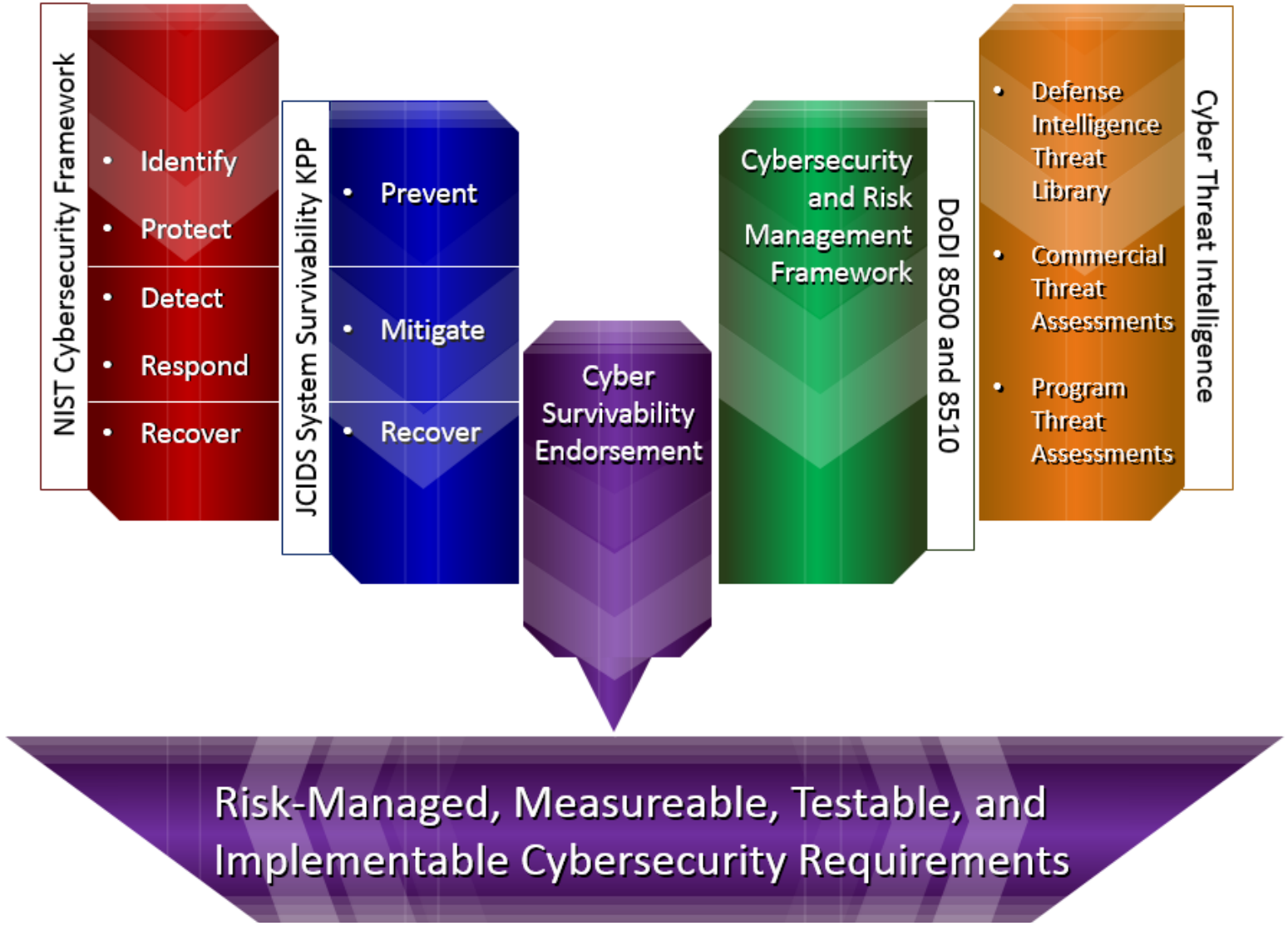
CSE Gatekeeper Assesment

Cyber Survivability Risk Category (CRSC) How was the CRSC calculated?		Cyber Survivability Attribute Mitigation of Cyber Risk: Cyber Survivability Attributes (CSAs)		State where CSAs are included in the document. To avoid delays, please explain why a CSA does not apply.	
Step 1. Mission Type (MT 1-4):		**CSA 1**	Control Access	**Page: Paragraph:**	Y/N
Step 2. Cyber Dependence Level (CDL 1-4):		**CSA 2**	Reduce Cyber Detectability	**Page: Paragraph:**	Y/N
Step 3. Adversary Threat Tier (ATT 1-4):		**CSA 3**	Secure Transmissions and Communications	**Page: Paragraph:**	Y/N
Step 4. Impact of System Compromise (IL 1-4):		**CSA 4**	Protect Information from Exploitation	**Page: Paragraph:**	Y/N
Step 5. Cyber Survivability Risk Category (CSRC 1-4) :		**CSA 5**	Partition and Ensure Critical Functions at Mission Completion Performance Levels	**Page: Paragraph:**	Y/N
ICD - Is the cyber survivability language consistent with the threat, and the CSRS rating?	Y/N	**CSA 6**	Minimize and Harden Cyber Attack Surfaces	**Page: Paragraph:**	Y/N
AOA - Were the System Survivability Pillars assessed within the AoA?	Y/N	**CSA 7**	Baseline and Monitor Systems and Detect Anomalies	**Page: Paragraph:**	Y/N
CDD/CPD - Is the CSRC referenced in the document and were the CSAs considered?	Y/N	**CSA 8**	Manage System Performance if Degraded by Cyber Events	**Page: Paragraph:**	Y/N
		CSA 9	Recover System Capabilities	**Page: Paragraph:**	Y/N
		CSA 10	Actively Manage System's Configuration to Counter Vulnerabilities at Tactically Relevant Speeds	**Page: Paragraph:**	Y/N

Cyber Survivability & DoD Acquisition



Cyber Survivability Provides an Integrated Framework



HOWEVER….. Case Study of Warfighter Information Network –Tactical (WIN-T) Inc 2


Network Operations Security Center - Lite (NOSC-L)

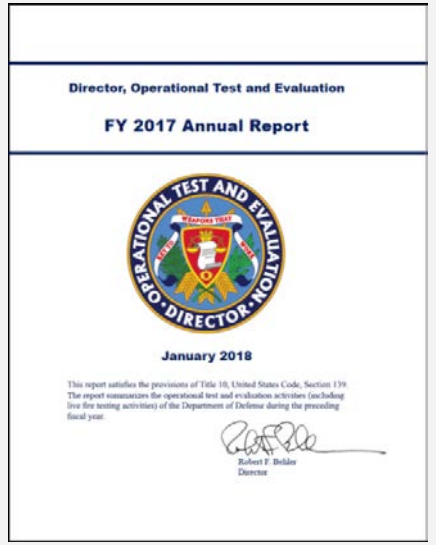

Tactical Communications Node - Lite (TCN-L)

Win-T Passed Adversarial Cyber FOT&E

- Directed by AT&L to change approach

Change of Approach

- Cybersecurity part ***systems engineering*** vice separate solution
- PM developed Tech Roadmap, responsive Vendors & instituted agile programming, incremental capability / patch drops
  - **% Fix Effectiveness was key metric!**
- ***Assumption of breach***: Lowest level of trust between SoS
- ***Independent and continuous testing*** (JHU-APL) for fixes & capability drops
  - Level of knowledge required was not complete in Program Office or Vendors
  - On the Spot Test & Developer fixes
  - Development of threat models, with > 10 million threat simulations


Director, Operational Test and Evaluation

FY 2017 Annual Report

January 2018

RMF Security Controls and Cyber Survivability Attributes: only part of the solution

Asymmetric Warfare: Excess Armor Doesn't Help

Kinetic Warfare is a modern Goliath

- Strikes fear in the heart of Adversaries
- Survivability / Armor, weapons & support cost a lot

Cyber is like David & his Slingshot

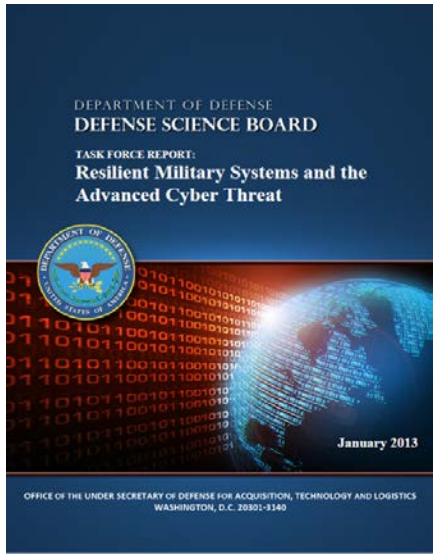
- Another Warfare Domain
- Armor doesn't work well
- Offense is Cheaper
- Disruptive Technology

Security Armor: Diminishing Return On Investment (ROI)

- GAO Audit: DHS $6 Billion "Einstein" IDS Not Effective
  - Does not scan for 94 percent of commonly known vulnerabilities or check web traffic for malicious content
- Multiple Denial of Service Vulnerabilities in Cisco Adaptive Security Appliance (ASA) Software: firewall, IPS, endpoint security (anti-x)
  - More than the Router it protects!
- AFRL Avionics Cyber Hardening and Resiliency Manual:
  - ***Attackers can use Security functions against you!***
    - Prevent Decryption of Data
    - Use Malware Detection to cause Shutdown
    - Use Monitoring System itself for Access to System

"Could protection add a vulnerability by adding features with unknown susceptibilities that an adversary could exploit or by causing the protection to trigger falsely?"

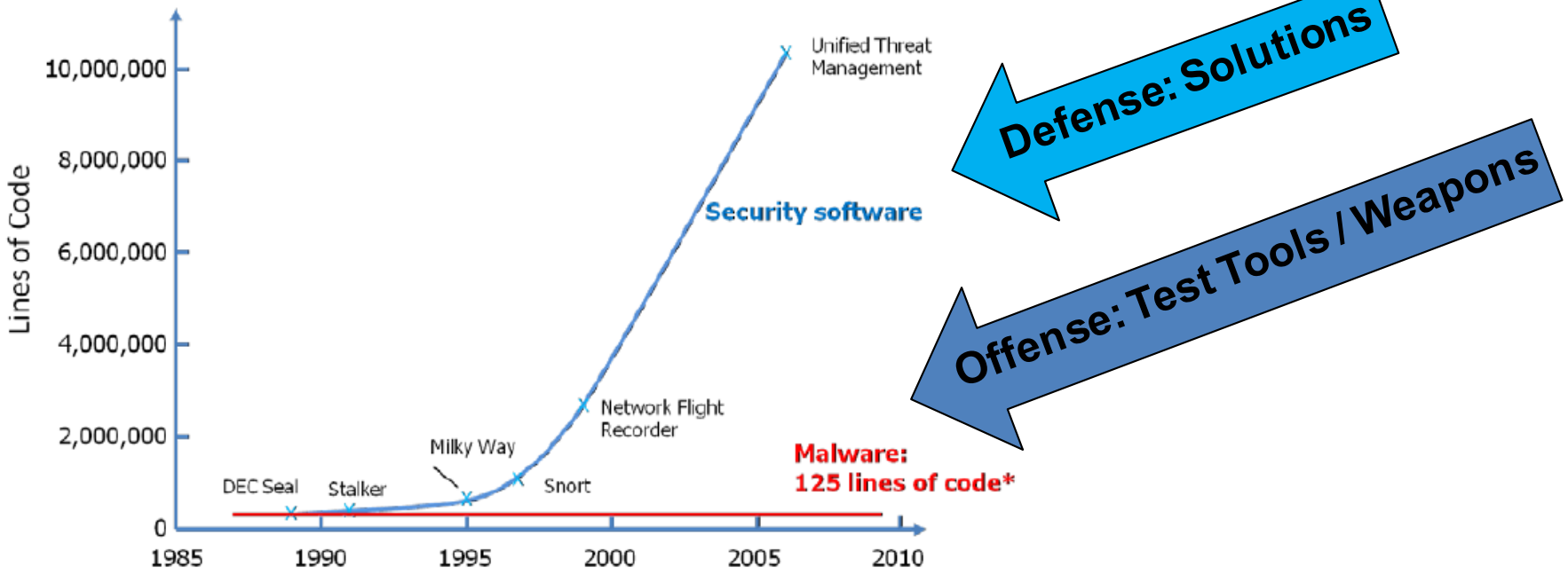
Uunderstanding Offense (Testing) is Key to Defining Sufficient Survivability



*Not possible to prevent all high-tier cyber attacks!

Resilient Military Systems and the Advanced Cyber Threat

DEFENSE SCIENCE BOARD | DEPARTMENT OF DEFENSE



Defense becomes more and more complex, yet still outmatched by offense

*DARPA Brief to DSB, May 2011

* Malware lines of code averaged over 9,000 samples

Figure 3.2 Graphic Illustration of the Complexity of Software Required to Defend and Attack our Systems. Very Small Changes (Even Single Bits) Can Cause Major Impacts to the Operation of a System

OODA:
Offensive Cyber vs Cyber Defense

Defense Acquisition University

Col John Boyd

Conventional Warfare
Cyber Defense Speed

Have to get inside your opponents OODA:
Countermeasures, Signature, Maneuverability

Cyber Survivability Courses of Action (COAs)

COA : Conventional Assumptions

- Armor (Flying Tanks / Diminishing Returns)
- Balance Performance & Survivability Engineering
- Don't Ignore Technological Change

Failure to Innovate Has Consequences

Cyber Survivability COAs

COA: Offense vs Defense

- Maneuverability Metric
  Ps=V(T-D)/W
- Red / Blue Teaming / Constant Practice
- Mission-based Cyber Risk Assessments (i.e., Cyber Table Tops)

Designs Focused on Attack Are More Survivable

Red Teaming is a Way of Life

Simian Army

- Kill/inspect running instances
  - Chaos Monkey
  - Janitor Monkey
  - Security Monkey
  - Conformity Monkey
  - Chaos Gorilla*
  - Chaos Kong*

https://github.com/Netflix/SimianArmy

https://github.com/Netflix/security_monkey

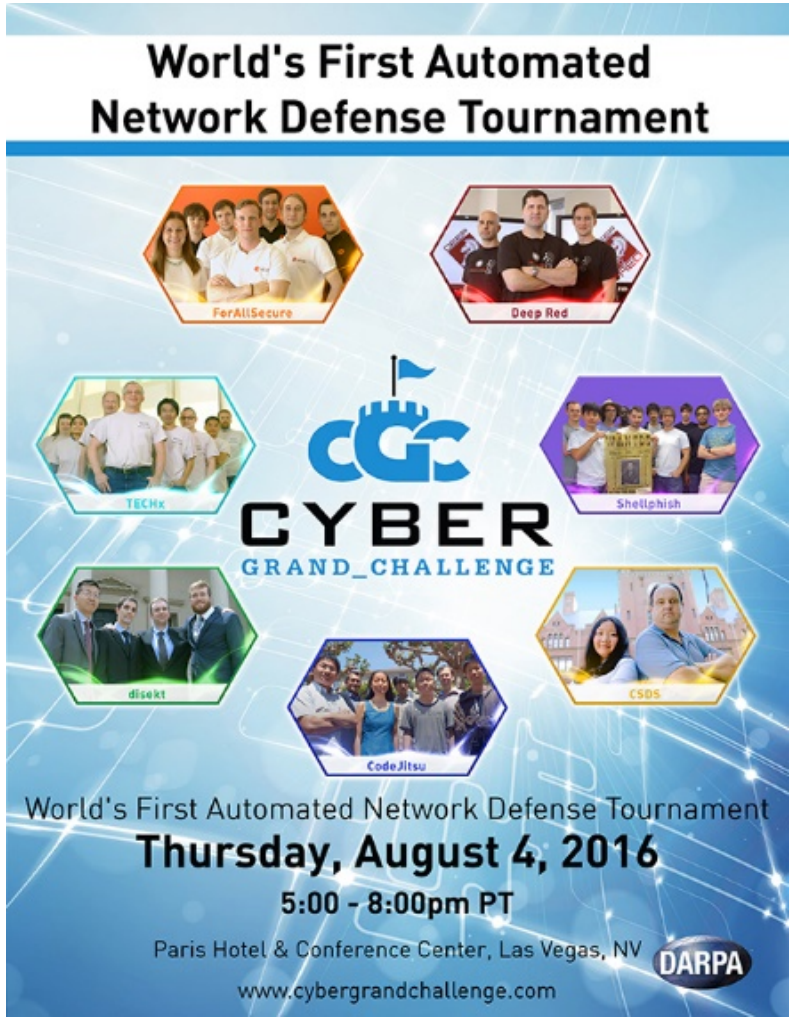
10/10/14 @SonOfGarr

Chaos Monkey randomly terminates virtual machine instances and containers that run inside of your production environment. ***Exposing engineers to failures more frequently incentivizes them to build resilient services.***

Cyber Survivability COAs

COA: Emergent Technology

- Automation Tools / Artificial Intelligence
  - Cyber Grand Challenge
  - Faster OODA with Machine Speed
  - Focus on Attacking (Yourself & the Adversary)



Auto-Patch / Defend / Attack: The New Speed of Cyber

Cost of Cyber Survivability? Resilience vs Perfect Design

Airborne Unmanned Sensor System (GAUSS) Cyber Resilience Demo - Georgia Tech, UVA & FAA

Triple Diverse Dynamic Redundancy

- 3 different computer boards
- 3 separate operating systems
- 3 versions of the security software

High-Assurance Cyber Military Systems (HACMS) - DARPA

1. Vehicle Experts	2. Operating Systems	3. Control Systems	4. Research Integration	5. Red Team
Boeing Pilot-able Unmanned Little Bird Helicopter	**NICTA** Synthesize file systems, device drivers, glue code; Verified sel4 kernel; Verified RTOS	**Galois** Embedded DSLs; Synthesize and verify control system code	**RC*/U. Minn** Compositional verification; Integrated workbench	**DRAPER*/AIS/ U. Oxford** Traditional penetration testing; novel formal methods approach
HRL*/GM American-Built Automobile	**SRI*/UIUC** EF-SMT solvers; Synthesize monitors and wrappers	**SRI*** Synthetic sensors; Synthesis for controllers of hybrid systems	**SRI*** Lazy Composition; Evidential Tool Bus & Kernel of Truth; Vehicle Integration	
	**Princeton*/Yale/ MIT** Build & verify in Coq OS for vehicle control; Verifying compiler for concurrent code; Program logics	**CMU*/Drexel/ SpiralGen/UIUC** Map high-level spec into low-level C code; Extend Spiral for hybrid systems		
	**Kestrel*** Synthesize protocols: refinement of high-level spec to low-level implementations	**UPenn*/UCLA** Synthesize attack-resilient control systems		

Program Timeline:

- BAA Release: Feb 23, 2012
- Kick-Off: Aug 8-10, 2012
- End of Phase 1: Jan 2014
- End of Phase 2: July 2015
- End of Phase 3: Jan 2017

Performers:

- 8 Primes (*)
- 22 Organizations Total

Scientifically Proven Secure Code

- 5 years in Development
- Only Critical Control Systems
- Only 1000's SLOC

Survive Every Attempted or Successful Hacking Attempt!
At a Great Cost / Schedule!

Generic PP / SSE RFP Language

Examples:

- Section C: Statement of Work - [SOWxxx1] The contractor shall develop and update mission criticality analysis(-es), vulnerability assessment(s), risk assessments(s), and identification and countermeasure implementation(s) for Mission-Critical Functions, the failure of which would result in either Catastrophic (Level I) or Critical (Level II) compromise of mission capability.

- Section C: System Requirements Document - [SRD001] For critical components of Level I Mission-Critical Functions, the system shall establish basic protection requirements unless justified by a cost-benefit analysis approved by the government. Those basic protections shall include:
  - Establish least privilege using distrustful decomposition (privilege reduction) or a similar approach to move Level I critical functions into separate mutually untrusting programs.
  - Physical and logical diversification of critical components for Mission-Critical Functions which require redundancy to meet reliability or safety requirements.
  - Physical and logical diversification with voting to establish trustworthiness of selected Level I Mission-Critical Function components.

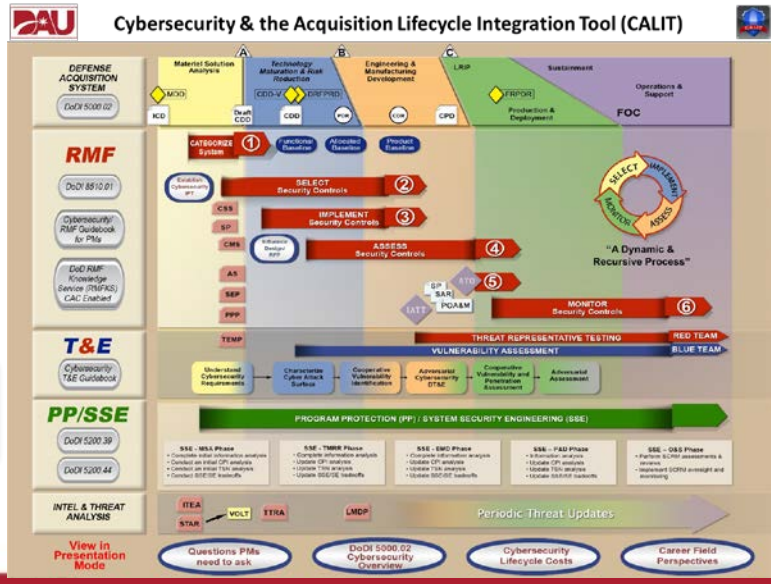
http://www.acq.osd.mil/se/initiatives/init_pp-sse.html
https://www.acq.osd.mil/se/docs/SSE-Language-for-TSN-in-DoD-RFPs.pdf

Cyber Survivability Best Practices: If I were a (Rich Man) PM

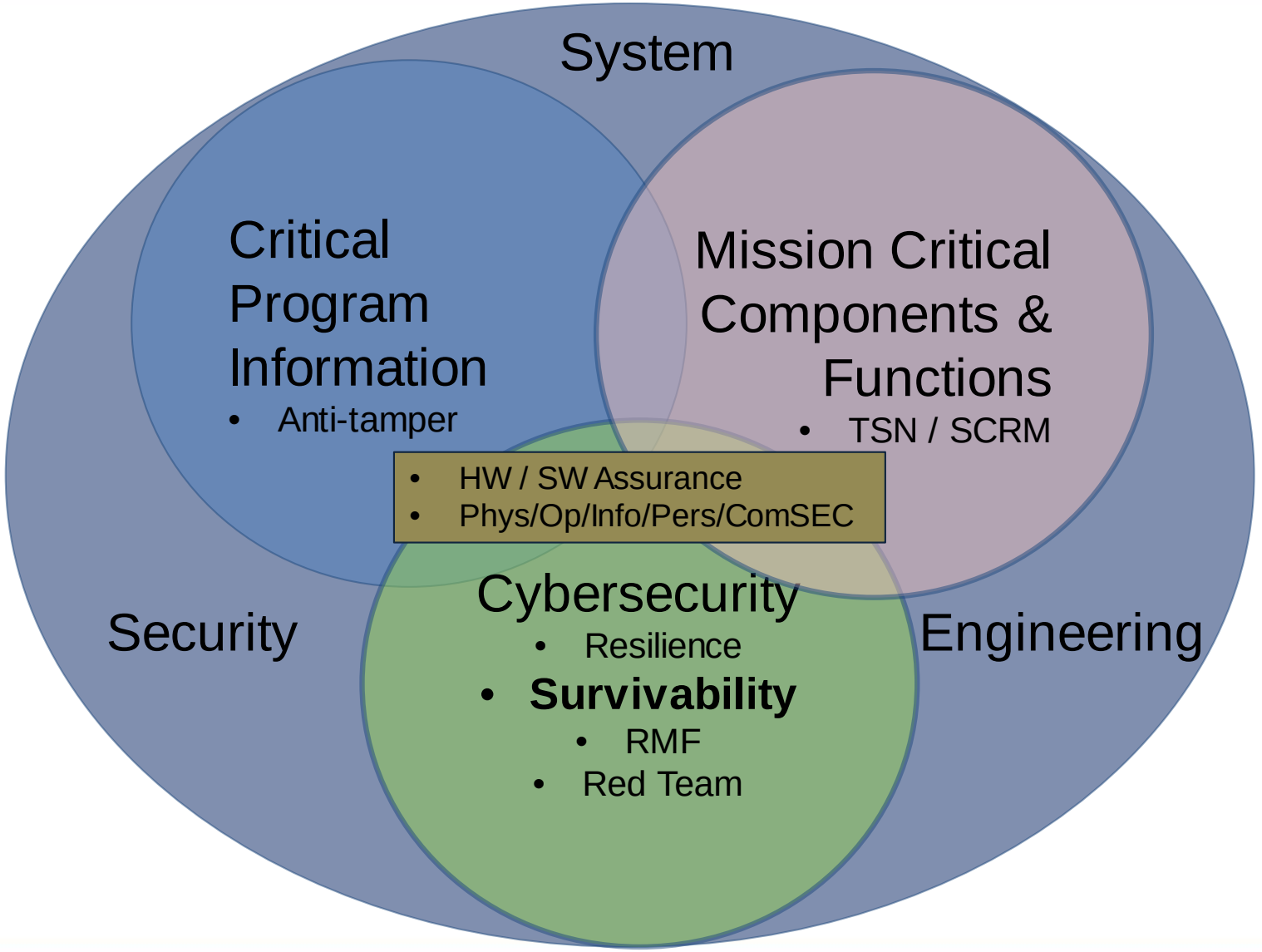
- Stand up Integrated Cyber Warfare Engineering Group / SSEWG
  - Testers, SwA, Logistics, IT, Intel, EW, Users and most of all Hackers
  - Train them with the pros (UARCs, FFRDCs, NSA, National Labs)
- Immediately conduct regular MBCRAs throughout lifecycle
- Build team a Lab were they can Attack systems and Learn
- Use Cyber Survivability Guidance to develop requirements: "Survive a zero-day attack on mission and flight computers"
- Invite Red Teams from day one: Use the Cyber Ranges
- Reward cost-wise solutions & deletion of excess Armor

Unified Acquisition: RMF, T&E, PP/SSE, Intel, CSE

A rich man is nothing but a poor man with money – W. C. Fields



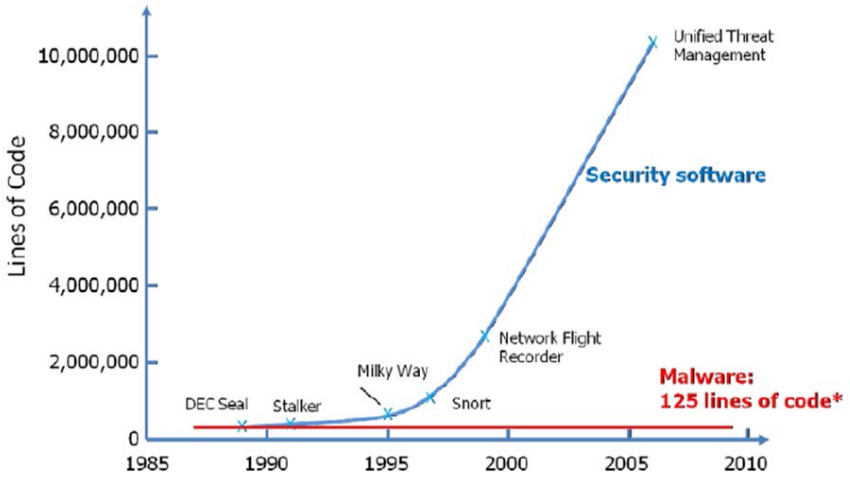
Integrated Cyber Warfare / System Security Engineering



Don't Just React to New Cyber Threats

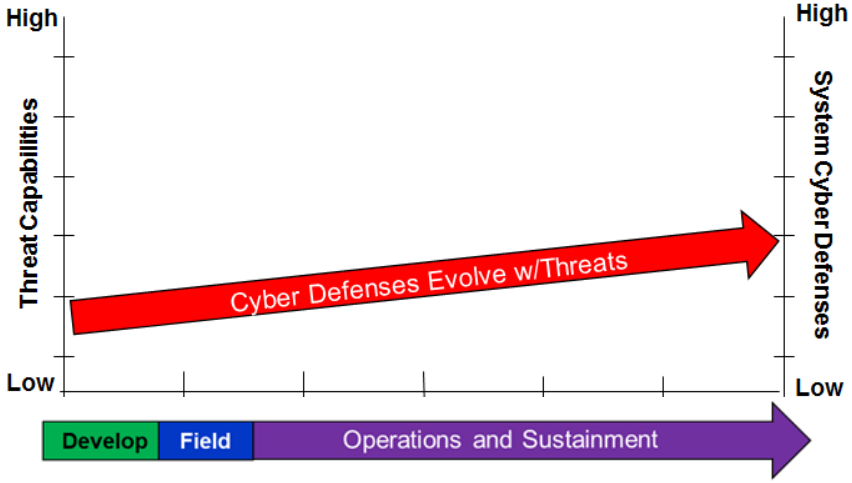
- Must PROACTIVELY ADAPT to new cyber threats
  - Must get inside of the Cyber Attacker's OODA!
- **Sustaining Cyber Survivability** requires PROACTIVE Resourcing, Design, Continuous Test, Life Cycle Sustainment Plans, and Ops & Maintenance procedures

Unsustainable



Agile Cyber Survivability SSE & Test

Requires Continuous Improvement



Cyber threats will continue to increase

Questions?

Additional Related Resources

- Cybersecurity Community of Practice (COP)

  https://www.dau.mil/cop/cybersecurity/Pages/Default.aspx

- Cybersecurity and Acquisition Lifecycle Integration Tool (CALIT)

  https://www.dau.mil/tools/t/Cybersecurity-and-Acquisition-Lifecycle-Integration-Tool-(CALIT)

- Cybersecurity Black Card

  https://www.dau.mil/tools/t/Cybersecurity-Quick-Reference-(Black-Card)

Contact Info

DAU Cybersecurity Enterprise Team

- Vinny Lamolinara

  240.895.7382

  Vincent.Lamolinara@dau.mil

- Roy Wilson

  240.895.7328

  Roy.Wilson@dau.mil