Understanding Cyber Risk to Mission:

A Challenge for the C2 Research Community

Mr. John Garstka, SES
Director, Cyber
OUSD(A&S) I&IPM

Presented to 23rd ICCRTS
November 2018

Cyberspace is a Critical Enabler of Operations

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

Non-cyber forces dependent upon cyberspace

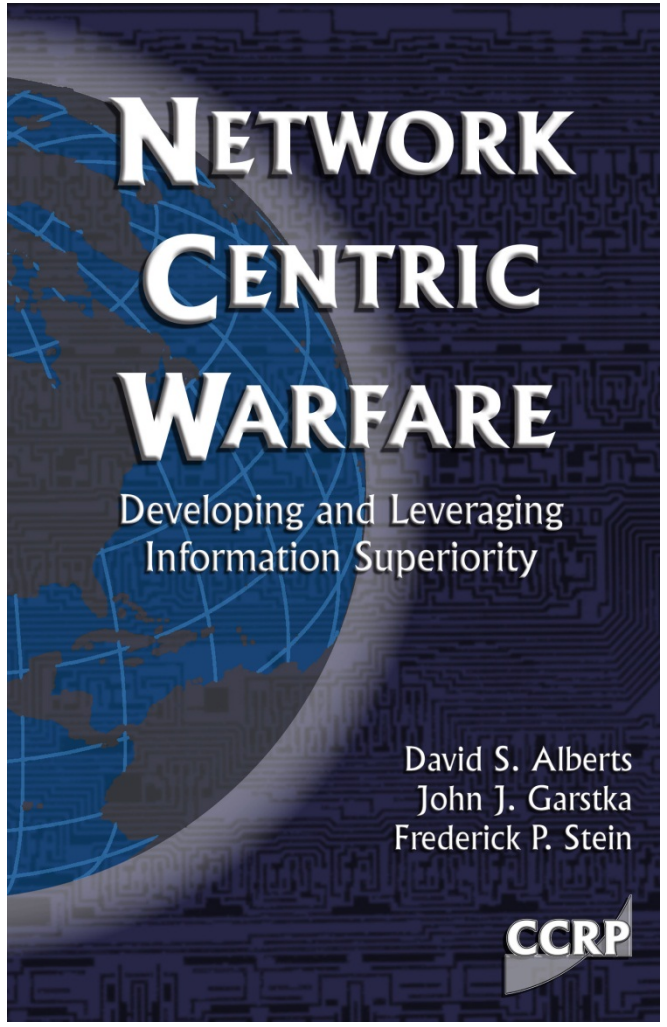
Cyber forces operating in cyberspace

DoD Cyberspace Missions

1. DoD must defend its own networks, systems, and information.
2. DoD must be prepared to defend the United States and its interests against cyberattacks of significant consequence.
3. If directed by the President or the Secretary of Defense, DoD must be able to provide integrated cyber capabilities to support military operations and contingency plans.

Source: DoD Cyber Strategy - April 2015

Cyber Capabilities Enable NCW



NCW was the answer to the question

“ What can I do with IT and networking to generate warfighting advantage?”

NCW Extended

A robustly networked force* → improves → Information Sharing

Information Sharing and Collaboration → enhances → Quality of Information and Shared Situational Awareness

Shared situational awareness → enables → Collaboration and Self-synchronization

These, in turn, dramatically increase mission effectiveness.

+

Cyber-Enabled

Tanks
Aircraft
Ships
Weapons
Sensors
Logistics
.
.
.

Have We Built / Are We Building “Battleships”?

You are never as invincible as you believe

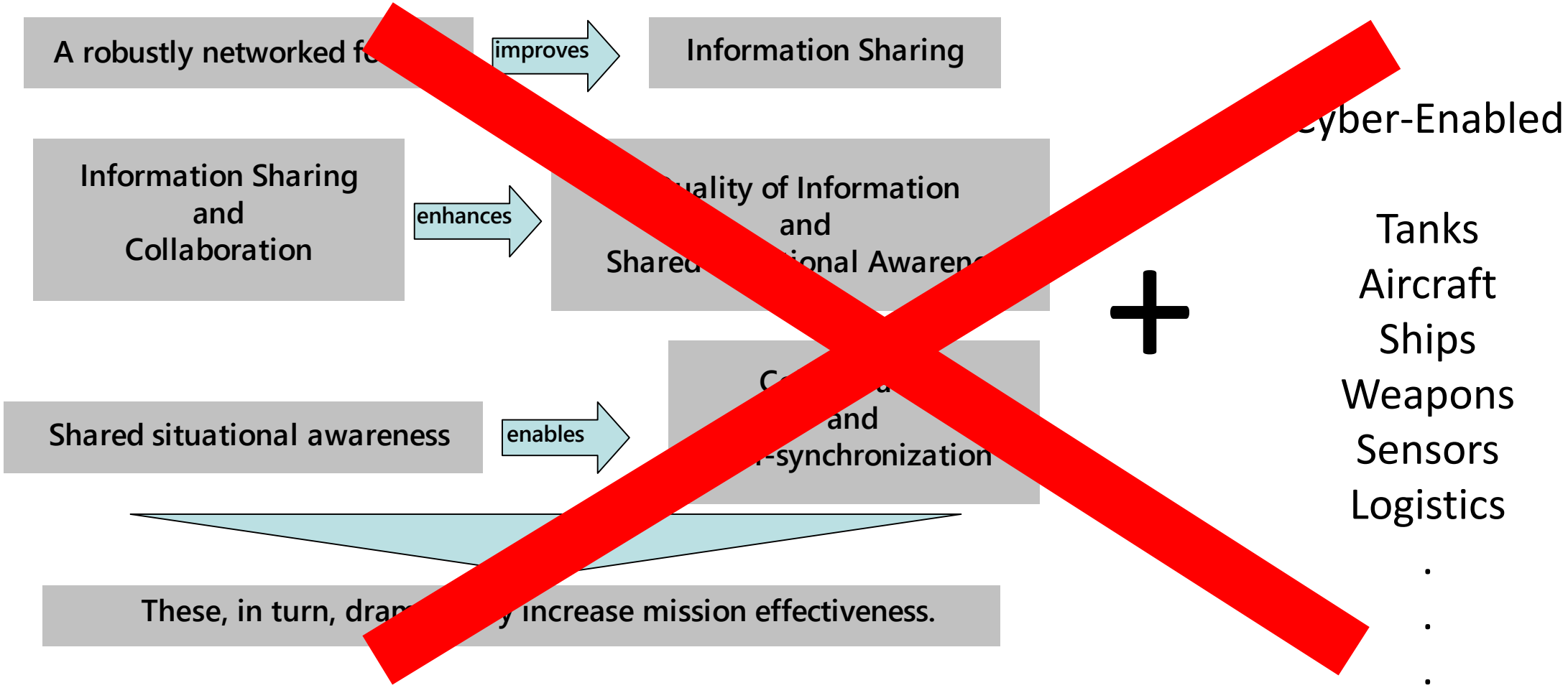
Ref: Army-Navy Football Game Program, Franklin Memorial Stadium, Philadelphia, Pennsylvania, November 29, 1941. Page 180. Navy defeated Army, 14-6.

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.

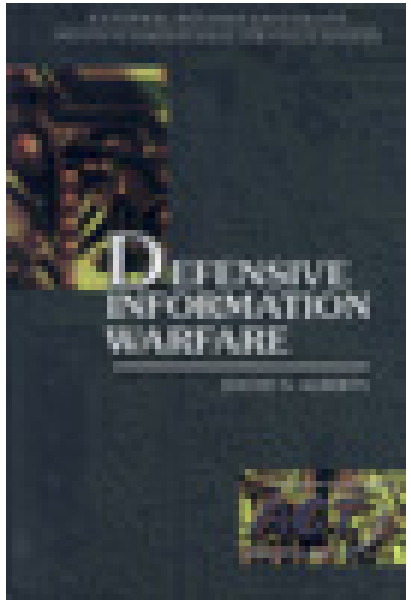
NCW Extended

The new "So What" Question



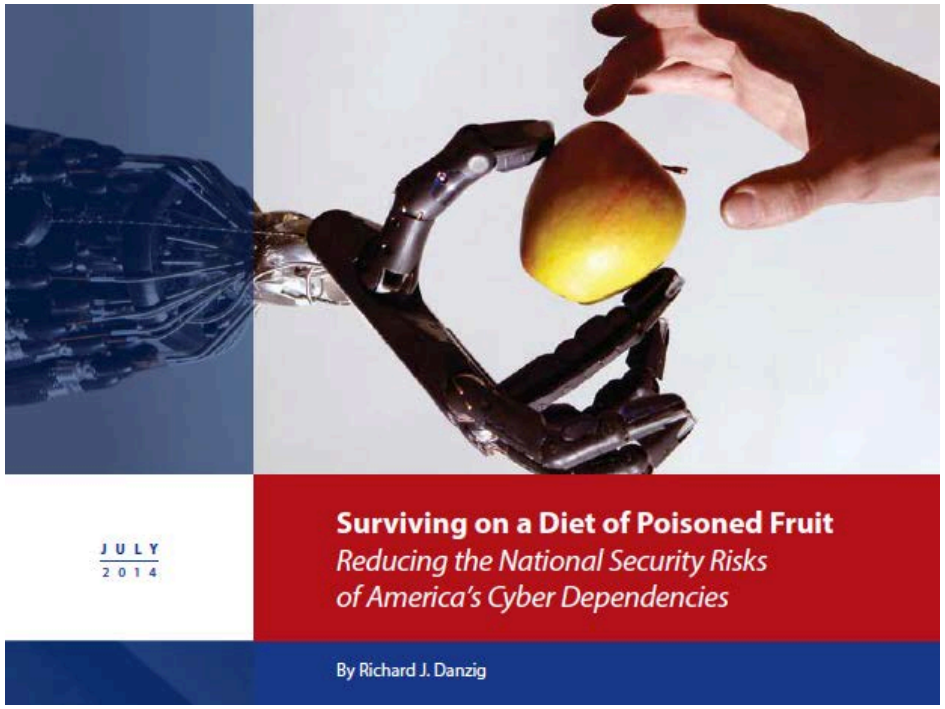
Dangers of Dependencies have been Recognized

1996



There is a growing consensus that national prosperity, if not survival, depends on our ability to effectively leverage information technology. Without being able to defend vital information, information processes, and information systems, such a strategy is doomed to failure.

2014



The risks of NCW are inherent in its opportunities. They cannot be eliminated; rather, they must be understood and managed.

Cyber Risk to Mission - How it Fits Together

Supply Chain Risk Management

DIB Cybersecurity

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**

Information Technology (IT)

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

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

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)/C3CB given primary responsibility for overseeing and coordinating responses to 1647 legislation**

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

Cyber Vulnerability Assessment of DoD Critical Infrastructure: FY17 NDAA – Section 1650

- **By end of CY 2020, DoD was directed to:**
  - **Evaluate the cyber vulnerabilities of DoD Critical Infrastructure**
  - **Build upon existing efforts regarding the identification and mitigation of cyber vulnerabilities of critical infrastructure**
  - **Develop strategies for mitigating the risks of cyber vulnerabilities identified**
  - **Report status during quarterly cyber operations briefings**
- **OUSD(A&S)/C3CB given primary responsibility for overseeing and coordinating responses to 1650 legislation**

DoD Plan Submitted to Congress – June 2018

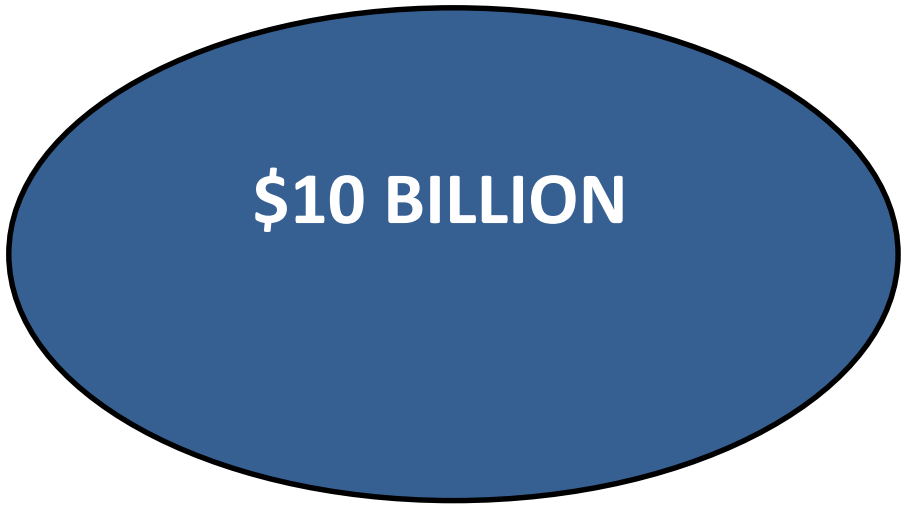
Dependency of Cyber Enabled Capabilities

Organization	Information Technology (IT)	Operational Technology (OT)	Operational Platforms
DOD	IT/Network	Power/Fuel/Weapons Handling	Planes/Ships/Tanks/ Satellites
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
Merck	IT/Network	Production Line	

Economic Impact of Cyber Attacks: NotPetya*

$870,000,000
Pharmaceutical company Merck

$400,000,000
Delivery company FedEx (European subsidiary TNT Express)



$384,000,000
French construction company Saint-Gobain

$300,000,000
Danish shipping company Maersk

$129,000,000
British manufacturer Reckitt Benckiser

$188,000,000
Snack company Mondelēz (parent company of Nabisco and Cadbury)

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

Example - Cyber Risk: Impact to Maersk Business Operations from 2017 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."

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**
  - **Enhance the capability for DoD forces to operate in a cyber contested environment**
- **Goal 3: Enhance Governance for DoD Cyber Investments**
  - Improve capabilities and data for analysis and oversight

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

Cyber Risk to Mission

- **Cyber Risk to System = probability of cyber event x system or information consequences**
- **Cyber Risk to Mission = probability of cyber event x mission consequences**
- **Probability of a cyber event is a function of**

  - Cyber vulnerabilities
  - Cyber dependencies
  - Cyber actor intent
  - Cyber actor capabilities
  - Cyber Agility

- **Probability that a cyber event will cascade and have an adverse impact on mission performance is a function of**

  - Severity of the damage
  - Time to restore capability
  - Mission system dependencies
  - Force Agility

- **Agility is a function of responsiveness, flexibility, versatility, resilience, adaptability, innovativeness**

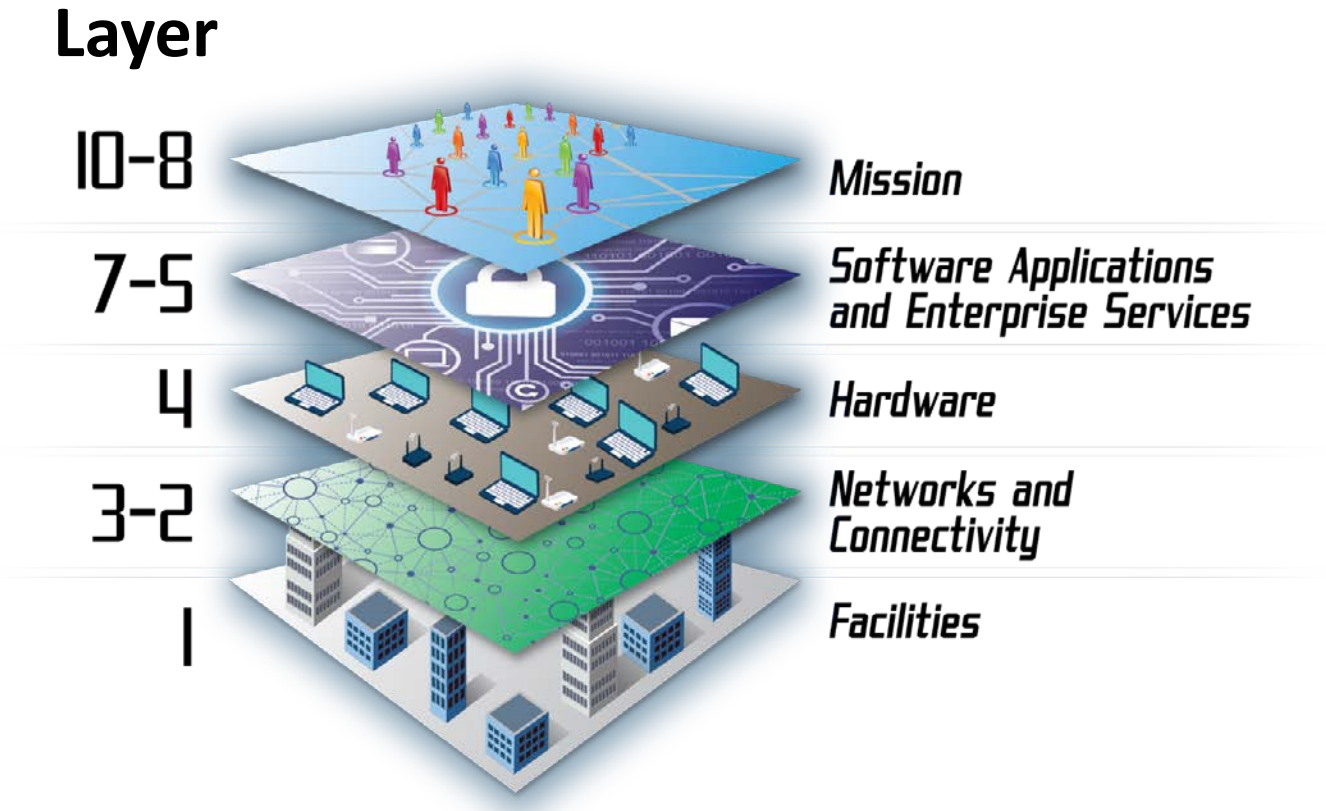
Understanding Cyber Risk to Mission

- There is potential Cyber Risk to Mission associated with a direct attack on DoD networks, platforms, operational technology (critical infrastructure) or supporting commercial infrastructure (e.g., power, communications) or with the collateral damage from a attack on someone else

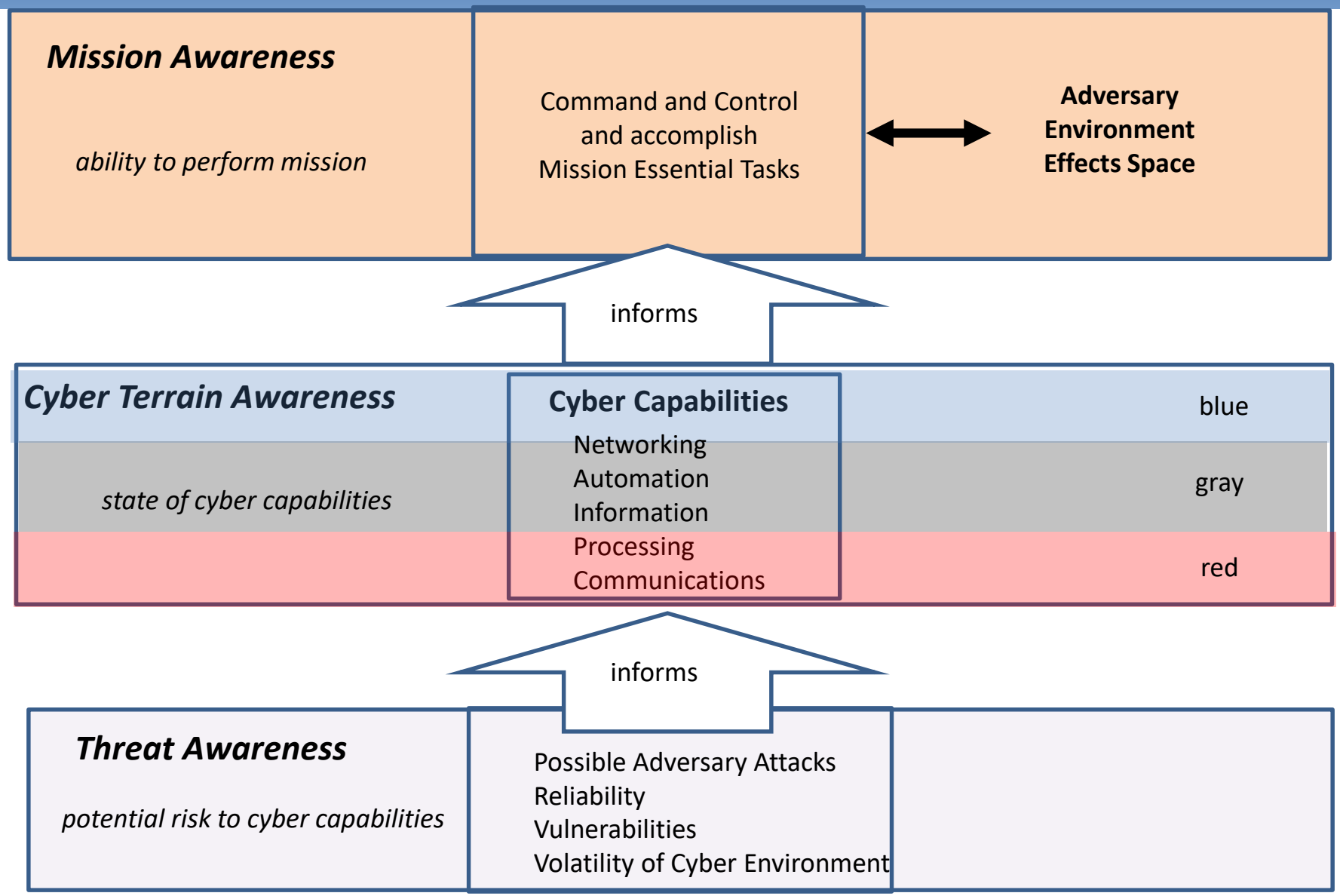
- This risk can only be understood by understanding the relationship between the capabilities that networks, platforms, operational technology, and commercial infrastructure provide and mission processes and tasks.

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

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



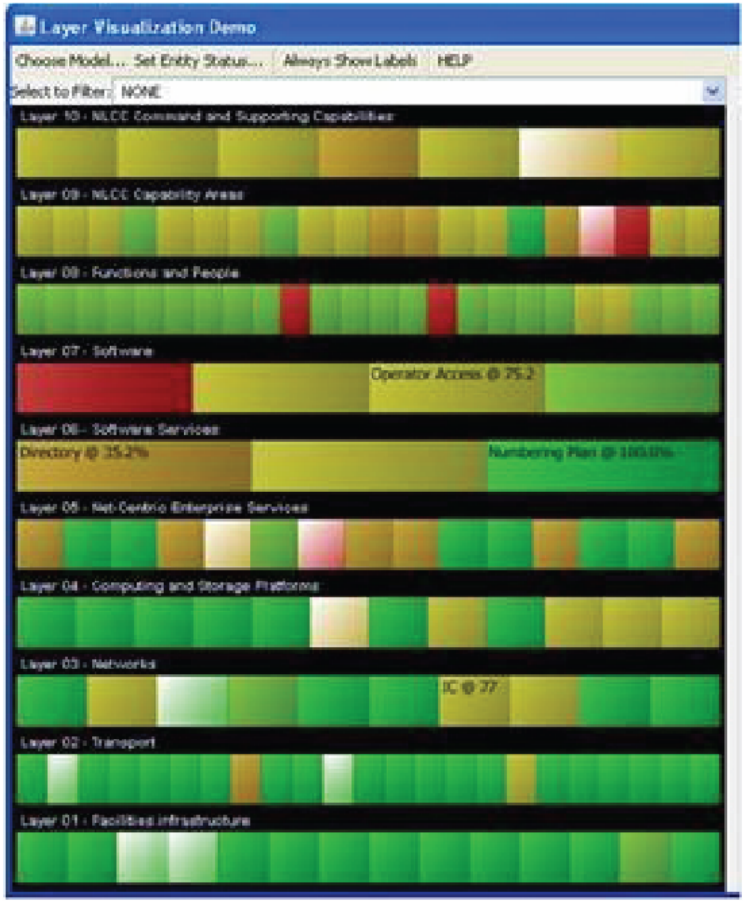
Understanding CRM



Understanding Cyber Risk to Mission: Application of Mission Mapping Methodology

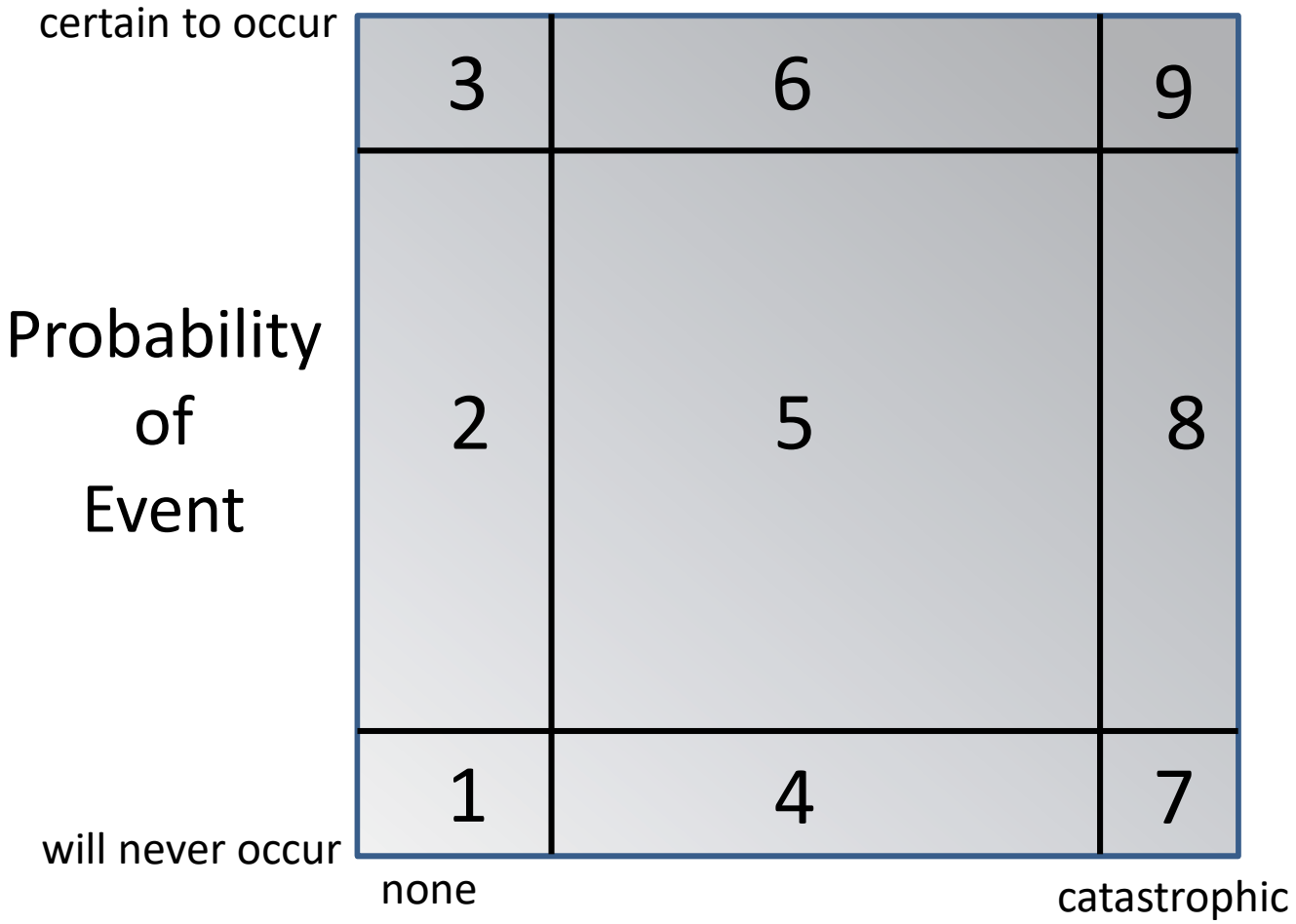
Mission	Objectives & Imperatives Processes & Capabilities Functional Capabilities & People
Software Applications and Enterprise Services	Software Applications & Content Software Framework Services Enabling Software & Data Services
Hardware	Computing & Storage Platforms
Networks and Connectivity	Networks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

INFORMATION LINKAGES
SECURITY LINKAGES
MANAGEMENT LINKAGES



Cyber Risk to Mission being explored in DoD Cyber Resiliency Wargames

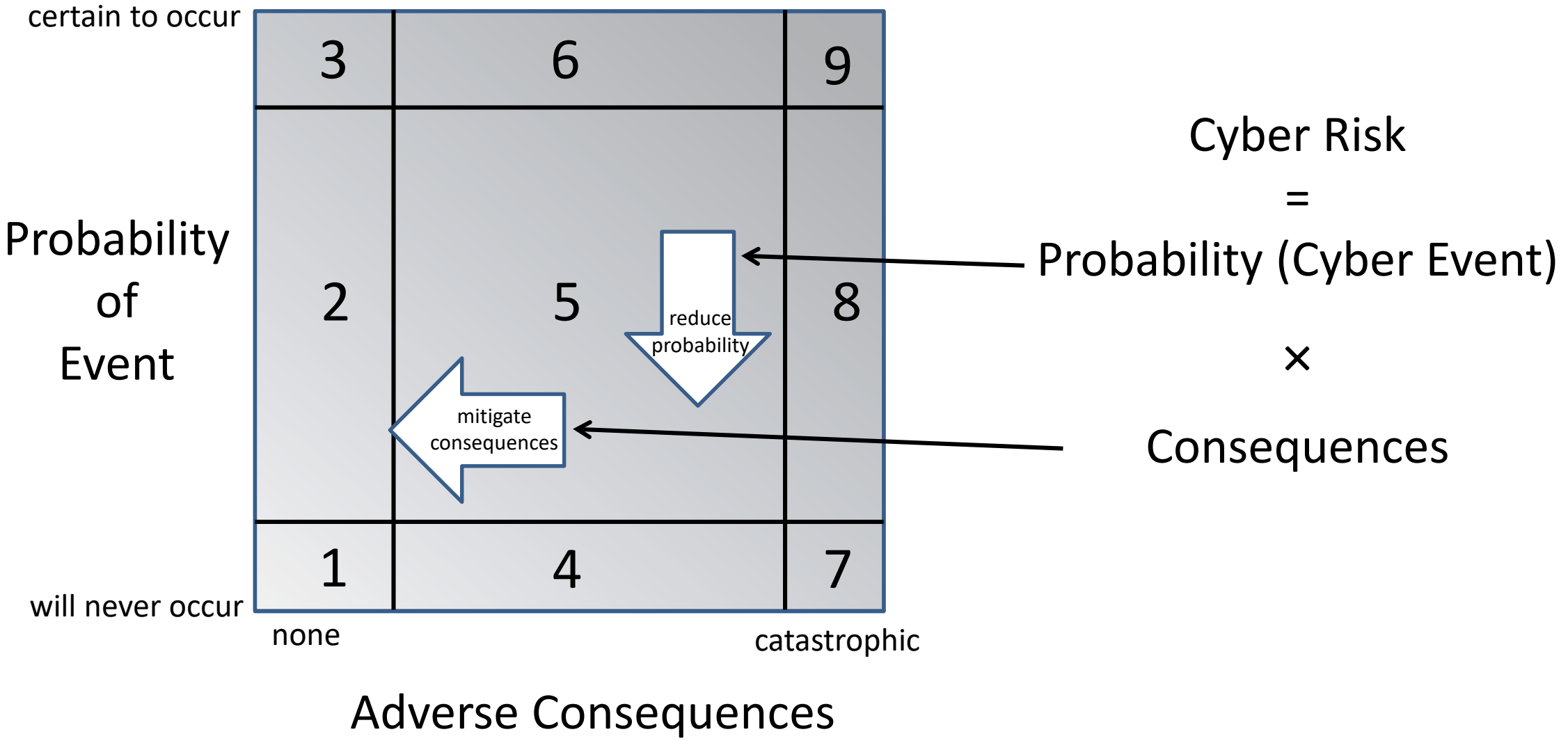
Managing Cyber Risk



Cyber Risk
=
Probability (Cyber Event)
×
Consequences

Alberts, D. S, (2011) The Agility Advantage.

Managing Cyber Risk



Summary

- **Maintaining the benefits of NCW+ in a contested cyber environment requires**
  - Cyberspace is a Contested Operational Domain
  - Today's Mission Capabilities are Cyber-Enabled
  - Understanding of Cyber Risk to Mission
  - Agility to minimize and/or mitigate this risk
- **Steps to allow DOD to operate in a cyber contested environment**
  - Improve risk posture of new and existing systems
  - Mitigate cyber event consequences in real time
  - Conduct cyber vulnerability assessments of Weapon Systems & Critical Infrastructure
  - Secure the Defense Industrial Base

Managing Cyber Risk to Mission is NOT Optional