Cyber Risk to Mission:
NDIA Systems & Mission Engineering Division Planning Meeting

Mr. John Garstka, SES
Director, Cyber, Office of the Chief Information Security Officer,
Office of the Under Secretary of Defense for Acquisition and Sustainment

November 9, 2020

National Defense Strategy - 2018

Strategic Environment

- ***Challenges to the U.S military advantage*** represent another shift in the global security environment. For decades the United States has enjoyed uncontested or dominant superiority in every operating domain. We could generally deploy our forces when we wanted, assemble them were we wanted, and operate how we wanted. ***Today, every domain is contested – air, land, sea, space, and cyberspace.***

Build a More Lethal Force

- ***Space and Cyberspace as warfighting domains:*** The Department will prioritize investments in resilience, reconstitution, and operations to assure our space capabilities. We will also invest in ***cyber defense, resilience***, and continued integration of cyber capabilities into the full spectrum of military operations.

- ***Command, control, communications, computers and intelligence, surveillance, and reconnaissance (C4ISR).*** Investments will prioritize developing resilient, survivable, federated networks and information ecosystems from the tactical level up to strategic planning. Investments will also prioritize capabilities to gain and exploit information, deny competitors those same advantages, and enable us to provide attribution while defending against and holding accountable state or non-state actors during cyberattacks.

DoD Cyber Strategy – 2018: Key Objectives

1. **Ensuring the Joint Force can achieve its missions in a contested cyberspace domain.**
2. **Enhancing Joint Force military advantages through the integration of cyber capabilities into planning and operations.**
3. **Deterring, preempting, or defeating malicious cyber activity targeting U.S. critical infrastructure that is likely to cause a significant cyber incident.**
4. **Securing DoD information and systems, including on non-DoD-owned networks, against cyber espionage and malicious cyber activity.**
5. **Expanding DoD cyber cooperation with allies, partners, and private sector entities.**

Have We Built/Are We Building "Battleships"?

You are never as invincible as you believe

Ref: Army-Navy Football Game Program, Franklin Memorial Stadium, Philadelphia, Pennsylvania, November 29, 1941. Page 180. Navy defeated Army, 14-6.

A classic bow shot of the U.S.S. Arizona with the following caption: "A bow on view of the U.S.S. Arizona as she plows into a huge swell. **It is significant that despite the claims of air enthusiasts no battleship has yet been sunk by bombs.**"

On December 7, just one week after this game was played, the Arizona was sunk by bombs dropped by Japanese aircraft with a great loss of life.

Cyber Risk to Mission: The Mission Stack

DoD Missions

- **DoD Weapon Systems / Platforms**

  FY16 NDAA Section 1647

- **DoD IT and Networks**

- **DoD Critical Infrastructure**

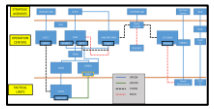
  FY17 NDAA Section 1650
  FY18 NDAA Section 1643

- **Commercial Critical Infrastructure**

- **Defense Industrial Base**

  DIB Cybersecurity
  Supply Chain Risk Management

People, Process & CONOPS



Information Technology (IT)

Operational Technology (OT) [ICS/SCADA, etc.]

ICS: Industrial Control System
SCADA: Supervisory Control and Data Acquisition

Operating in a Contested Cyber Environment

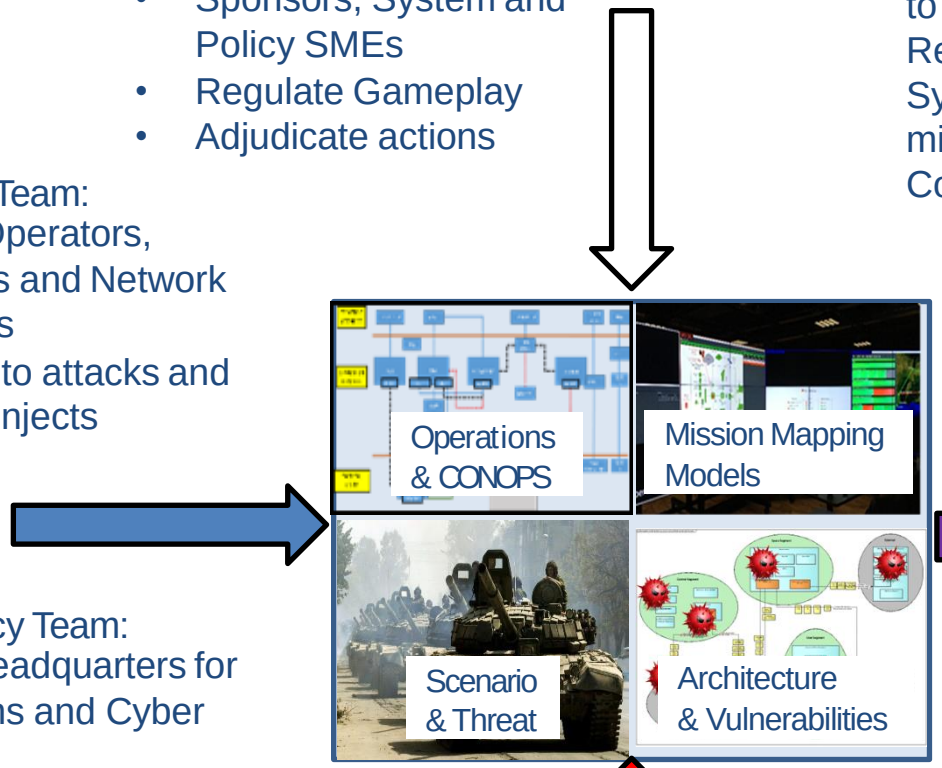
- **Cyber Risk to Mission is present whenever the cyber or cyber-enabled capabilities that a commander depends upon fail to match operational expectations putting the mission at risk**
- CRM is not about why one's cyber and cyber-enabled capabilities do not satisfy mission requirements; it is about the consequence to mission effectiveness that results from adversely impacted cyber capabilities
- Cyber Risk to Mission is an "All Hazard" Risk; a shortfall in cyber and/or cyber-enabled capability can result from a variety of causes (not only as a result of cyberattacks but could be a result of a kinetic attack or an accident)
- The attack surface includes much more than the network itself; we need to defend the entire mission stack

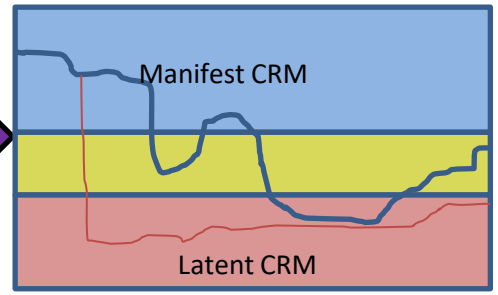
Mission Resiliency Wargame Overview

White/Control Team:
- Sponsors, System and Policy SMEs
- Regulate Gameplay
- Adjudicate actions

Four moves over four days to assess the Cyber Resiliency of the Weapon System and risks to the mission in a Cyber Contested Environment

Blue Tactical Team:
- System Operators, Engineers and Network Defenders
- Respond to attacks and scenario injects

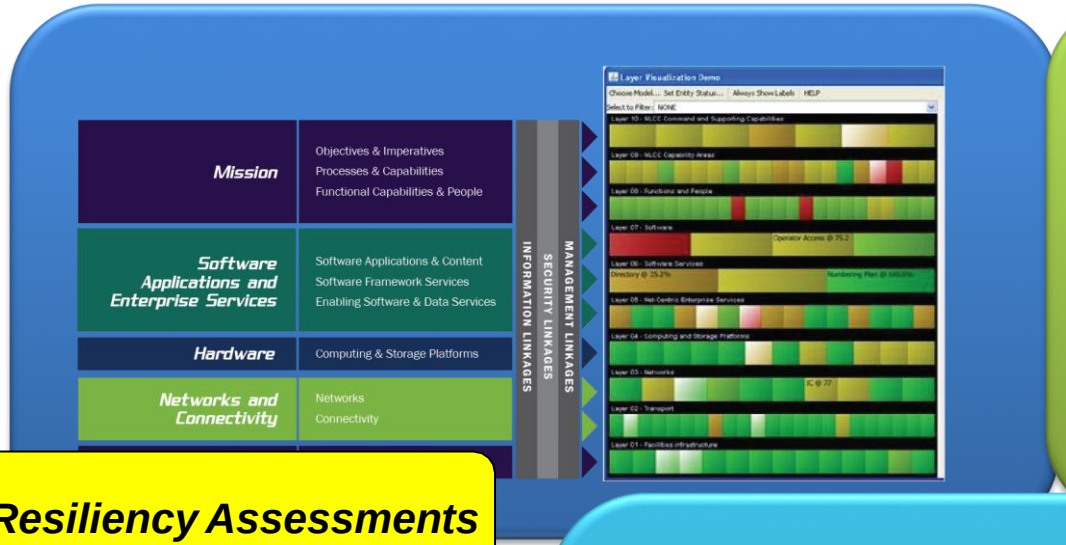




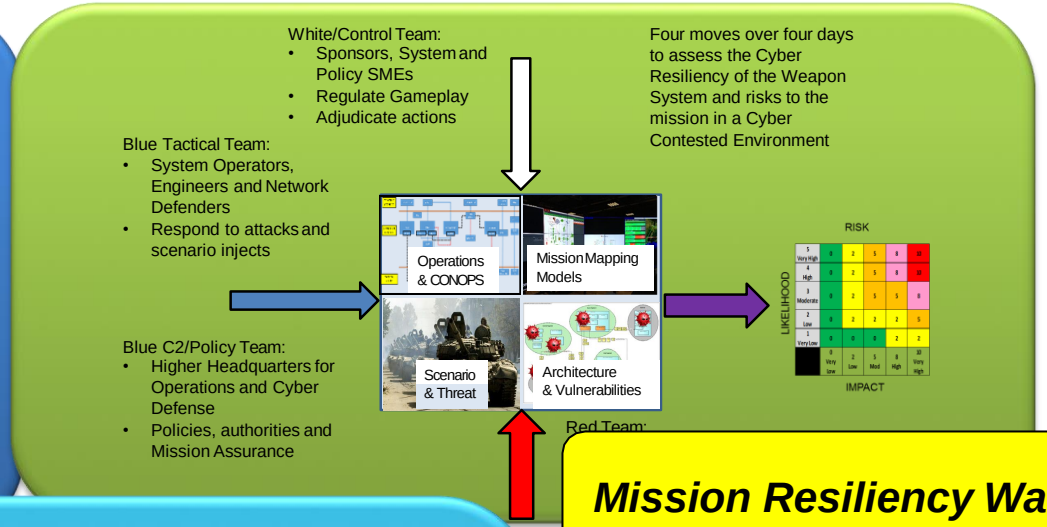
Blue C2/Policy Team:
- Higher Headquarters for Operations and Cyber Defense
- Policies, authorities and Mission Assurance

Red Team:
- IC, System SMEs and Attack/Red Team SMEs
- Campaign Plan
- Attack planning and execution

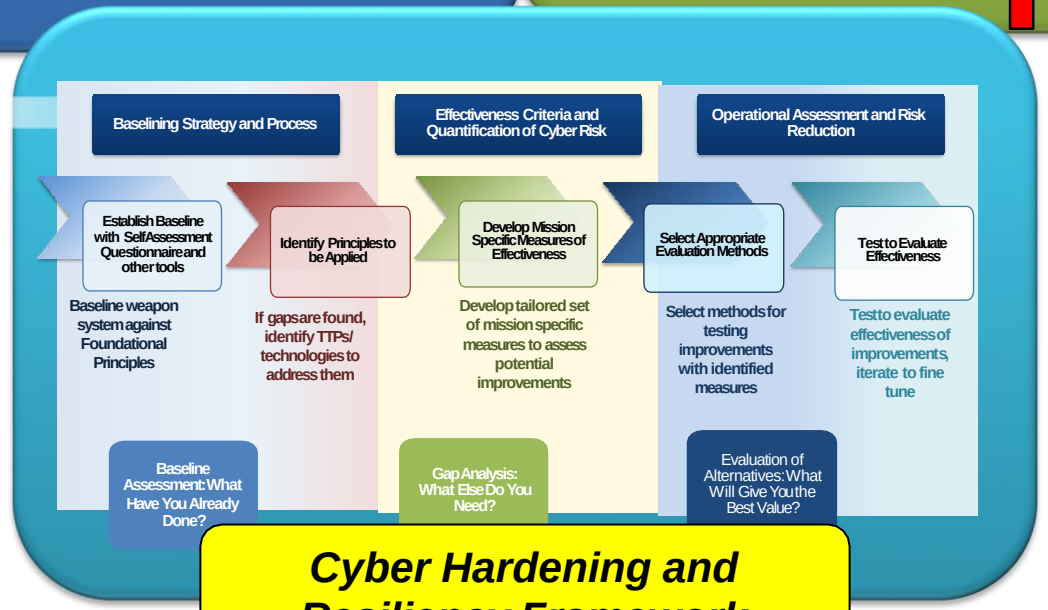
Understanding and Countering Cyber Risk to Mission Takes Ongoing Cooperative Efforts



Cyber Resiliency Assessments



Mission Resiliency Wargaming



Cyber Hardening and Resiliency Framework

Summary

- Mission “ecosytems” are systems of systems architectures, supported by people, processes and policies
- Cyber security and cyber defense must be part of system design and engineering
- Managing Cyber Risk to Mission (CRM) is critical for mission success when operating in a Contested Cyber Environment
- Remediations and mitigations must be brought throughout the whole Mission Stack manage this risk
- C2 of Cyberspace and Kinetic Operations must be harmonized to effectively and efficiently manage CRM