Cyberspace as the 5th Domain of Conflict

Mr. John Garstka, Director Cyber Warfare

Office of the DASD for Platform and
Weapon Portfolio Management

OUSD Acquisition and Sustainment

October 24, 2024

Cybersecurity as an Element of National Security

(U) National Cybersecurity Strategy

- (U) “Defending the systems and assets that constitute our critical infrastructure is vital to our national security, public safety, and economic prosperity. The American people must have confidence in the availability and resilience of this infrastructure and the essential services it provides”
- (U) “Software and systems are growing more complex, providing value to companies and consumers but also increasing our collective insecurity. Too often, we are layering new functionality and technology onto already intricate and brittle systems at the expense of security and resilience”

FIGURE IS UNCLASSIFIED

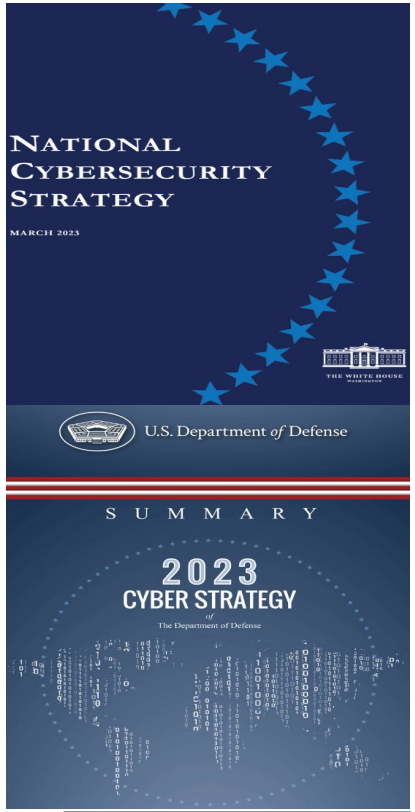


FIGURE IS UNCLASSIFIED

(U) Summary of the DoD Cyber Strategy

- (U) “The Department will enhance the cyber resilience of the Joint Force and ensure its ability to fight in and through contested and congested cyberspace.”
- (U) “As cyber threats grow and intensify, every soldier, sailor, airman, marine, guardian, coast guardsman, DoD civilian, and contractor is responsible for exercising cyber awareness and helping to manage the risk of the Department.”
- (U) “The United States is challenged by malicious cyber actors who seek to exploit our technological vulnerabilities and undermine our military's competitive edge. They target our critical infrastructure and endanger the American people.”

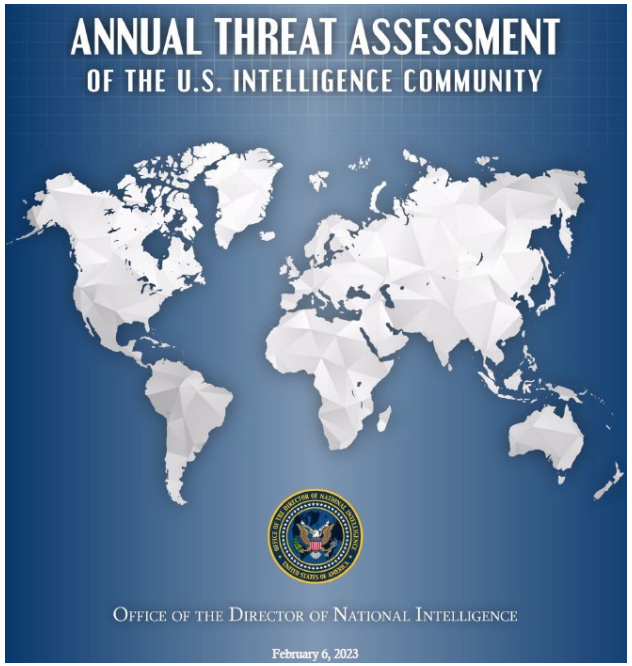
(U) “Defending the nation is paramount among our missions. It means defending our military systems, networks and the critical infrastructure that enable national security”
–(U) GEN Paul Nakasone, Commander, USCYBERCOM 2023 Posture Statement

The Cyber Threat is a Clear and Present Danger (1 of 2)

(U) People's Republic of China

- (U) "Counterspace operations will be integral to potential PLA military campaigns…intended to target U.S. and allied satellites."
- (U) "The PLA will continue to integrate space services…and satellite communications into its weapons and command-and-control systems in an effort to erode the U.S. military's information advantage."
- (U) "If Beijing feared that a major conflict with the United States were imminent, it almost certainly would consider **undertaking aggressive cyber operations against U.S. homeland critical infrastructure and military assets worldwide**."

FIGURE IS UNCLASSIFIED



Source: www.dni.gov

FIGURE IS UNCLASSIFIED

(U) Russia

- (U) "Russia continues to train its military space elements, and field new antisatellite weapons to disrupt and degrade U.S. and allied space capabilities."
- (U) "Russia will remain a top cyber threat as it refines and employs its espionage, influence, and attack capabilities. Russia views cyber disruptions as a foreign policy lever to shape other countries' decisions."
- (U) "Russia is particularly focused on improving its ability to target critical infrastructure…because compromising such infrastructure improves and demonstrates **its ability to damage infrastructure during a crisis**."

The Cyber Threat is a Clear and Present Danger (2 of 2)

Recent Cyber Attacks on US Infrastructure Underscore Vulnerability of Critical US Systems, November 2023–April 2024

CTIIC | JUNE 2024

Iran-affiliated and pro-Russia cyber actors gained access to and in some cases have manipulated critical US industrial control systems (ICS) in the food and agriculture, healthcare, and water and wastewater sectors in late 2023 and 2024. These attacks highlight a potential public safety threat and an avenue for malicious cyber actors to cause physical damage and deny critical services. Outdated software, poor password security, the use of default credentials, and limited resources for system updates render ICS devices vulnerable to compromise, as they are commonly connected to corporate IT networks and increasingly to the Internet. Many operators face numerous competing priorities, such as physical facilities operations and maintenance, which further constrains the time and resources that operators can dedicate to cybersecurity practices. Furthermore, the limited number of ICS vendors, wide availability of product configurations, and operational commonalities across the water sector make it easier for cyber actors to compromise vulnerable systems.

IRGC-affiliated "Cyber Av3ngers" compromise Unitronics programmable logic controllers (PLCs)

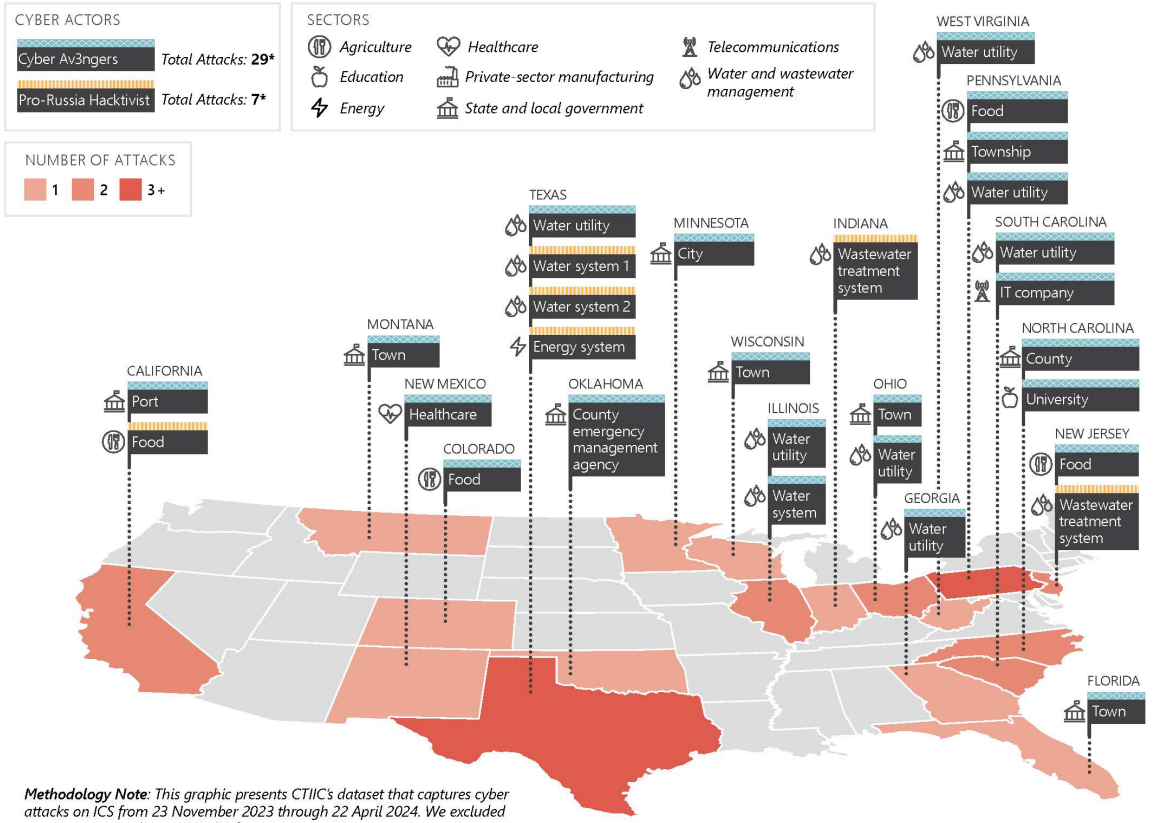
In November 2023, IRGC-affiliated actors operating under the Cyber Av3ngers persona gained access to the Israeli-made Unitronics Series ICS PLCs in multiple US entities, mostly water and wastewater systems, and defaced the PLCs' touch screens with an anti-Israel message. In response to the defacement, a few of the water-sector victims briefly shut down their systems and switched to manual operations.

Pro-Russia hacktivist compromised several water plants and claimed to compromise two dairies

A pro-Russia hacktivist remotely manipulated control systems within five water and wastewater systems and two dairies. The actors have typically accessed the ICS components via control interfaces with public-facing IP addresses.

- On 20 and 24 April 2024, the group posted videos showing an attacker remotely manipulating settings on human-machine interfaces (HMIs) within two US wastewater systems and one purported US energy company.
- On 18 January 2024, the group accessed control systems at two Texas water facilities and tampered with their water pumps and alarms, causing water to run past designated shutoff levels and overfill storage tanks.
- On 23 and 27 November 2023, the group also claimed on its public Telegram channel that it had attacked two US dairy systems.

REPORTED CYBER ATTACKS ON US ICS, 23 NOVEMBER 2023 THROUGH 22 APRIL 2024



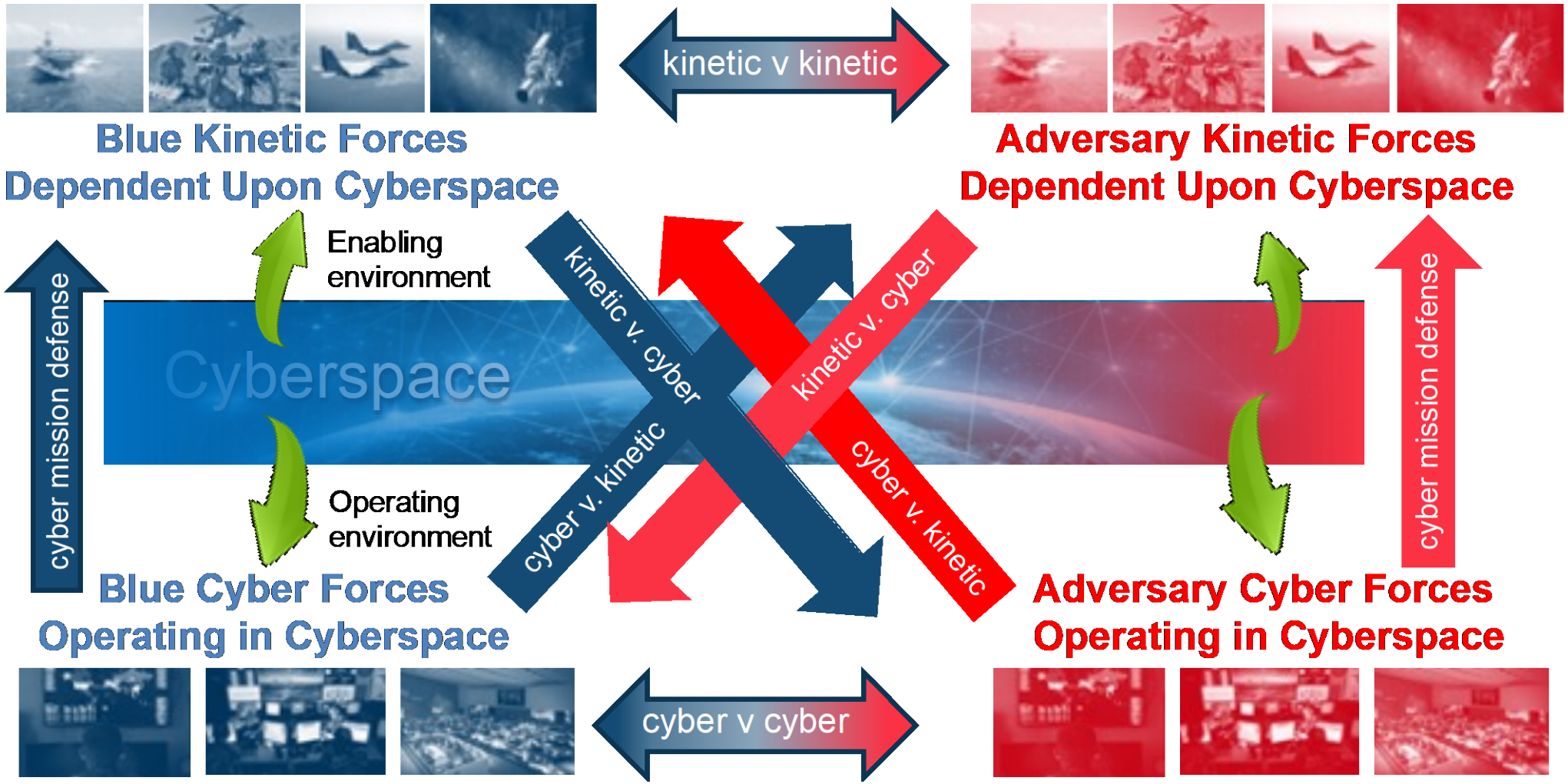
***Methodology Note**: This graphic presents CTIIC's dataset that captures cyber attacks on ICS from 23 November 2023 through 22 April 2024. We excluded ransomware attacks on critical infrastructure entities.*

*Including seven attacks at additional US locations.

Office of the Director of National Intelligence

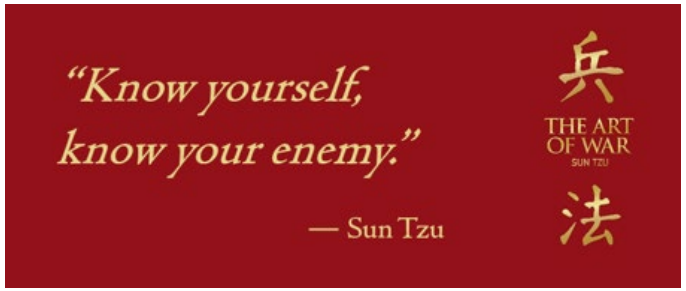
https://www.dni.gov/files/CTIIC/documents/products/Recent_Cyber_Attacks_on_US_Infrastructure_Underscore_Vulnerability_of_Critical_US_Systems-June2024.pdf

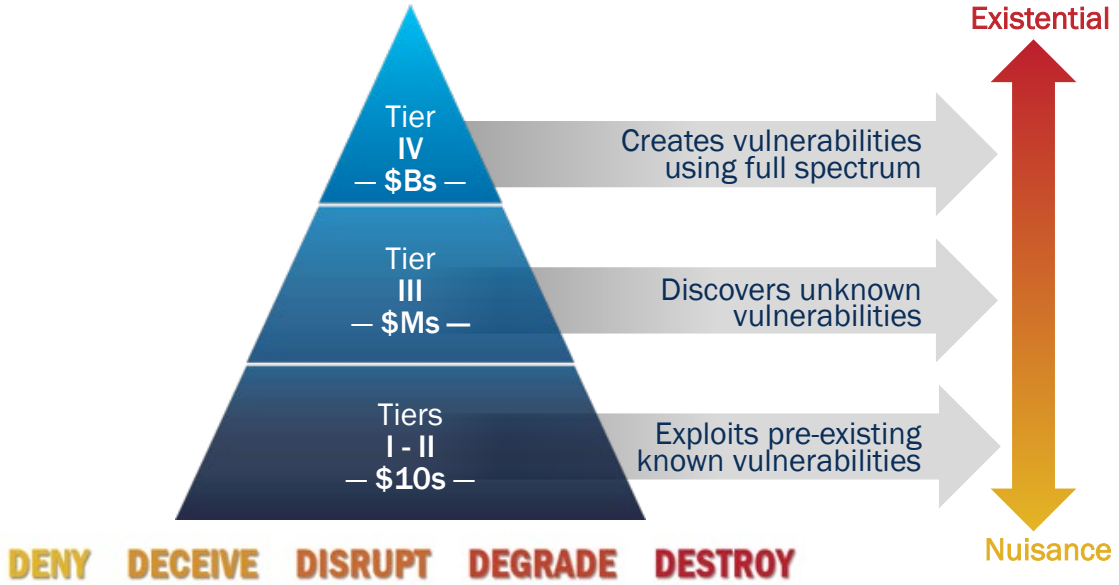
Cyberspace is a Warfighting Domain



Cyberspace is a Contested Operational Domain

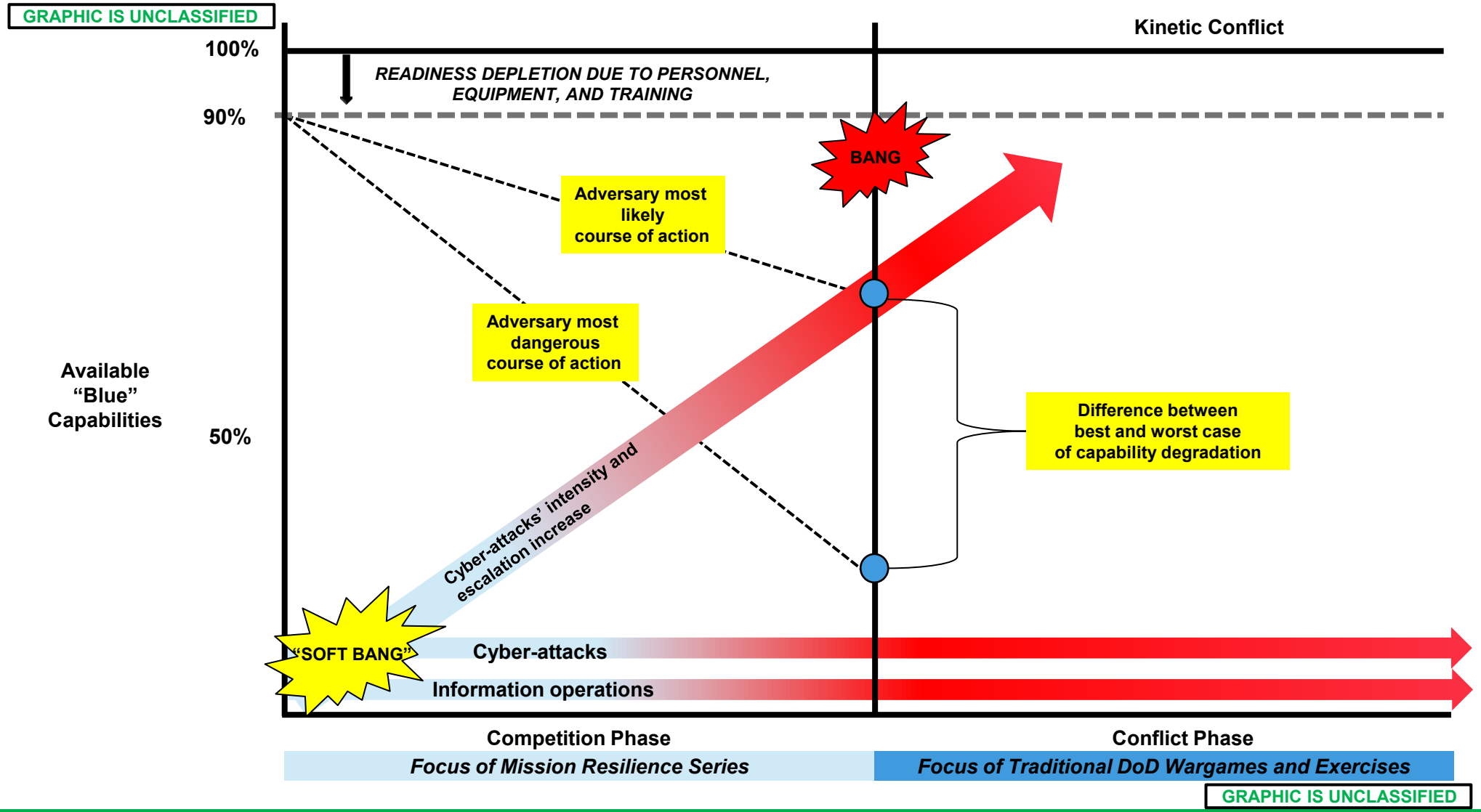
Tier	Description
IV	**Advanced** – Have the capacity to conduct complex, long term cyber attack operations that combine multiple intelligence disciplines to obtain access to high-value networks
III	**Moderate** – Able to use customized malware with OPSEC practices to conduct wider-range intelligence 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 publicly available tools.
I	**Nascent** – Little to no organized cyber capabilities, with no knowledge of a networks underlying systems or industry beyond publicly connected open-source information.





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

Cyber-Attack Degradation Prior to the Initiation of Armed Conflict



Parallels in Historical and Modern Capital Asset Development

GRAPHIC IS UNCLASSIFIED

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

You are never as invincible as you believe.

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.

GRAPHIC IS UNCLASSIFIED

The majority of operational DoD weapon systems were conceived and developed prior to the evolution of current cyber threats. The DoD must ensure its weapon systems do not become the "battleships" of the 21st century.

Parallels in Historical and Modern Capital Asset Development

GRAPHIC IS UNCLASSIFIED

March 1914
Construction commences

October 1916
Commissioned at Brooklyn Yard

1929
Major modernization completed, anti-air and torpedo defenses added

1940
Significant upgrades completed

December 7, 1941
USS Arizona sunk

1914 1915 1916 1917 1918 1919 1920 1921 1922 1923 1924 1925 1926 1927 1928 1929 1930 1931 1932 1933 1934 1935 1936 1937 1938 1939 1940 1941

27 Years between program development and when USS Arizona was sunk

Risk to Surface Combatants From Air Threats

RAF bi-planes destroy 3 Italian Surface Warships

Bi-planes capable with early bombs and entered into service

December 7, 1941
USS Arizona sunk in Pearl Harbor

1914 1915 1916 1917 1918 1919 1920 1921 1922 1923 1924 1925 1926 1927 1928 1929 1930 1931 1932 1933 1934 1935 1936 1937 1938 1939 1940 1941

GRAPHIC IS UNCLASSIFIED

Parallels in Historical and Modern Capital Asset Development

1981
Program Initiated

1993
Program Developed

1994
DFS-1 Launch

2010
27 years after program developed

1981 1982 1983 1984 1985 1986 1987 1988 1989 1990 1991 1992 1993 1994 1995 1996 1997 1998 1999 2000 2001 2002 2003 2004 2005 2006 2007 2008 2009 2010 2011 2012 2013 2014 2015 2016 2017 2018 2019 2020 2021 2022

$5 billion spent

Increasing capability of malicious cyber actors

The PRC and Russia…are already using non-kinetic means against our defense industrial base and mobilization systems, as well as deploying counterspace capabilities that can target our Global Positioning System and other space-based capabilities that support military power and daily civilian life

2022 National Defense Strategy

NASA Satellites targeted

Yahoo account compromises

NotPetya ransomware attacks

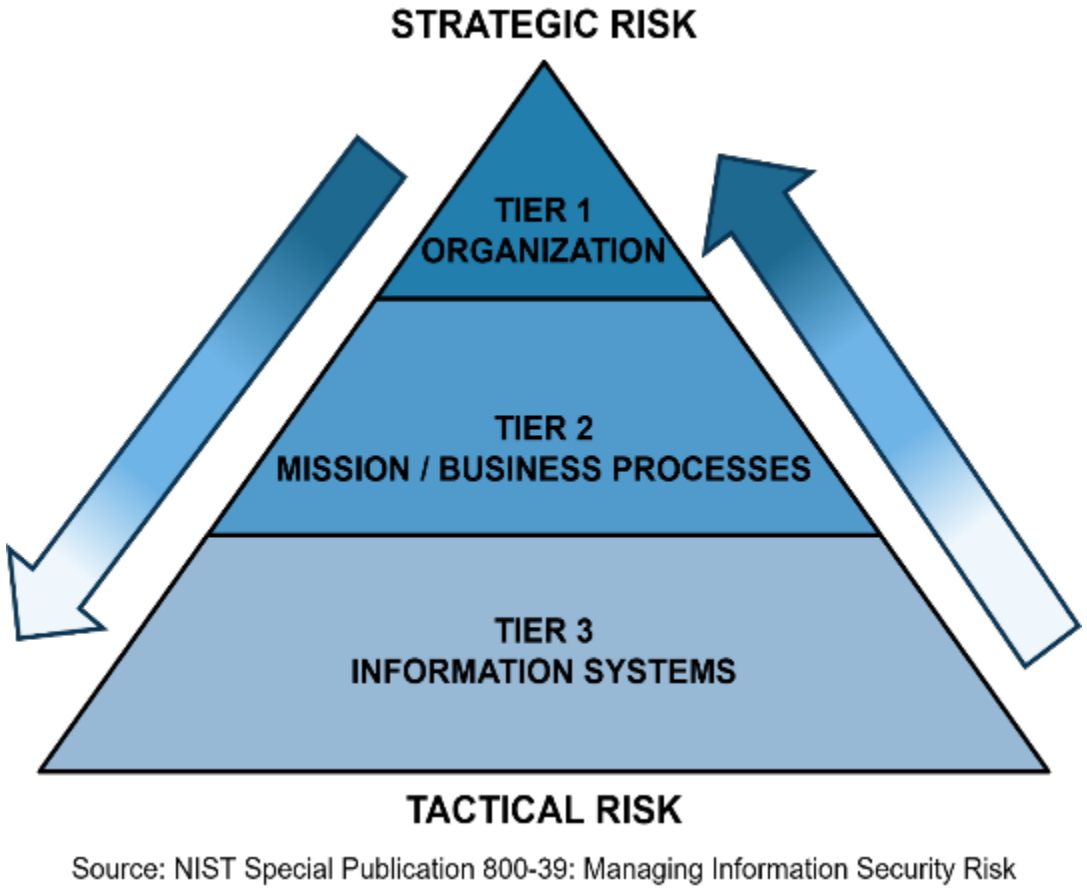
Colonial Pipeline attacks

1981 1982 1983 1984 1985 1986 1987 1988 1989 1990 1991 1992 1993 1994 1995 1996 1997 1998 1999 2000 2001 2002 2003 2004 2005 2006 2007 2008 2009 2010 2011 2012 2013 2014 2015 2016 2017 2018 2019 2020 2021 2022

GRAPHIC IS UNCLASSIFIED

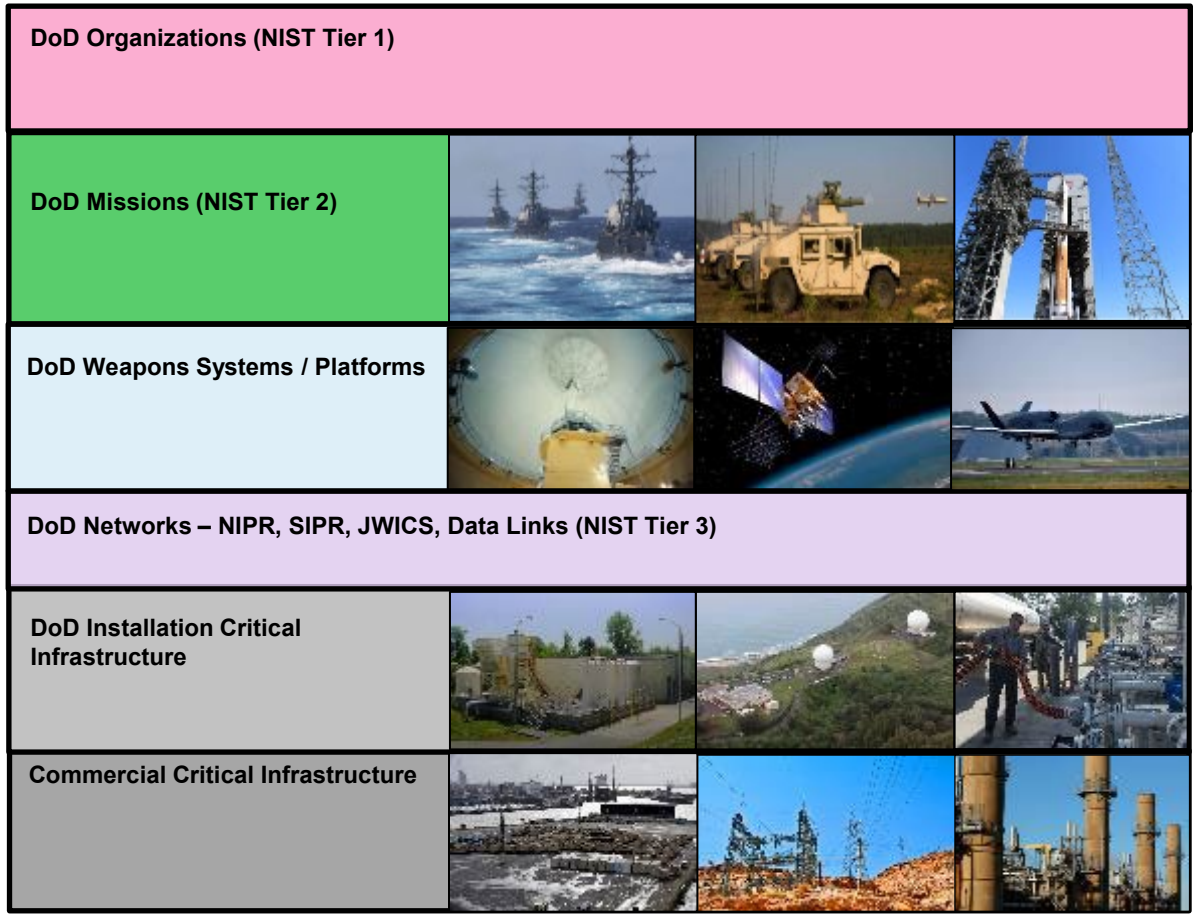
Assessing Cyber Risk to Mission

GRAPHIC IS UNCLASSIFIED



Source: NIST Special Publication 800-39: Managing Information Security Risk

THE MISSION STACK



GRAPHIC IS UNCLASSIFIED

Notional Weapon System

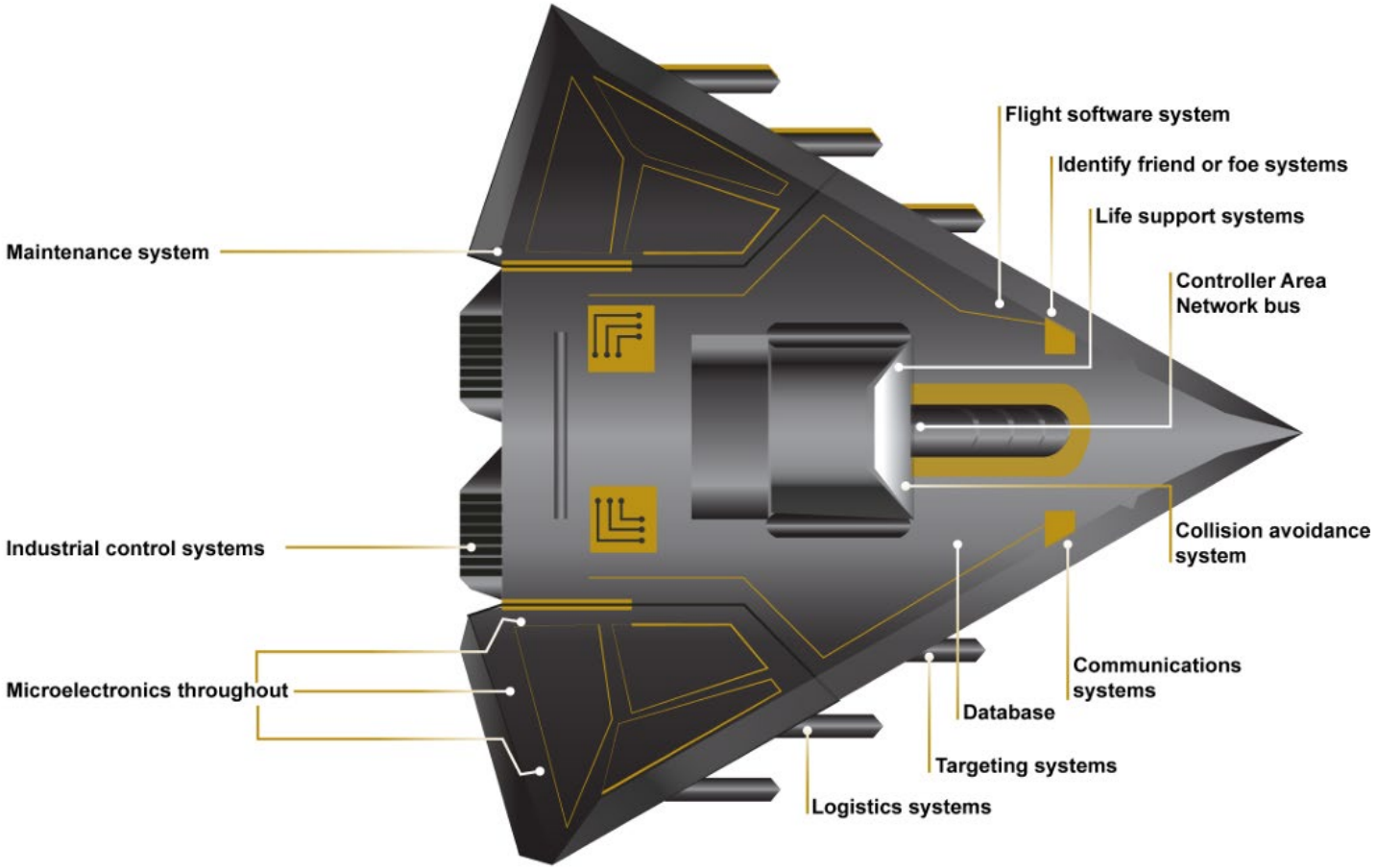


FIGURE IS UNCLASSIFIED

Reference: GAO-19-128

Installation Critical Infrastructure (SV-1)

FIGURE IS UNCLASSIFIED

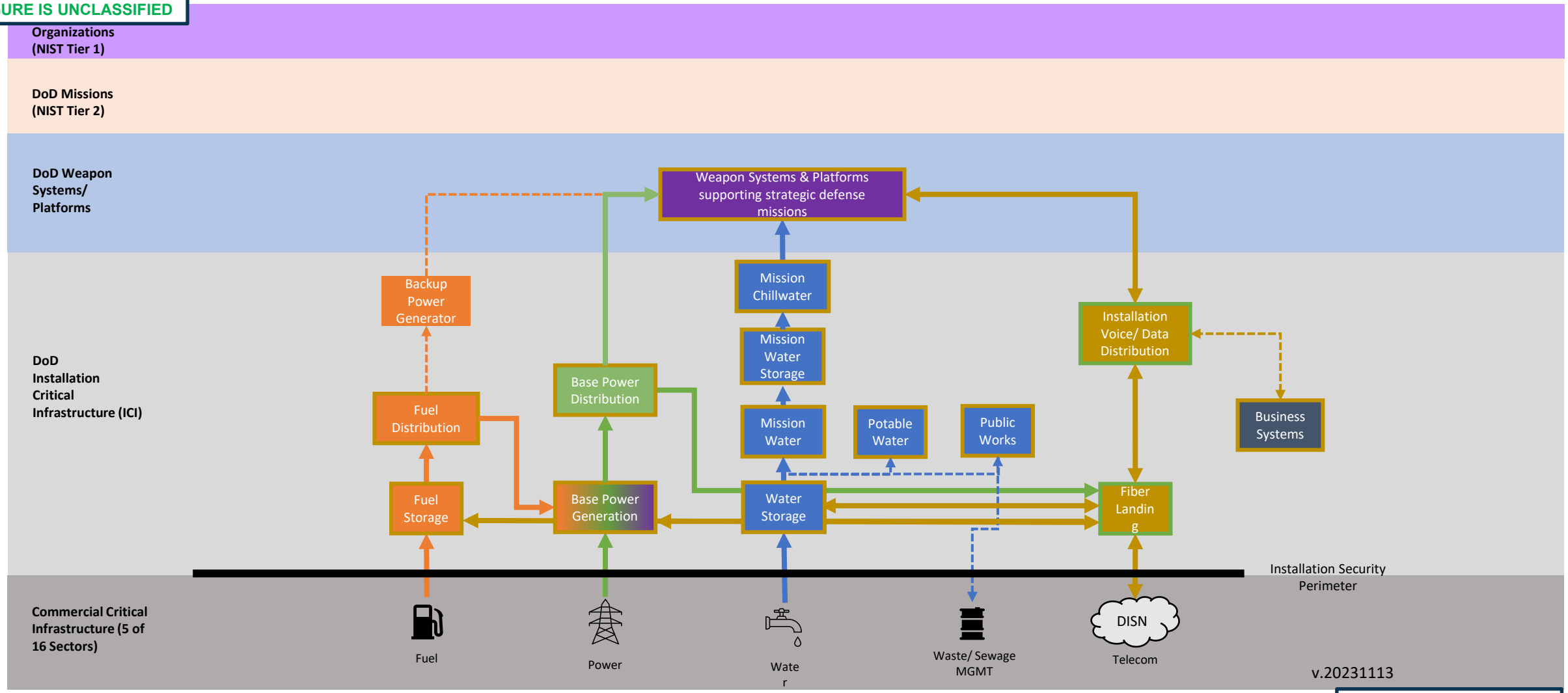


FIGURE IS UNCLASSIFIED

OT Support of the Mission Stack

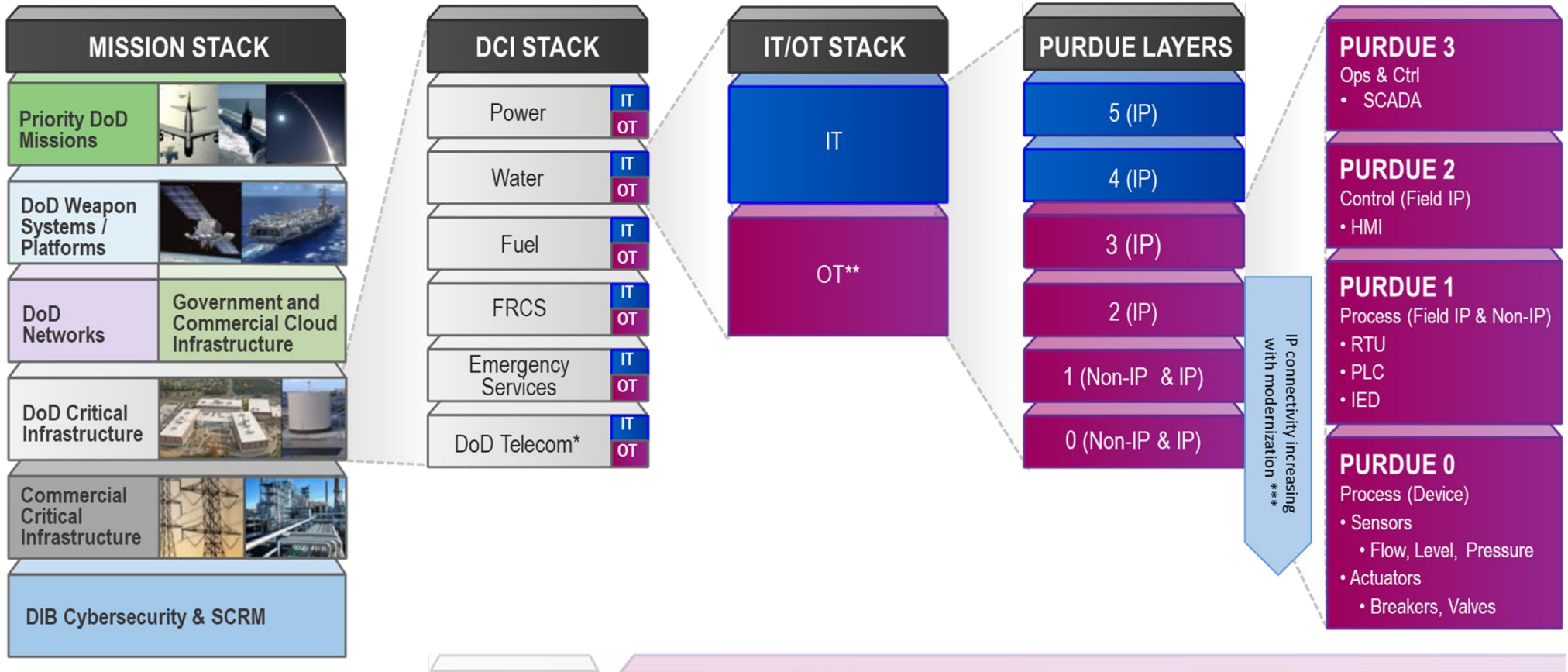


FIGURE IS UNCLASSIFIED

v.20230321

Diversity of Cyber Terrain

FIGURE IS UNCLASSIFIED

System Type	Objectives/ Goals	Service Life	Components and Functions	Types of Operating Systems	Types of Protocols	Functionality
Weapon Systems/Platforms ***Embedded Information Technology and Operational Technology***	Resiliency, Reliability, Survivability, Availability	10 – 30+ Years *Varies on Platform Utilization	Actuators, Sensors, Servers, Pressurizers, Payload Delivery, Persistent Surveillance, Predictability and Deterministic Services	VxWorks, Windows, Embedded Linux, LynxOS, Various RTOS	MIL-STD 1553, ARINC 400-800 Series, CANBUS, LINK 11/16/22, TCP, Ethernet	Mission Focus and Control System Functions
Enterprise Systems ***Network Information Technology***	Confidentiality, Integrity, Availability	3 – 5 Years *Varies on Information Utilization	Cloud Services, Data Centers, Servers, Networking Equipment, Logistical Services, Operations Management	Windows, Linux, Unix	HTTPS, SNMP, NTP, SFTP, SSL/TLS, SMS, DNS, TCP, UDP, Ethernet	General Purpose
Industrial Control Systems ***Operational Technology***	Safety, Availability, Reliability, Repeatability	10 – 30+ Years *Varies on Operational Utilization	Human Machine Interfaces, Sensors, Remote Terminal Units, Actuators, Programmable Logic Controllers, Intelligent Electronic Devices	CMX RTOS, VxWorks, OS-9, Windows IoT/Embedded, Embedded Linux	Modbus RTU, TSAA, Ethernet/IP CIP, BACnet, DNP3, Modbus TCP NTP, HTTPS, OPC, HART, Zigbee	Specific Control System Functions

FIGURE IS UNCLASSIFIED

Cyber Key Terrain Landscape: Examples

FIGURE IS UNCLASSIFIED

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

FIGURE IS UNCLASSIFIED

Global Impact of the 2017 "Tactical Cyber Attack" in Ukraine

FIGURE IS UNCLASSIFIED

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

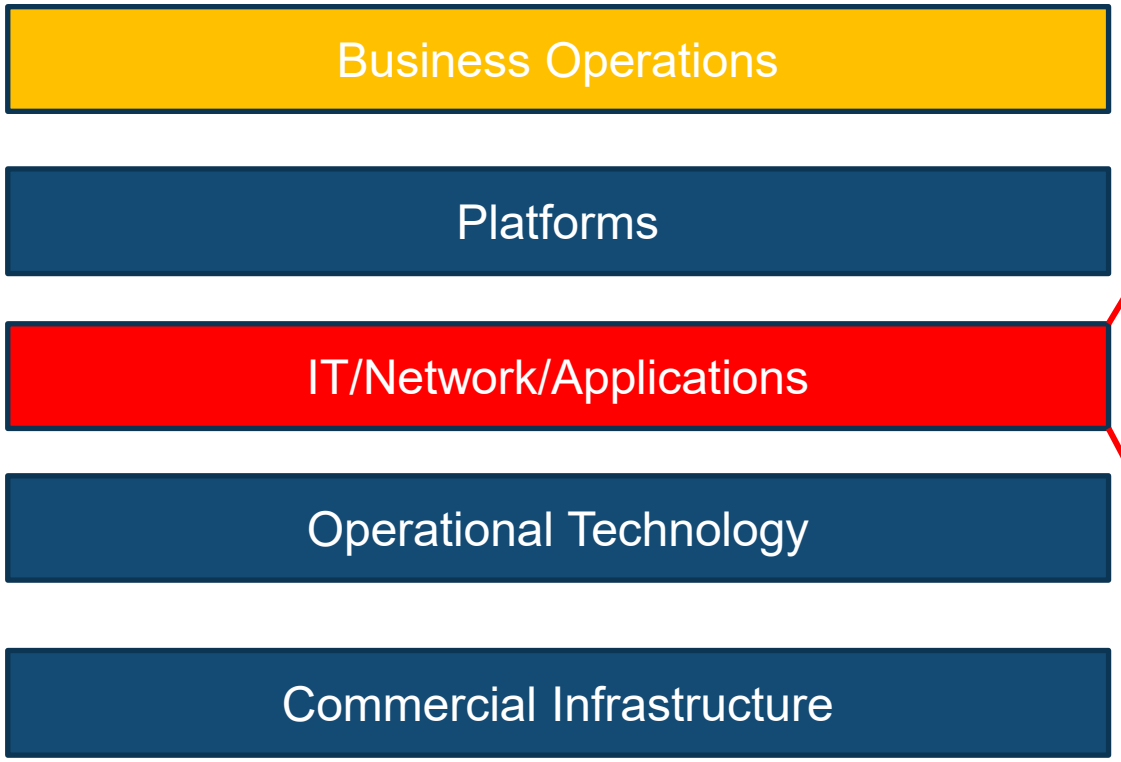
- **"It was the equivalent of using a nuclear bomb to achieve a small tactical victory"**
- **"To date, it was the fastest propagating piece of malware we've ever seen" [Cisco]**
  - Within hours, the worm spread around the world and crippled numerous multinational companies
- **Total cost: $10B**
  - 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)

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

"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." -Andy Greenberg, Wired

Example – Cyber Risk: Impact to Maersk Business Operations from 2017 Cyber-Attack

FIGURE IS UNCLASSIFIED



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

FIGURE IS UNCLASSIFIED

(U) Maersk CEO's Perspective: "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."

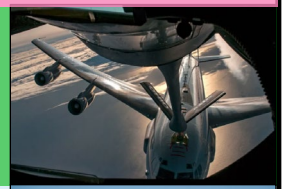
Real World Degradation to DoD Global Logistics Mission/Commercial Airlines: Notice to Air Missions (NOTAMs)

FIGURE IS UNCLASSIFIED

DoD Organizations (NIST Tier 1)
USTRANSCOM, USAF

Priority DoD Missions (NIST Tier 2)

Global Logistics



DoD Weapons Systems / Platforms

USTRANSCOM AOC

DoD Networks (NIST Tier 3)
Defense Internet NOTAM Service (DINS)

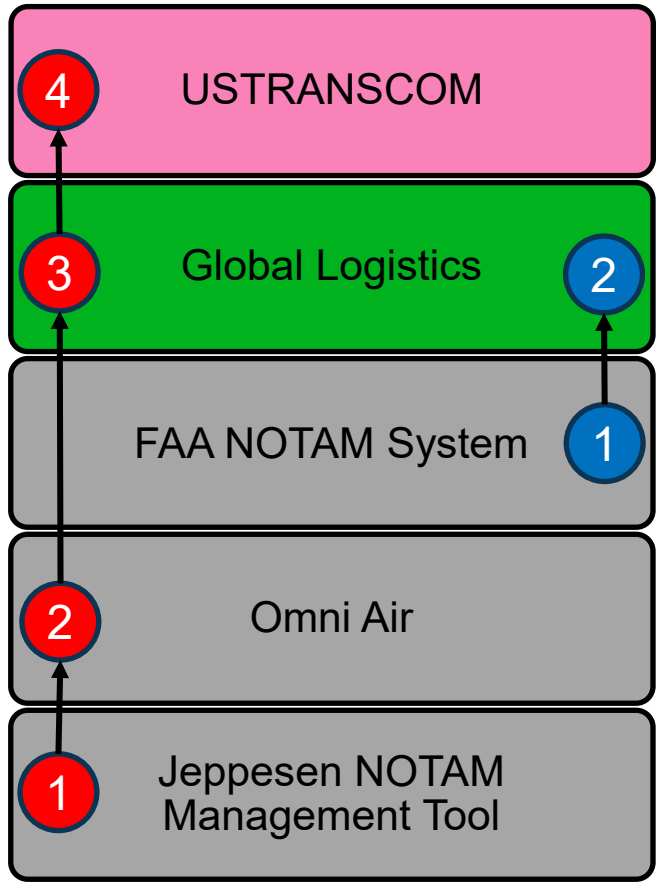
DoD Critical Infrastructure

Military airport, DoD installations

Commercial Critical Infrastructure

DIB, FAA NOTAMs system, communications, transportation sector

Civil Reserve Air Fleet, Supply Chain Risk Management, Commercial NOTAM Management Tool



Incident 1 Nov 2022

1. Cyber-attack degrades data integrity for commercial NOTAM management tool; company takes tool offline in response
2. CRAF carrier does not possess trusted NOTAMs data
3. CRAF carrier delays, cancels flights while NOTAMs tool offline
4. PAXs delayed

System offline for ~14 hours, ~1,100 PAX delayed

Incident 2 Jan 2023

1. Poor database management allowed an inadvertent input error to degrade FAA NOTAM System data integrity; FAA issues ground stop until it can ensure data integrity
2. DoD airlift unaffected as DoD possesses its own NOTAMs system: DINS

First ground stop since September 11, 2001 ~1,300 flights cancelled, ~10,000 flights delayed

FIGURE IS UNCLASSIFIED

Cyber Risks to U.S. Government Missions: Cyber-Attack that Impacted Civil Reserve Air Fleet Partner

The U.S. Government failed to address and appreciate the latent risk-to-mission that remained present after the November 2022 cyber-attack against Boeing's Jeppesen NOTAM Management Tool that degraded confidence in NOTAMs data. Omni Air operations remain dependent on this Jeppesen-provided service, which enables users to build and edit NOTAMs.

FIGURE IS UNCLASSIFIED

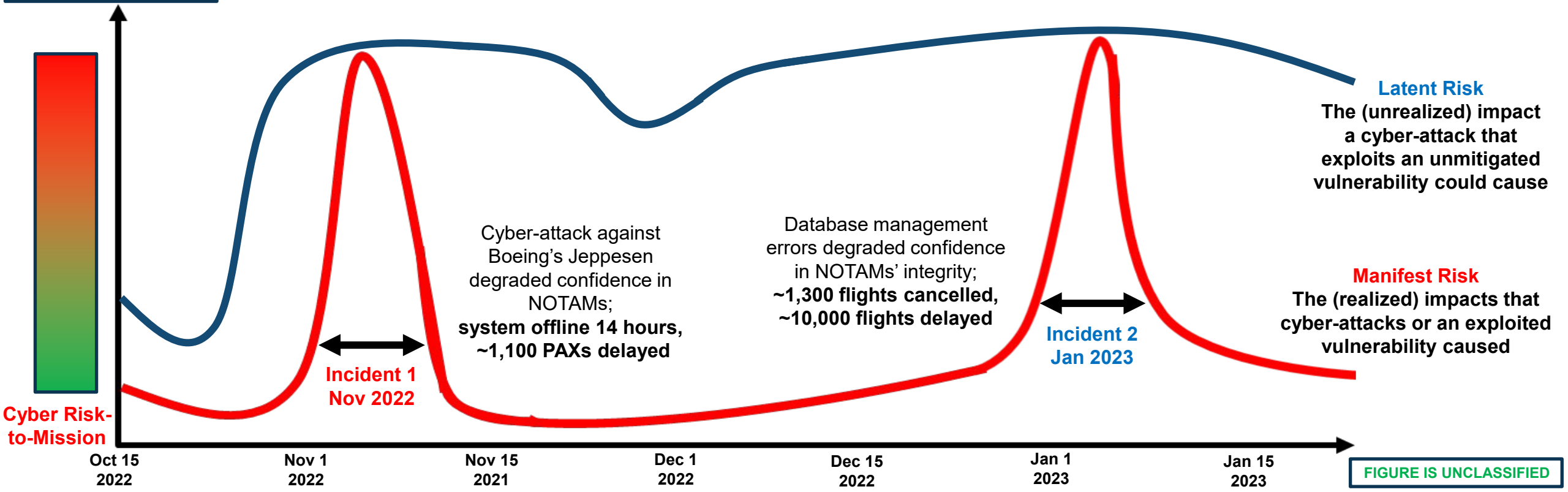
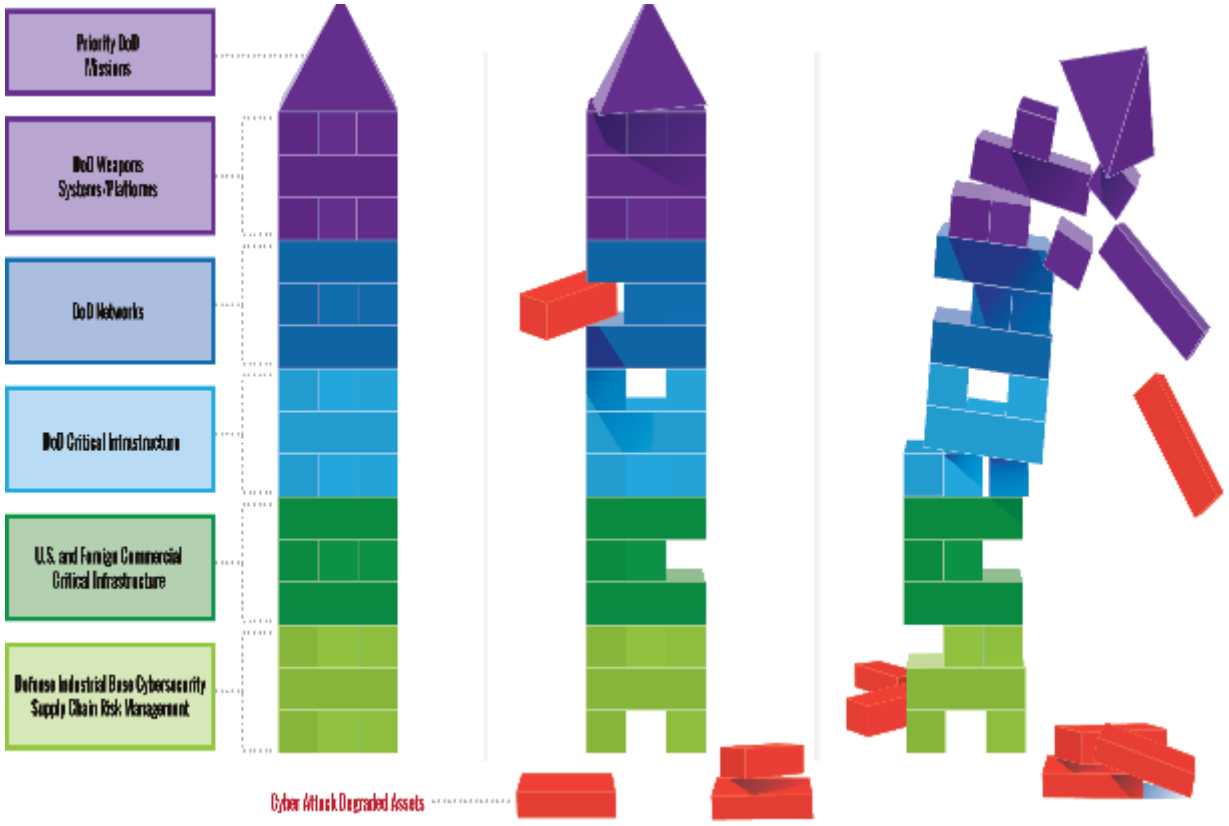


FIGURE IS UNCLASSIFIED

The Mission Stack, Modeled

DAGGER provides OUSD(A&S) with means to model and simulate cyber terrain's mission dependencies and reflect cyber-attacks second- and third-order effects.

GRAPHIC IS UNCLASSIFIED



GRAPHIC IS UNCLASSIFIED

Mission Level Cyber Risk Assessment (MLCRA) Structure

GRAPHIC IS UNCLASSIFIED

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

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

Cyber Risk to Mission Assessment

GRAPHIC IS UNCLASSIFIED

Cyber/Mission Resilience Series Overview

GRAPHIC IS UNCLASSIFIED

May 2017: Cyber Resilience I GPS/OCS (USSTRATCOM)

Apr 2018: Cyber Resilience II NC3 AEFH MILSTAR (USTRATCOM)

Mar 2019: Cyber Resilience III Theater BMD (USEUCOM)

Nov 2019: Cyber Resilience IV Wideband Global SATCOM (USINDOPACOM)

Aug 2020: Cyber Invictus CPT Capacity (USCYBERCOM)

Oct 2021: Mission Resilience I Global Logistics (USTRANSCOM/USEUCOM)

January 2023: Mission Resilience II (USSPACECOM)

August 2024: Mission Resilience III (USNORTHCOM)

GRAPHIC IS UNCLASSIFIED

Mission Resilience Analysis Process

GRAPHIC IS UNCLASSIFIED

Research (7 Months)
- Understand combatant command missions
- Model systems of interest and cyber terrain
- Coordinate with SMEs

Plan (4 Months)
- Develop red campaign based on identified cyber vulnerabilities (red cell)
- Organize blue defense of key assets (blue cell)

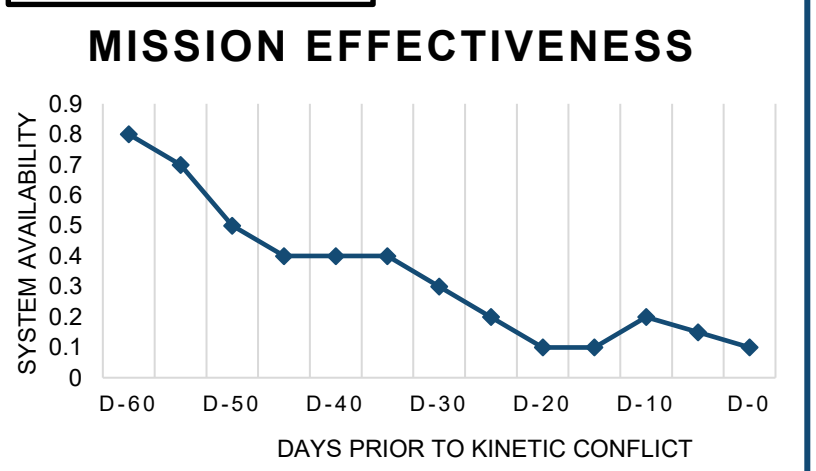
Execute (1 week)
- Hold wargame capstone event
- Observe Red and Blue player interactions
- Simulate cyber effects

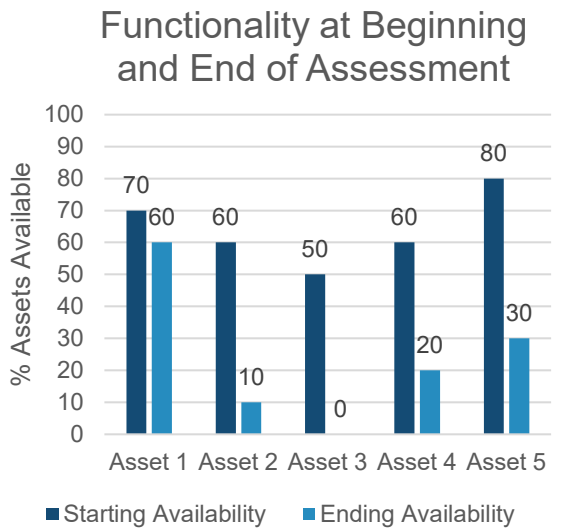
Assess (6 Months)
- Examine mission degradation
- Characterize cyber risk-to-mission

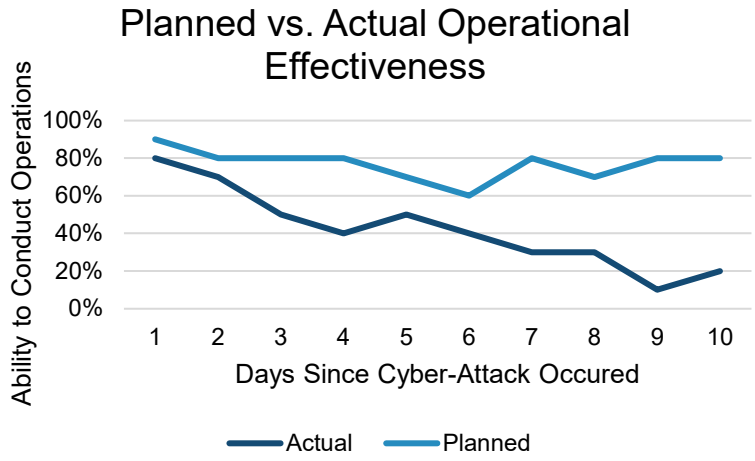
GRAPHIC IS UNCLASSIFIED

Example Analysis Outputs

GRAPHIC IS UNCLASSIFIED







Note: Data is notional and does not represent MLCRA wargame findings

GRAPHIC IS UNCLASSIFIED

Cybersecurity Workforce Maturity for Each System Type

GRAPHIC IS UNCLASSIFIED

Focus for Cybersecurity Workforce Initiative

	Cybersecurity Workforce	Acquisition Workforce	Available Certificates (Offerors)	Cybersecurity Education, and Training (Offerors)
Weapon Systems/Platforms			No specific certificate available for weapon system cybersecurity (due to uniqueness of systems and limited application)	
Network Information Technology		Government courses in IT and OT acquisition offered but vary	CompTIA ITIL Foundation (ISC)²	
Operational Technology	Control system security specialist work role		DHS CISA's NICCS GICSP GRID InfoSec Institute	EC-Council *SANS Institute*

GRAPHIC IS UNCLASSIFIED

Cybersecurity Workforce Maturity differs across system types and requires increased attention.

Summary

- (U) Cybersecurity is National Security
- (U) The cyber threat is a clear and present danger to the public and private sectors
- (U) Cybersecurity for weapon systems/platforms creates unique challenges
- (U) Unfilled cybersecurity positions create a workforce gap
- (U) The educational sector can play a critical role in preparing and training the cybersecurity workforce