Operating in a Cyber Contested Environment

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

October 31, 2019

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.

Cyberspace is a *Contested* Operational Domain

Blue Kinetic Forces
Dependent Upon
Cyberspace

Adversary Kinetic Forces
Dependent Upon
Cyberspace

Enabling information and computing environment

Terrain and effects medium

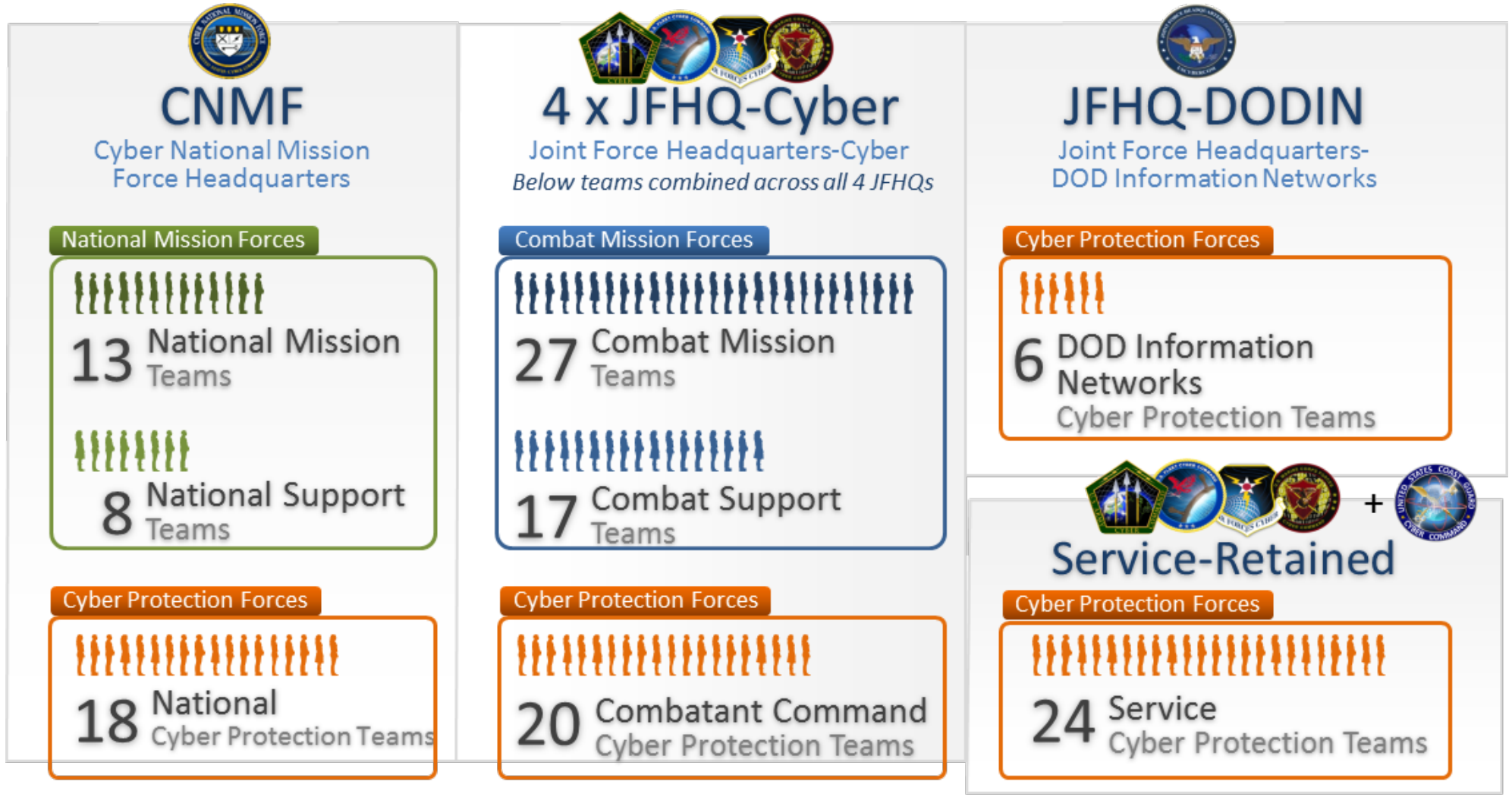
Adversary Cyber Forces
Operating in Cyberspace

Blue Cyber Forces Operating in Cyberspace

Offensive Forces
Defensive Forces

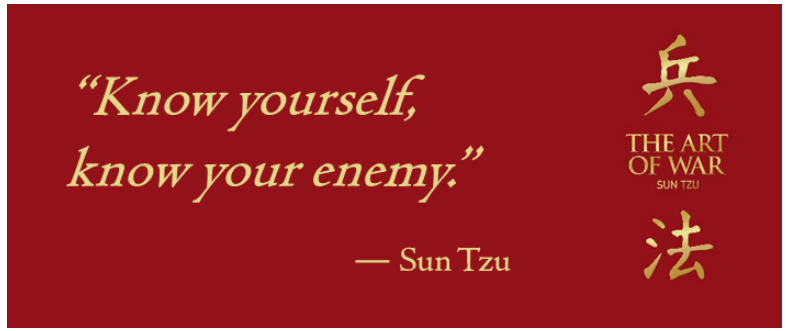
Organization of U.S Forces Operating in Cyberspace: Operational Level

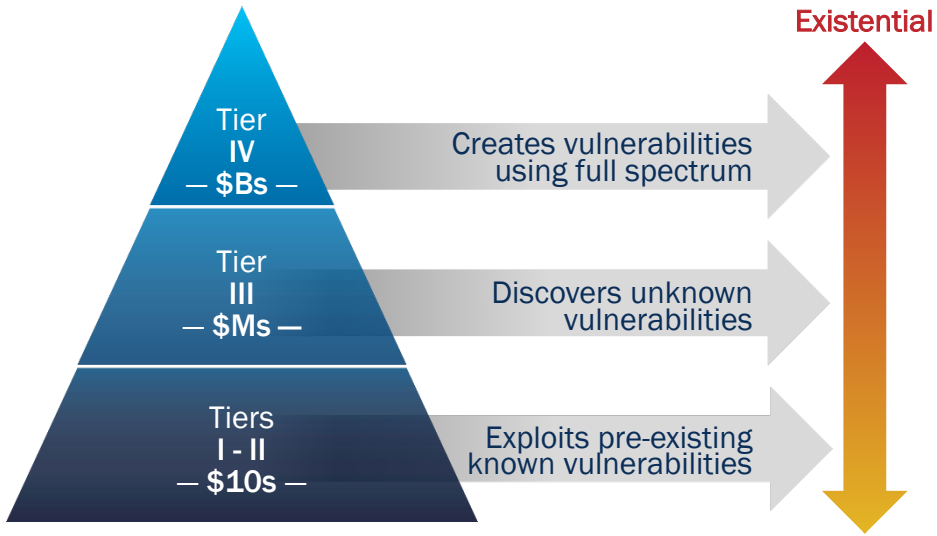
Organization of U.S. Forces Operating in Cyberspace: Tactical Level



Cyberspace is a *Contested* Operational Domain: Capabilities of Adversary Cyber Actors

Tier	Description
IV	**Advanced** – Have the capacity to conduct complex, long term cyber attack operations that combine multiple intelligence disciplines to obtain access to high-value networks
III	**Moderate** – Able to use customized malware with OPSEC practices to conduct wider-range intelligence collection operations, gain access to more isolated networks, and create short duration effects against critical infrastructure networks.
II	**Limited** – Able to identify and target for espionage or attack easily accessible unencrypted networks running common operating systems using publically available tools.
I	**Nascent** – Little to no organized cyber capabilities, with no knowledge of a networks underlying systems or industry beyond publically connected open-source information.



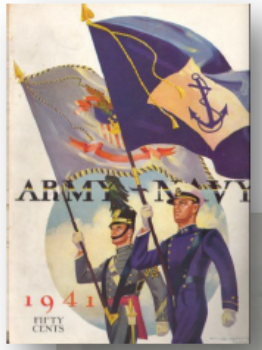


DENY DECEIVE DISRUPT DEGRADE DESTROY

DoD Forces must be able to operate in a contested cyber environment

Have We Built/Are We Building "Battleships"?

You are never as invincible as you believe



U.S.S. Boise, a light cruiser. It is remarkable that a light cruiser may be, and often is, heavier than a heavy cruiser, the only criterion of the heavy cruiser being that she mounts guns greater than 6.1 inch. At present our Navy has almost sixty such cruisers on order, most of which are to be delivered by 1944. Each such ship requires a crew of approximately 700 officers and men to man its fifteen 6-inch guns, and its four to eight planes. Within its blue-gray hull it carriers four sets of geared turbines which turn up well over 100,000 horsepower, the power of more than 1,000 average automobiles.

Right—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.

180

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

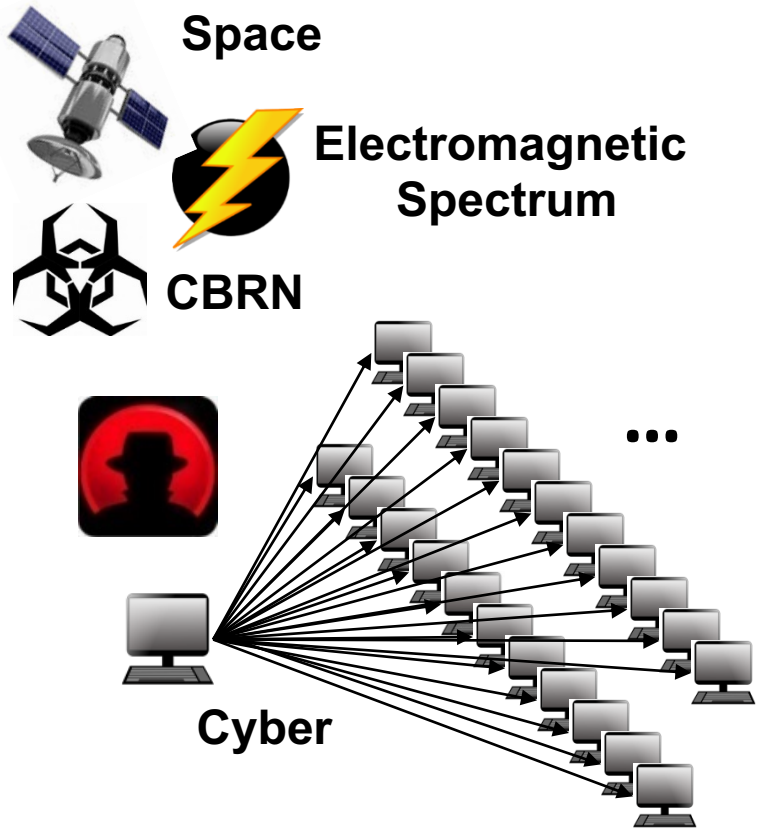
A classic bow shot of the U.S.S. Arizona with the following caption: "A bow on view of the U.S.S. Arizona as she plows into a huge swell. **It is significant that despite the claims of air enthusiasts no battleship has yet been sunk by bombs.**"

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.

SS-KPP & Cyber Survivability Endorsement

Kinetic Threats

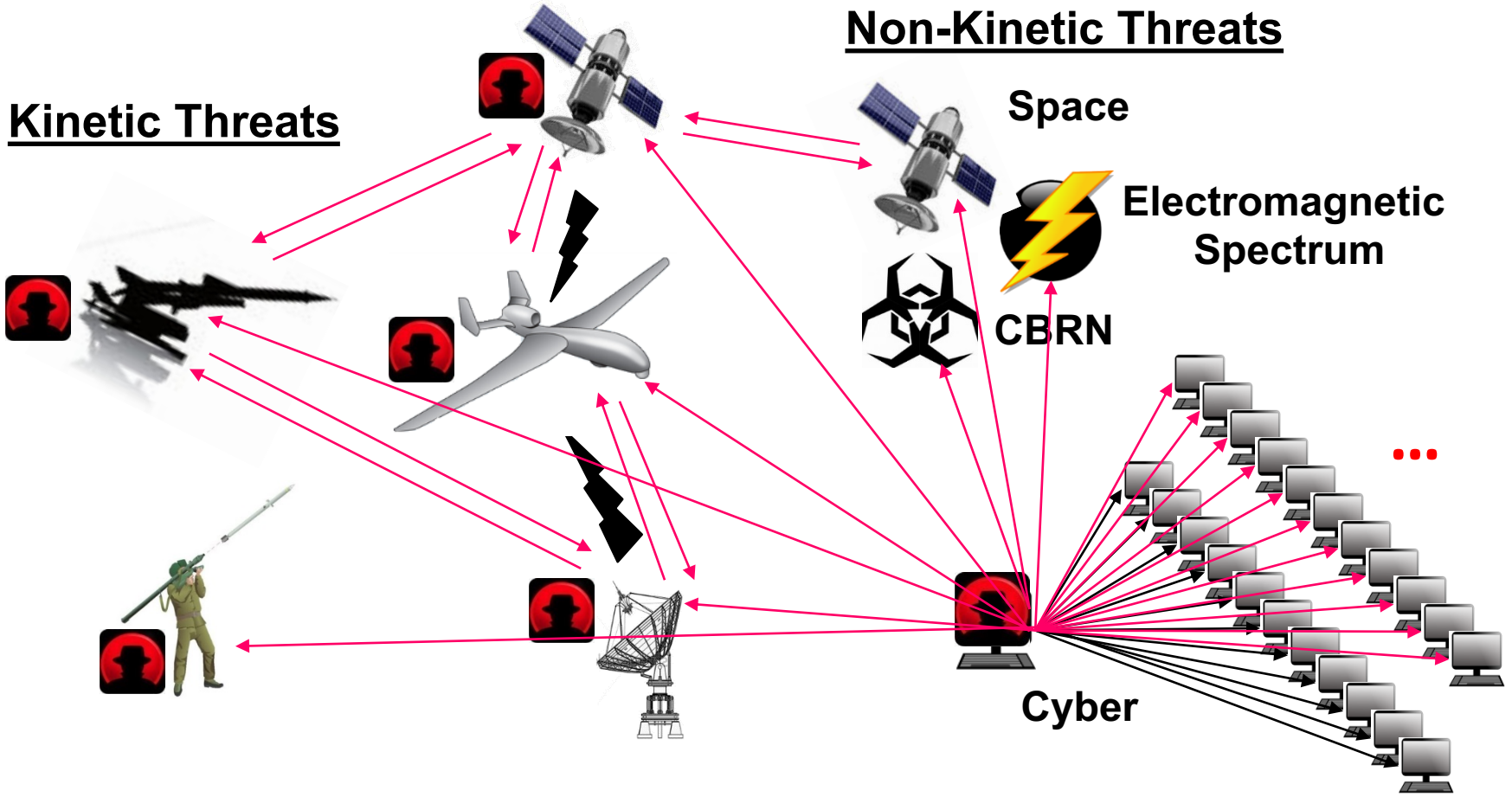
Non-Kinetic Threats



Paradigm Shift

1+ kinetic bullet → 1 kinetic kill … 1 cyber bullet → 1+++ kinetic kills, multi-path

SS-KPP & Cyber Survivability Endorsement



Paradigm Shift

1+ kinetic bullet → 1 kinetic kill … 1 cyber bullet → 1+++ kinetic kills, multi-path

Cyber Key Terrain Landscape: Examples

Organization	Information Technology (IT)	Operational Technology (OT)	Operational Platforms
Merck	IT/Network	Production Line	
Amazon	IT/Network/AWS	Processing Center	Planes
Shell/Exxon Mobil	IT/Network	Production Plant	Exploration Platforms/ Ships/Trucks
Maersk	IT/Network	Cargo Handling/Fuel Handling	Ships
UPS/FEDEX	IT/Network	Processing Center	Planes/Trucks
Airlines	IT/Network	Baggage Handling/Fuel Handling	Planes
DoD	IT/Network	Power/Fuel/Weapons Handling	Planes/Ships/Tanks/ Satellites

Impact of the "NotPetya" Cyber Attack

[Jun 2017] 'Fancy Bear' hackers release malware 'NotPetya' in Ukraine

- **"It was the equivalent of using a nuclear bomb to achieve a small tactical victory"**
- **"To date, it was the fastest propagating piece of malware we've ever seen" [Cisco]**
  - Within hours, the worm spread around the world and crippled numerous multinational companies
- **Total cost: $10B**
  - Merck: $870M; FedEx (TNT Express): $400M; Saint-Gobain: $384M; Maersk: $300M; Nabisco and Cadbury: $188M
- **Impact to Maersk operations of NotPetya Cyber Attack:**
  - Created chaos at 17 of 76 ports worldwide causing tens of thousands of shipping trucks to be turned away
  - Effectively took down entire global corporate network (4,000 servers, 45,000 PCs, etc.)
    - Simultaneously wiped out nearly all of the domain controller servers, which are needed to map its global network and set basic rules for access, except for one in Ghana (because of a local blackout which prevented NotPetya from spreading)

"Almost everyone who has studied NotPetya, however, agrees on one point: that it could happen again or even reoccur on a larger scale. Global corporations are simply too interconnected, information security too complex, attack surfaces too broad to protect against state-trained hackers bend on releasing the next world-shaking worm."

https://www.wired.com/story/notpetya-cyberattack-ukraine-russia-code-crashed-the-world/

Example - Cyber Risk: Impact to Maersk Business Operations from the 2017 "NotPetya" Cyber Attack

- Business Operations
- Platforms
- IT/Network/Applications
- Operational Technology
- Commercial Infrastructure

Impact to Operations: 20% drop in shipping volume – managed 80% percent of volume manually – with help from customers
Impact to Earnings: $200M - $300M

Business Applications Impacted: E-mail, invoicing, systems for sharing system rates, online track and trace, and customer support phone lines that transport and logistics operations depend on

IT Infrastructure Rebuild: 4000 new servers, 45,000 new PCs, 2,500 applications

Perspective of MAERSK CEO: "It is time to stop being naive when it comes to cybersecurity. I think many companies will be caught if they are naive. Even size doesn't help you."

How it Fits Together - Cyber Risk to Mission

DoD Missions

- **DoD Weapon Systems / Platforms**

  FY16 NDAA Section 1647

- **DoD IT and Networks**

- **DoD Critical Infrastructure**

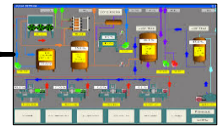
  FY17 NDAA Section 1650
  FY18 NDAA Section 1643

- **Commercial Critical Infrastructure**

- **Defense Industrial Base**

  DIB Cybersecurity
  Supply Chain Risk Management

Information Technology (IT)



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

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

Cyber Directorate Goals

- **Goal 1: Trained and Equipped Cyber Mission Force (CMF)**
  - Oversight of the acquisition of cyberspace operations capabilities for the CMF
  - Develop a cyber capability roadmap to guide development and acquisition of cyber capabilities
  - Improve acquisition policy for DoD cyber capabilities
- **Goal 2: DoD Forces are capable of operating in a cyber contested environment**
  - Understand the Cyber Vulnerabilities of DoD Platforms and Critical Infrastructure and Associated Risks to Operational Missions
  - Prioritize Mitigations at the Mission Level to enhance the capability for DoD forces to operate in a cyber contested environment

Understanding and enabling mitigation of cyber vulnerabilities in weapon systems and DoD facilities is a high priority

Cyber Vulnerability Assessment of DoD Weapon Systems: FY16 NDAA – Section 1647

- **By end of CY 2019, DoD was directed to:**
  - Evaluate the cyber vulnerabilities of each major weapon system
  - Build upon existing efforts regarding the identification and mitigation of cyber vulnerabilities of major weapon systems
  - Develop strategies for mitigating the risks of cyber vulnerabilities identified
  - Report status during quarterly cyber operations briefings
- **OUSD(A&S)/DASD (I&IPM) given primary responsibility for overseeing and coordinating responses to 1647 legislation**
- **FY19 Congressional Funding - $89.1M**

DoD response to Congress recognized need for effects validation in operational context (major and Joint exercises) to inform mission impact assessment

Perspectives

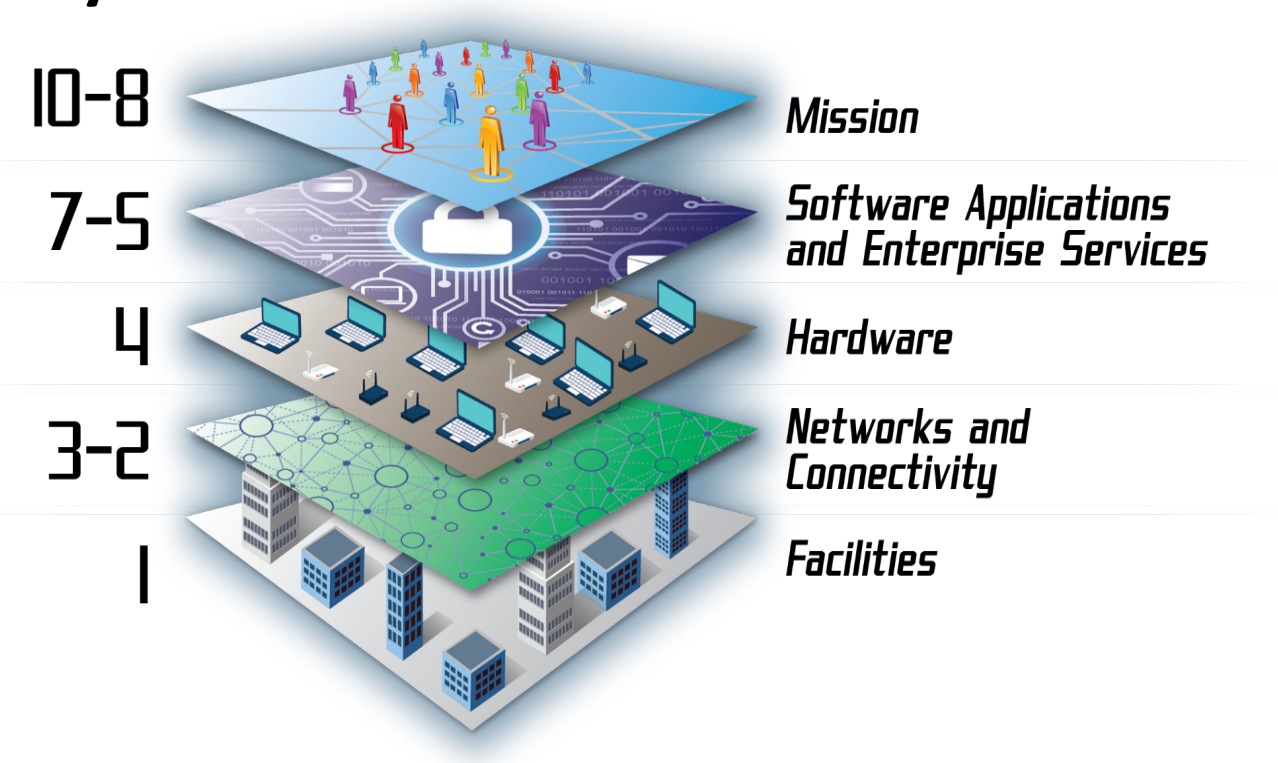
- "Cyber risk" means any risk of financial loss, disruption or damage to the reputation of an organization from some sort of failure of its information technology systems (Source: Institute of Risk Management).
- Cyber Event Risk = Probability of cyber event x consequence of cyber event.
- Probability of a cyber event is a function of:
  - Cyber actor capabilities
  - Cyber actor intent
  - Cyber vulnerabilities

Cyber Risk to Mission

- The "Cyber Risk to Mission" is risk to a DoD Mission associated with a Cyber Attack on DoD networks, platforms, operational technology (critical infrastructure) or supporting commercial infrastructure (e.g., power, communications).
- This risk can only be understood and countered by understanding the relationship between mission functions and the networks, platforms, operational technology, and commercial infrastructure that supports the mission.
- Cyber Risk to Mission varies by attack type/effect:
  - E.g., deceive, deny, disrupt, degrade, destroy.

Understanding Cyber Risk to Mission: Linking DoD Missions to Enabling Capabilities

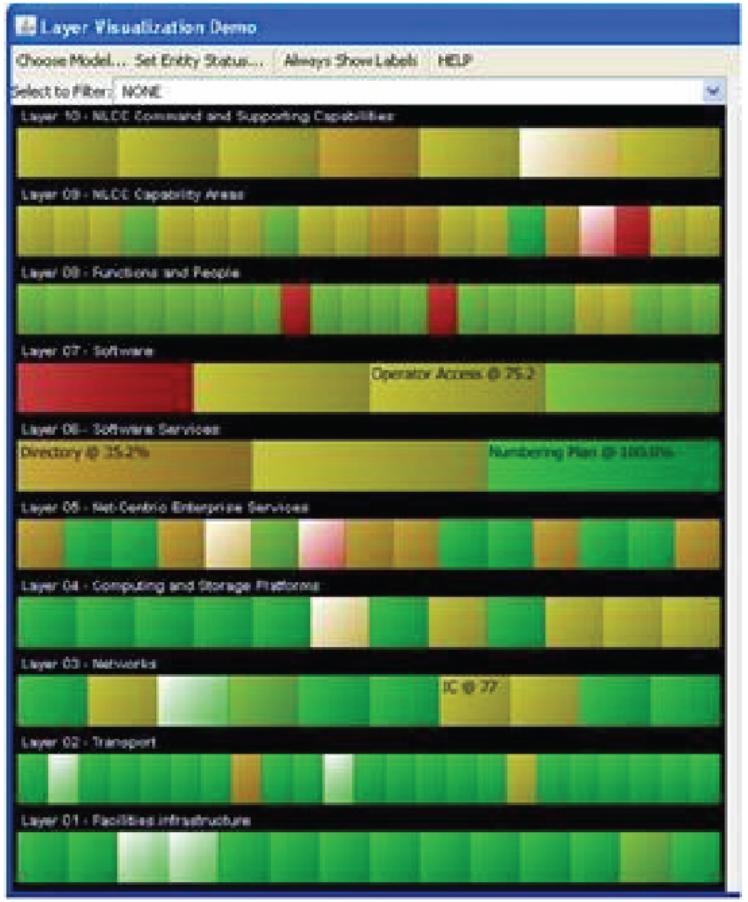
- Mission
- Mission System/Platform
- IT/Network
- Operational Technology
- Commercial Infrastructure



Understanding Cyber Risk to Mission: Application of Mission Mapping Methodology

Mission	Objectives & Imperatives Processes & Capabilities Functional Capabilities & People
Software Applications and Enterprise Services	Software Applications & Content Software Framework Services Enabling Software & Data Services
Hardware	Computing & Storage Platforms
Networks and Connectivity	Networks Connectivity
Facilities	Infrastructure / Facilities

INFORMATION LINKAGES
SECURITY LINKAGES
MANAGEMENT LINKAGES



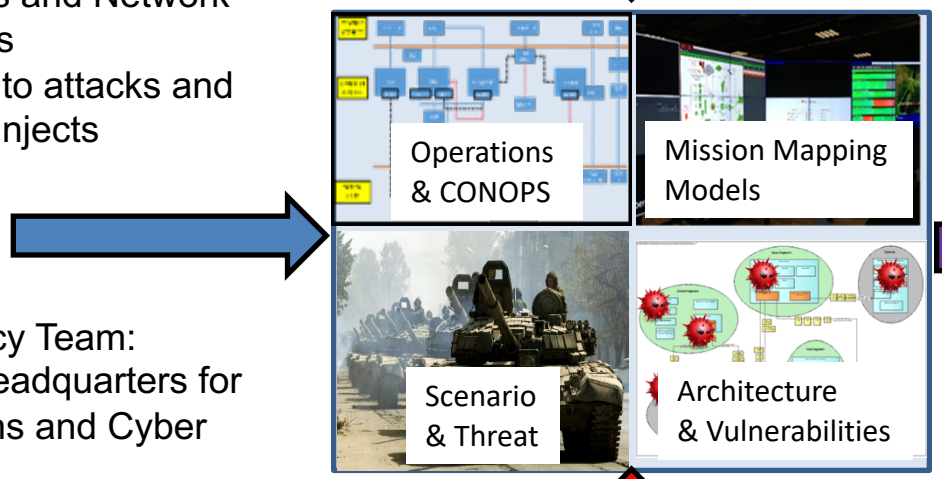
Cyber Risk to Mission being evaluated in DoD Cyber Resiliency Wargames and Cyber Resiliency Assessments

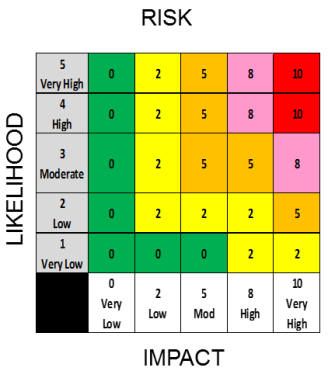
Cyber Resiliency Wargame Overview

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

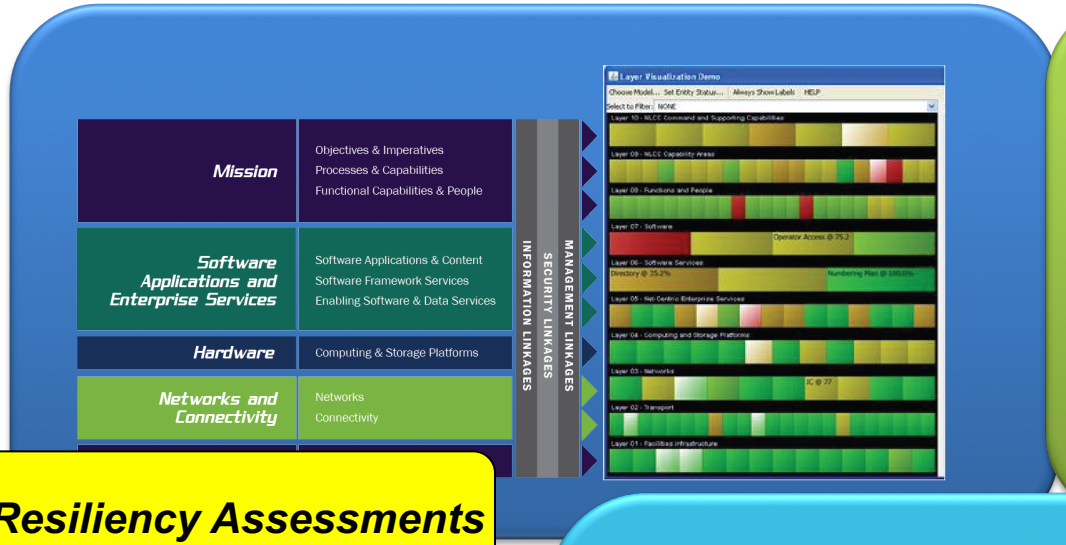




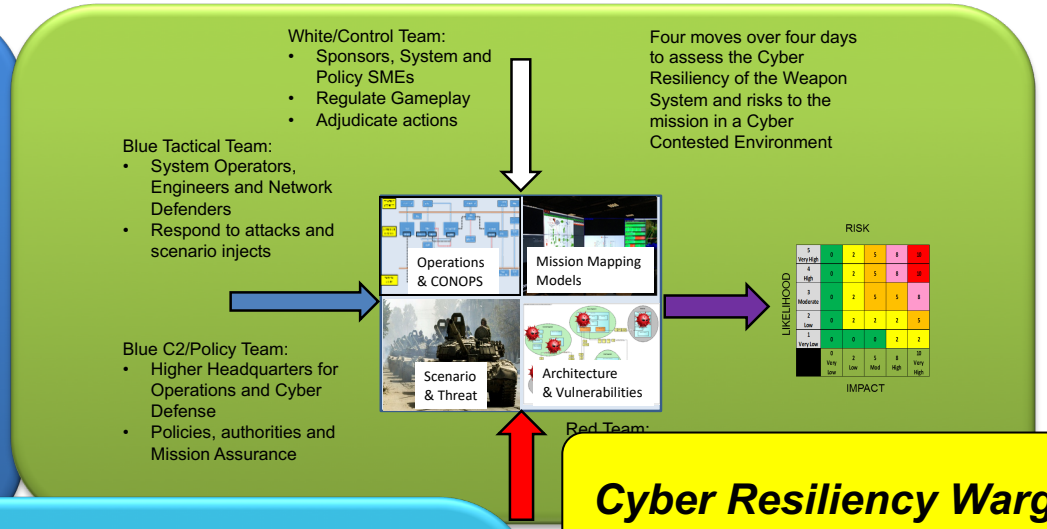
Blue C2/Policy Team:
- Higher Headquarters for Operations and Cyber Defense
- Policies, authorities and Mission Assurance

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

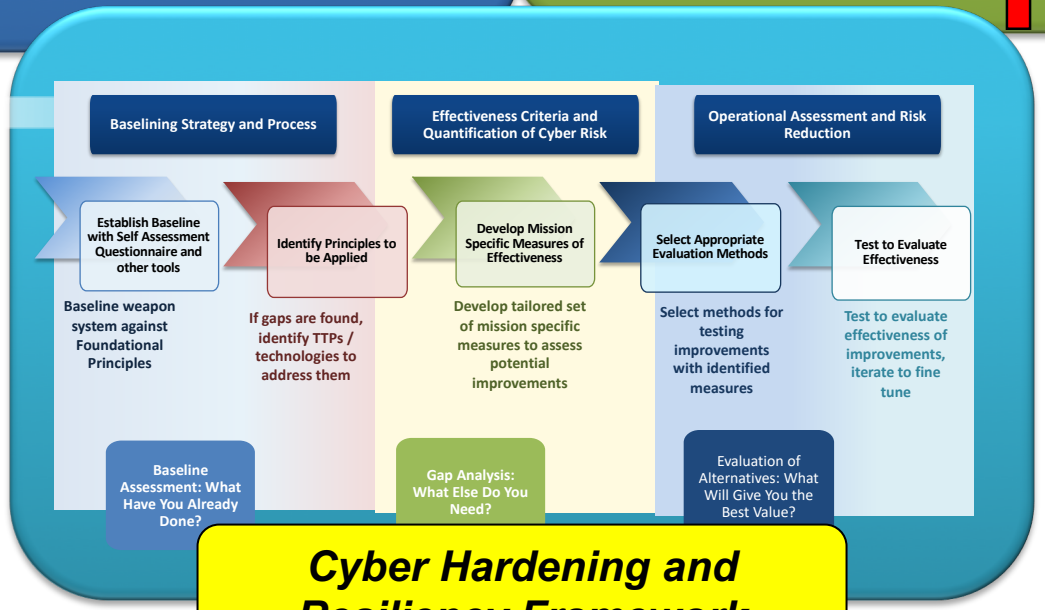
Understanding and Countering Cyber Risk to Mission Takes Ongoing Cooperative Efforts



Cyber Resiliency Assessments



Cyber Resiliency Wargaming



Cyber Hardening and Resiliency Framework

Summary

- Cyberspace is a ***Contested*** Operational Domain
- DoD Forces need to be able to operate in contested cyber environment
- Extensive cyber vulnerability assessments underway for DoD Weapon Systems and Critical Infrastructure
- Ongoing efforts to understand and counter cyber risks to critical DoD Missions
- Cyber Resilience is ***Not Optional***