



(U) Enhancing the Cybersecurity Posture of Commercial Critical Infrastructure

SLIDES ONLY
NO SCRIPT PROVIDED



Remarks to High Performance Computing User Forum

Mr. John Garstka
Director, Cyber Warfare
OUSD Acquisition and Sustainment
3 Sep 2025

CLEARED
For Open Publication

Sep 02, 2025

Department of Defense

OFFICE OF PREPUBLICATION AND SECURITY REVIEW

Overall classification: **UNCLASSIFIED**
Discussion classification: **UNCLASSIFIED**



(U) 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

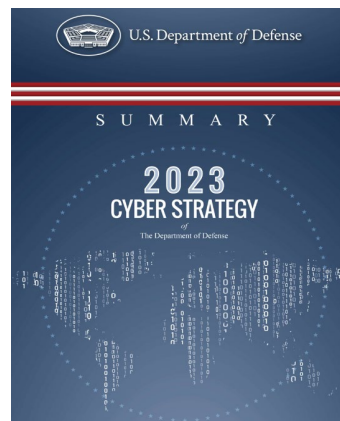
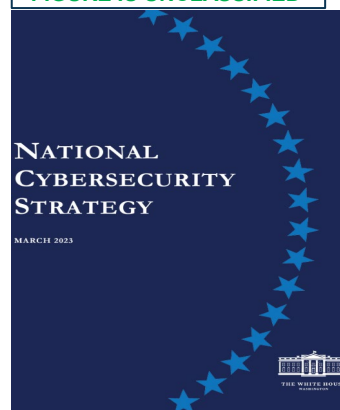


FIGURE IS UNCLASSIFIED

(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) “Sophisticated adversaries increasingly demonstrate the ability to extend a contested environment across the globe and to our homeland with the specific aim to disrupt the responsive and strategic reach of USTRANSCOM.”

– GEN Randall Reed, Commander, United States Transportation Command, FY2026 Posture Statement, March 26, 2025.



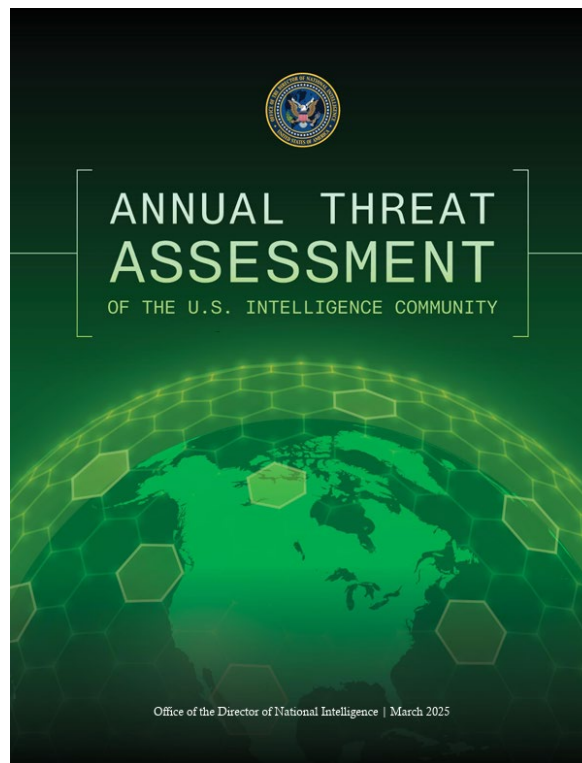
(U) The Cyber Threat is a Clear and Present Danger



(U) People's Republic of China

- (U) “The PRC remains the most active and persistent cyber threat to U.S. government, private-sector, and critical infrastructure networks.”
- (U) “China has demonstrated the ability to compromise U.S. infrastructure through formidable cyber capabilities that it could employ during a conflict with the United States.”
- (U) “If Beijing believed that a major conflict with Washington was imminent, it could consider aggressive cyber operations against U.S. critical infrastructure and military assets.”
- (U) “China has eclipsed Russia as a space leader and is poised to compete with the United States as the world’s leader in space [...]”

GRAPHIC IS UNCLASSIFIED



Reference: ODNI Annual Threat Assessment of the USIC 2025

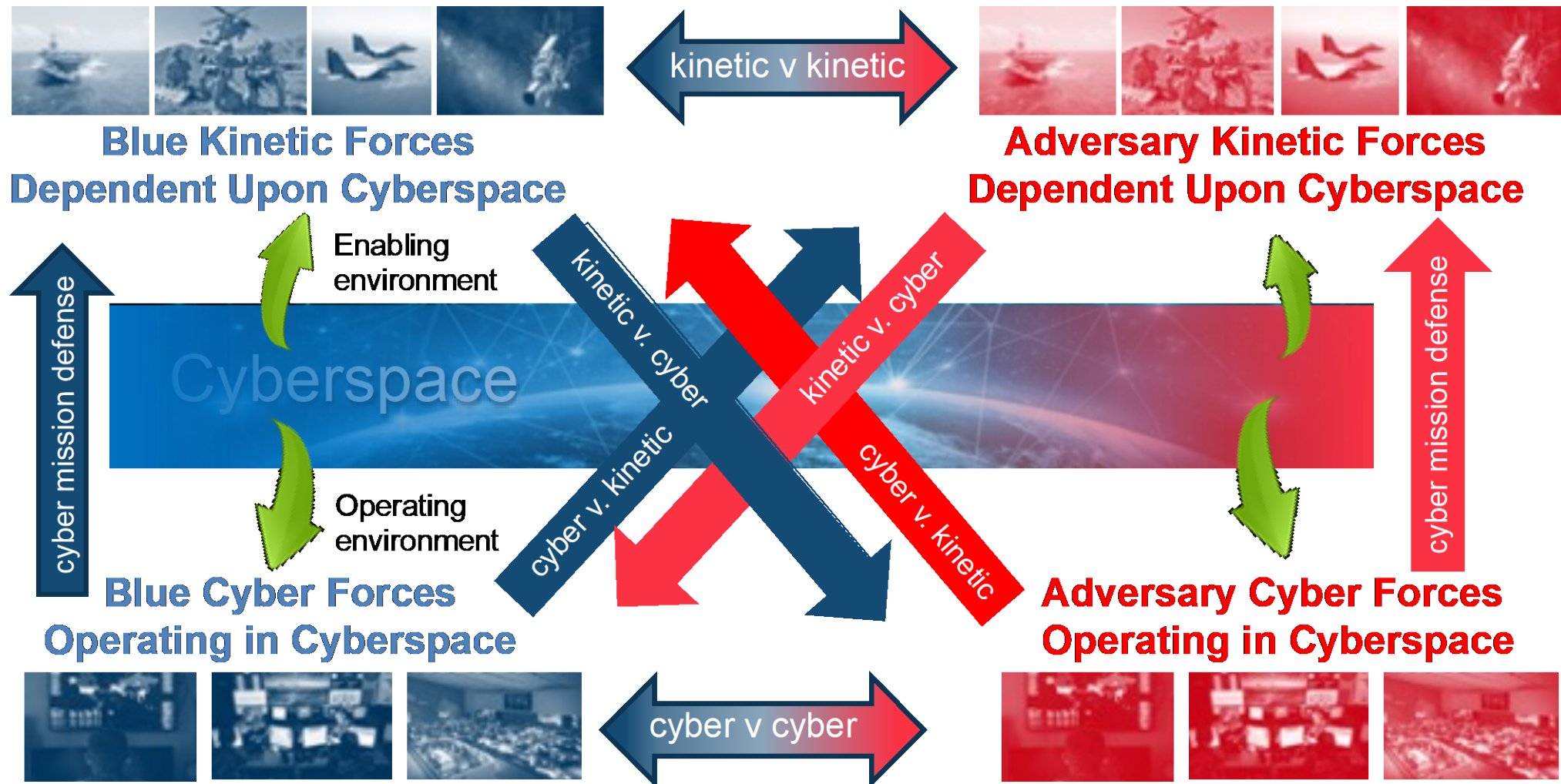
GRAPHIC IS UNCLASSIFIED

(U) Russia

- (U) [...] “Russia’s current geopolitical, economic, military, and domestic political trends underscore its resilience and enduring potential threat to U.S. power, presence, and global interests.”
- (U) “Russia’s advanced cyber capabilities, its repeated success compromising sensitive targets for intelligence collection, and its past attempts to pre-position access on U.S. critical infrastructure make it a persistent counterintelligence and cyber attack threat.”
- (U) “Russia has demonstrated real-world disruptive [cyber] capabilities during the past decade.”
- (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) Cyberspace is a Warfighting Domain ... and the 5th Domain of Conflict





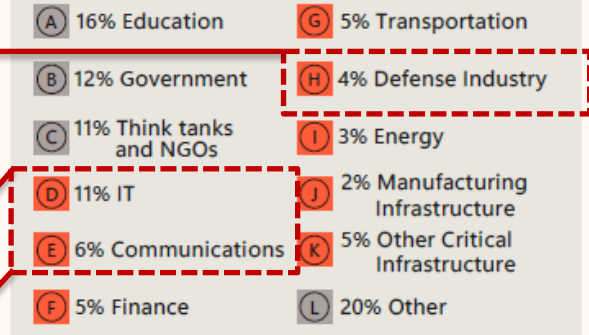
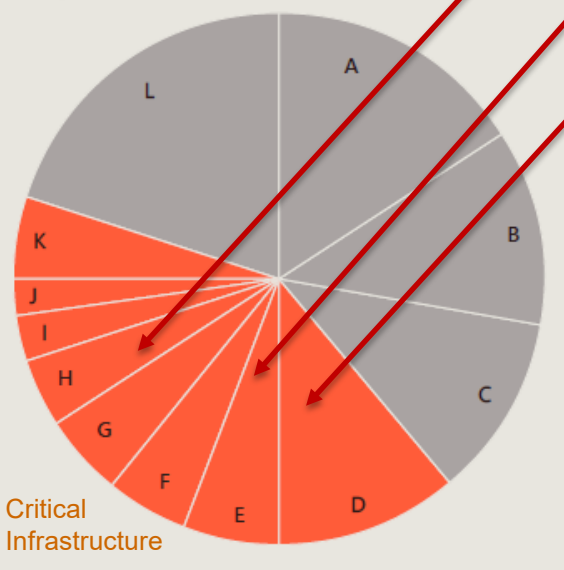
(U) Malicious Cyber Actors Targeting Critical Infrastructure Sectors

GRAPHIC IS UNCLASSIFIED

(U) State-sponsored threat groups targeting of Global Critical Infrastructure

Most targeted sectors globally

State-sponsored threat groups target broadly as part of their intelligence collection. Critical infrastructure sectors (highlighted) comprised 41% of the NSNs sent in FY2023.



Source: Microsoft Threat Intelligence NSN data.

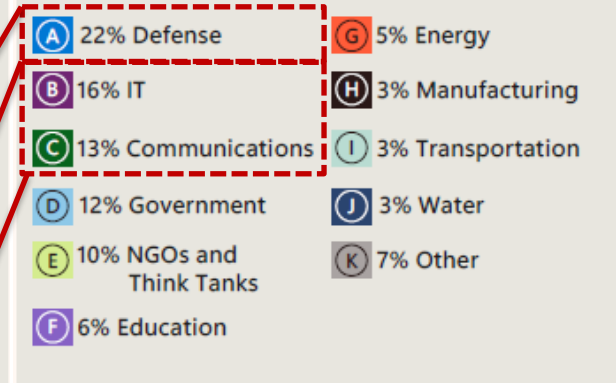
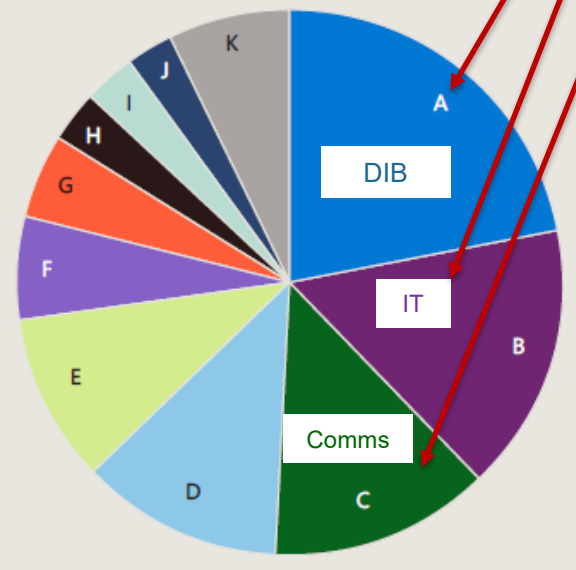
Ref: Microsoft Digital Defense Report 2023

NSN: Nation state notifications

(U) Chinese threat groups targeting of U.S. Critical Infrastructure Sectors

Chinese targeting of US sectors

Chinese state-sponsored threat actors were broadly interested in US military capabilities and its policymaking during this reporting period.



Source: Microsoft Threat Intelligence

Ref: Microsoft Digital Defense Report 2023

GRAPHIC IS UNCLASSIFIED

(U) Different threat actors could prioritize and select firms in accordance with their primary motivation where these motives align with the highest probability of attack success.



(U) The Cyber Threat is a Clear and Present Danger



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

CTIIC | JUNE 2024

Page 1 of 2

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.

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

CYBER ACTORS

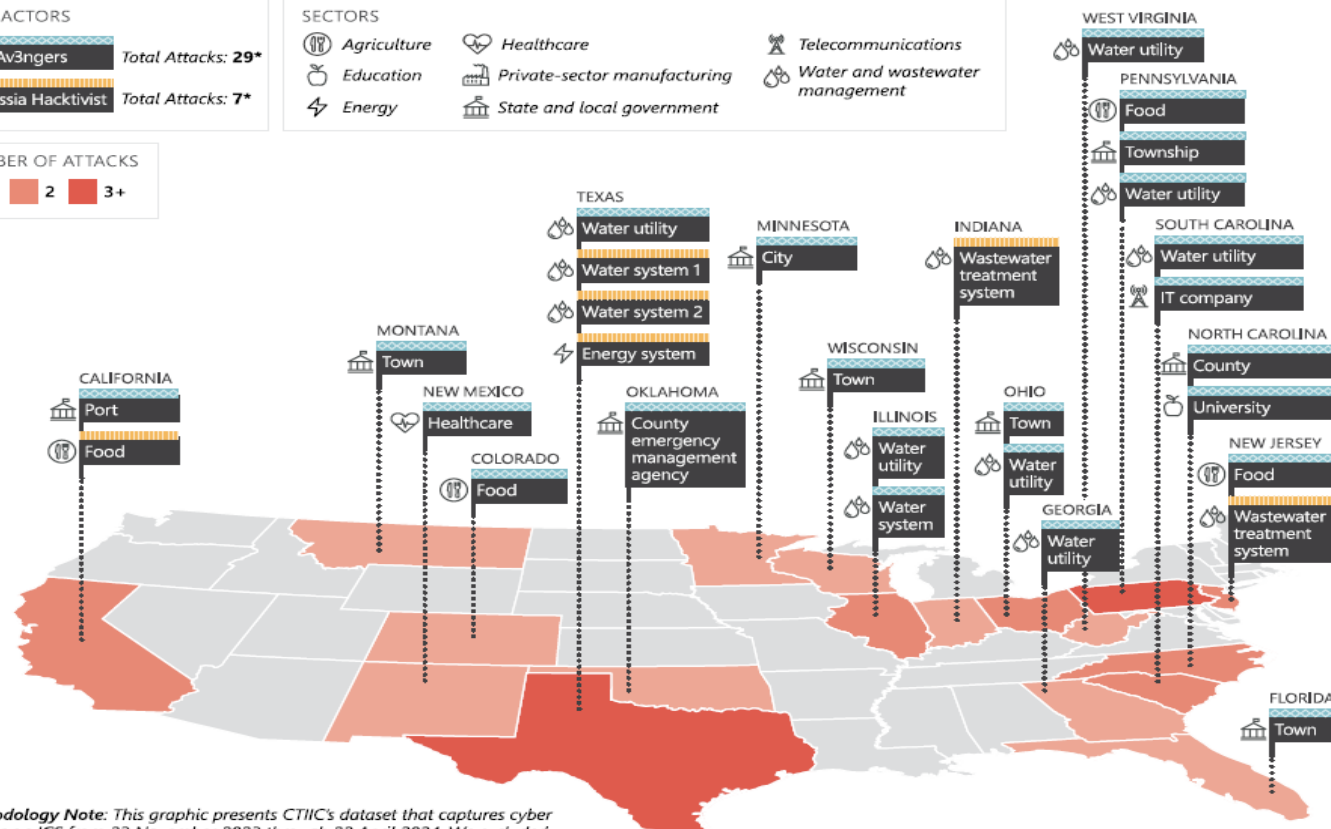
Cyber Avengers	Total Attacks: 29*
Pro-Russia Hacktivist	Total Attacks: 7*

SECTORS

Agriculture	Healthcare	Telecommunications
Education	Private-sector manufacturing	Water and wastewater management
Energy	State and local government	

NUMBER OF ATTACKS

1	2	3+
---	---	----

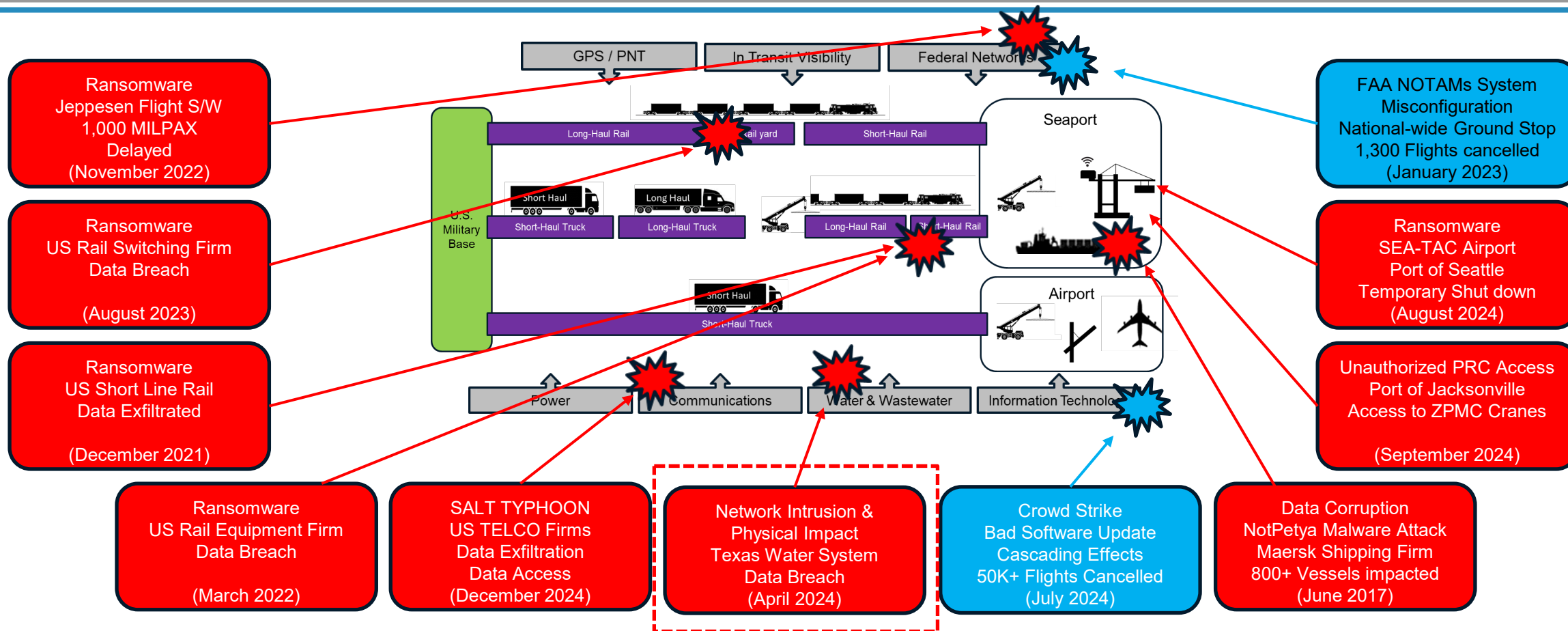


Methodology Note: This graphic presents CTIIC's dataset that captures cyber attacks on ICS from 23 November 2023 through 22 April 2024. We excluded ransomware attacks on critical infrastructure entities.

*Including seven attacks at additional US locations.



(U) The Cyber Threat is a Clear and Present Danger: Example Cyber Attacks Against U.S. Domestic TSP, TCI, and CCI Networks



Malicious Cyber Activity is impacting all layers of the Expanded Transportation Mission Stack



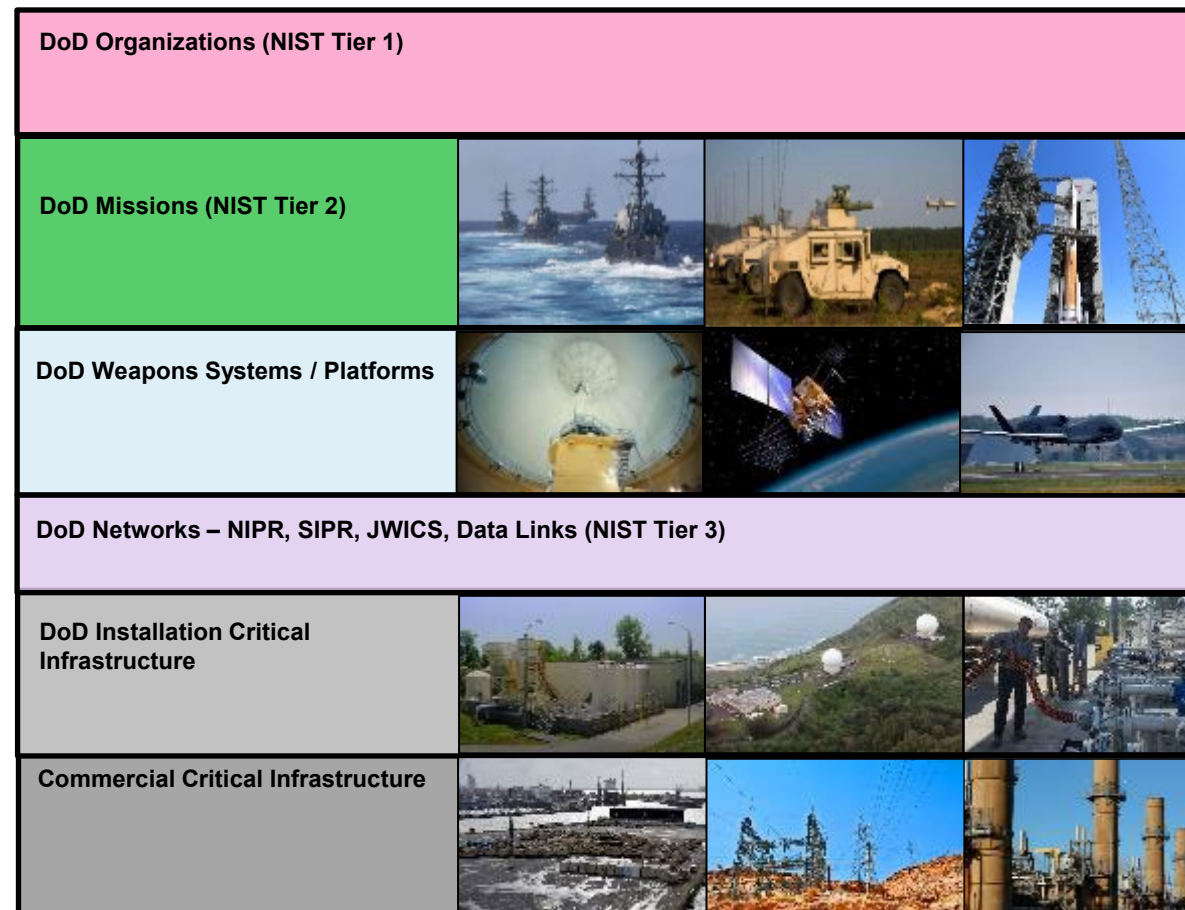
(U) Assessing Cyber Risk to Mission

GRAPHIC IS UNCLASSIFIED



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

THE MISSION STACK

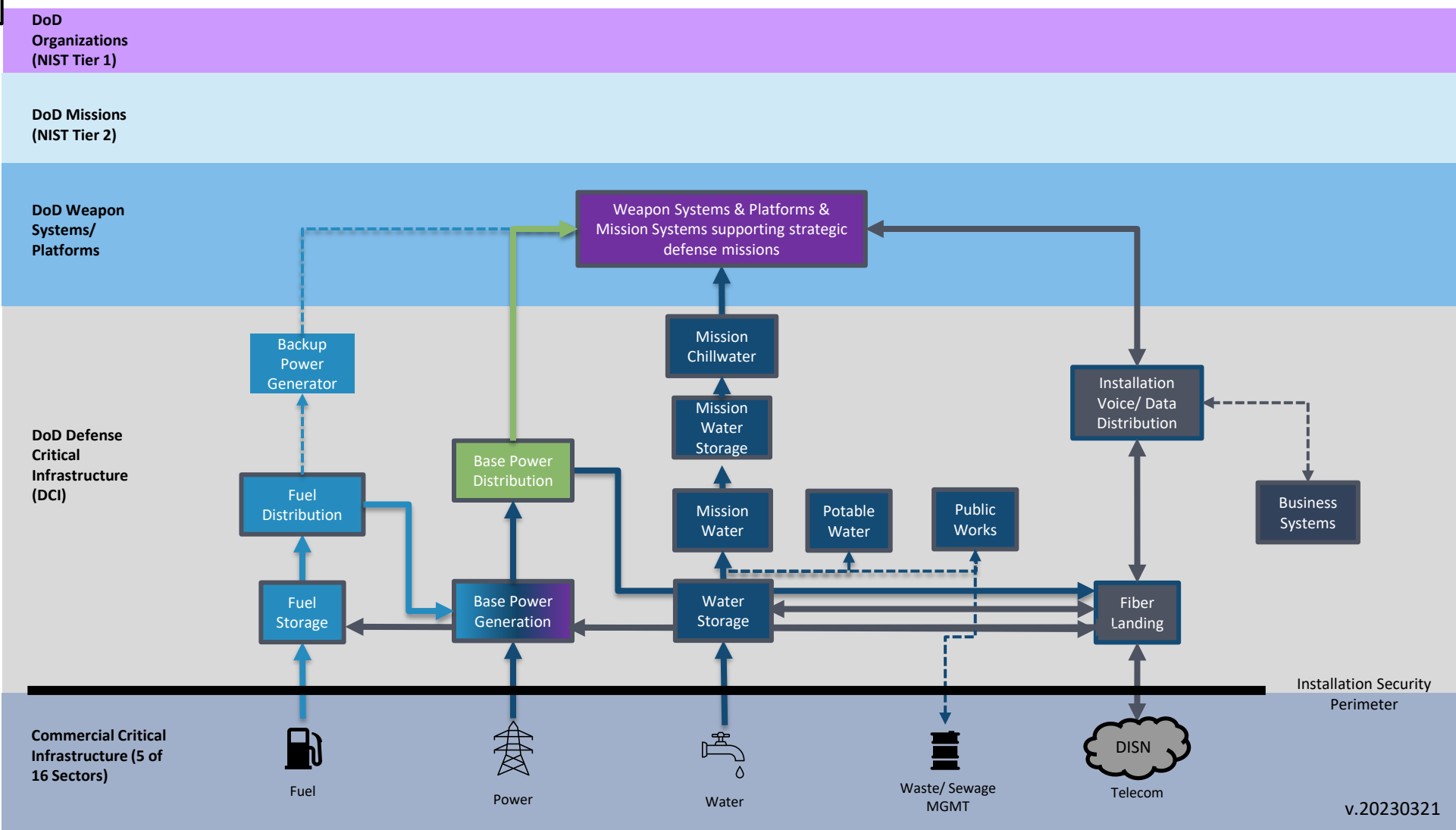


GRAPHIC IS UNCLASSIFIED



(U) Installation Critical Infrastructure (ICI) Supporting DoD Missions

GRAPHIC IS UNCLASSIFIED



v.20230321

GRAPHIC IS UNCLASSIFIED



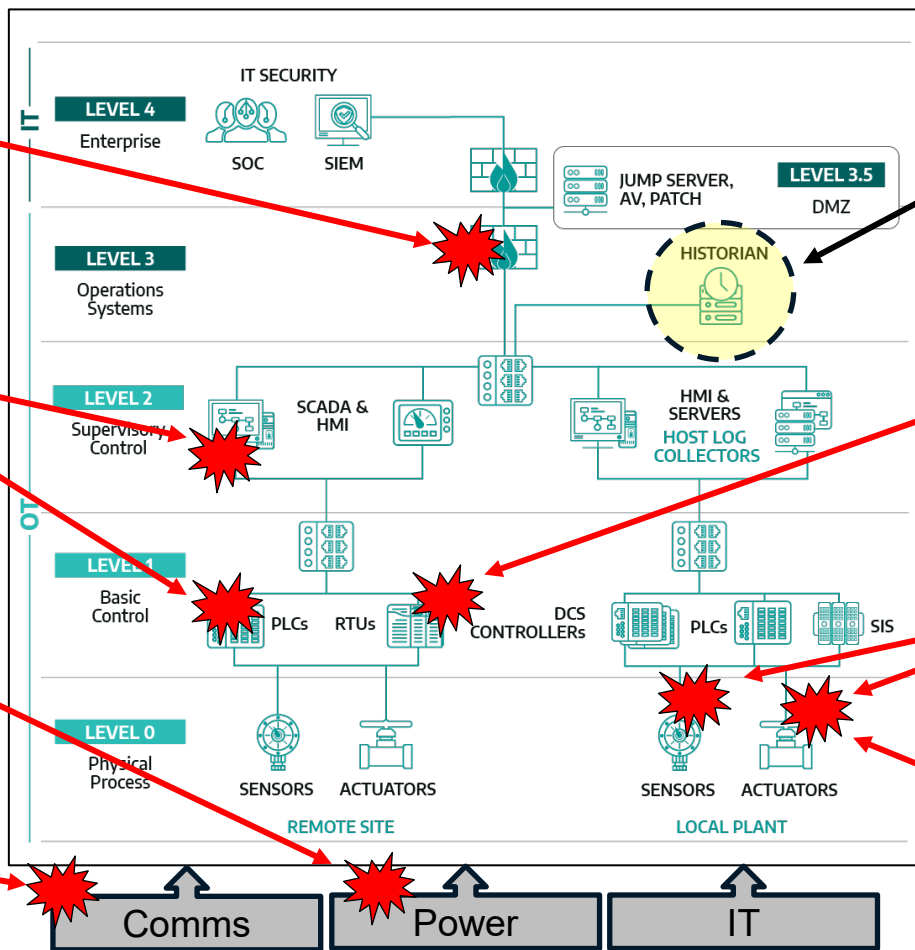
(U) The Cyber Threat is a Clear and Present Danger: Real-world Malicious Cyber Activity directed against Operational Technology

Zyxel Firewall Root Privilege
May 2023

Iranian-affiliated Cyber Attack
Unitronic PLC @ WWS
November 2023

Industroyer2
Cyber Attacks against
Ukrainian Power Grid
April 2022

Chinese Cyber Intrusion
SALT TYPHOON
Data access for US TELCOs
October 2024



GE Proficy Historian Server
CISA identified Vulnerability
January 2023

Ghost Sec Group
Claims ability to Encrypt RTUs
January 2023

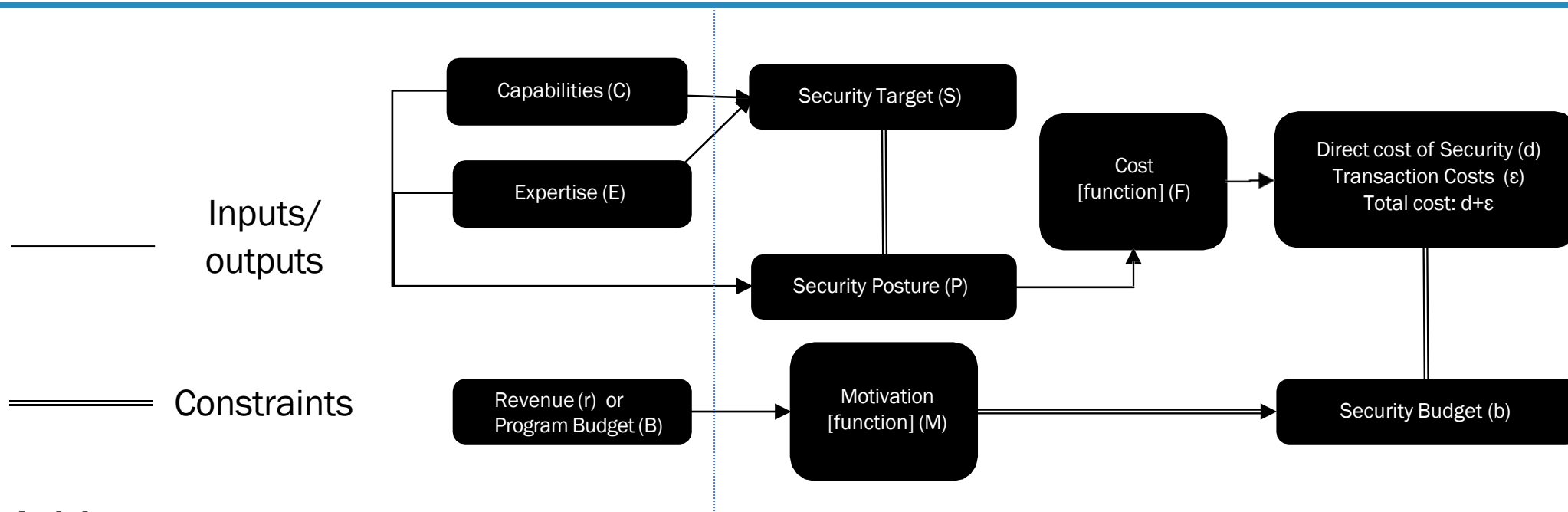
Predatory Sparrow Group
Khuzestan Steel
Compromised Cameras and Valves
June 2022

Russia-affiliated Group
Network Breach Texas Water Firms
April 2024

(U) The threat to Operational Technology is not notional; Nation-state and criminal actors are already targeting and attacking Commercial Critical Infrastructure



(U) Economics of Cybersecurity



Key Variables:

P: Cybersecurity Posture

S: Cybersecurity Target

B: Program Budget

b: Security Budget

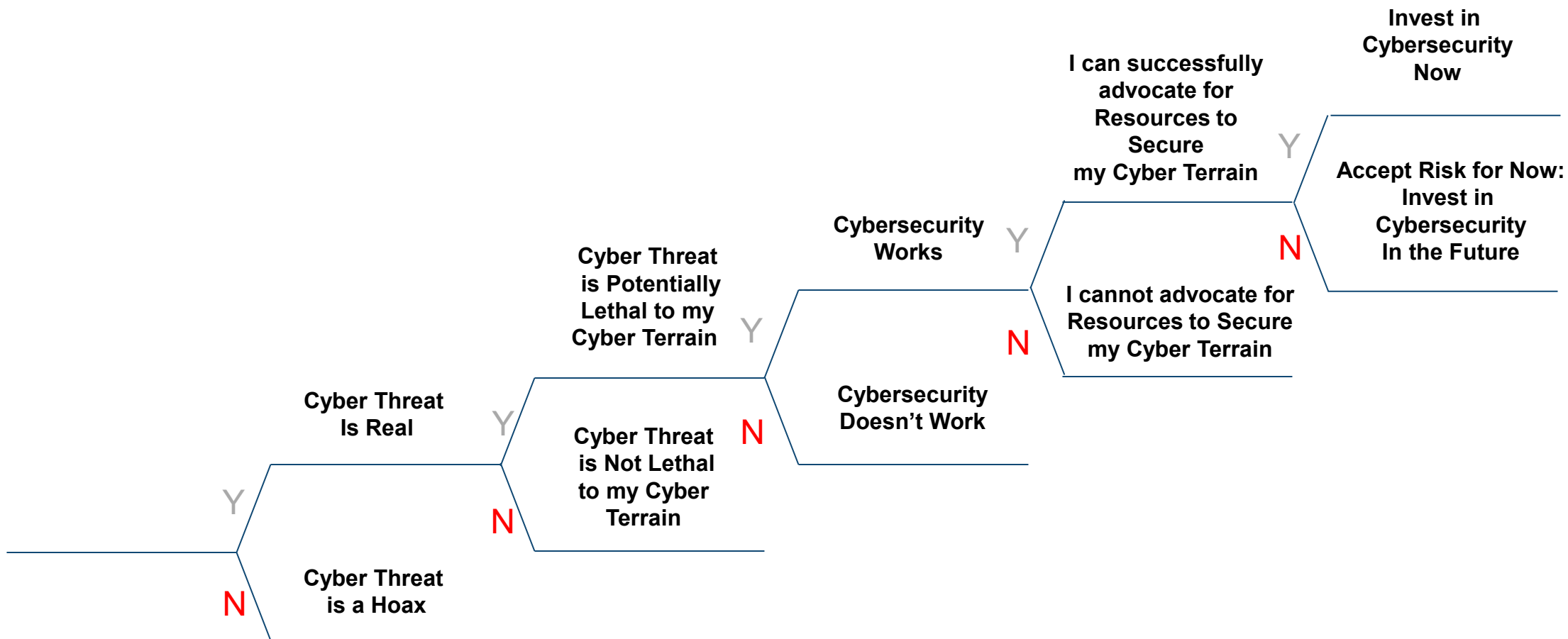
r: Revenue

GRAPHIC IS UNCLASSIFIED

(U) Motivation involves risk assessment and is key to increasing cybersecurity posture



(U) Cyber Risk Assessment: Cybersecurity Decision Analysis





(U) Summary

1. Cyber threats to commercial critical infrastructure are **significant**.
2. Quantifying cyber risk is key to **resourcing** risk mitigation
3. **Motivation** is the critical factor in improving cybersecurity posture.

(U) We must honor the cyber threat posed by adversaries and criminals to our missions and supporting operations.



(U) Questions and Discussion

Cyberspace is the 5th Domain of Conflict