



Facility-Related Control System Cybersecurity Overview

Federal Facilities Council – OT/CS
Workshop

9 July 2024

Ms. Sandra Kline

Director, Mission Assurance &
FRCS Cybersecurity
Office of the Secretary of Defense
(Energy, Installations, & Environment)

Current State

[DHS CISA] has seen an evolution of threat activity from China-linked hackers “burrowing deep” into **U.S. critical infrastructure** for years as part of an effort to potentially incite “societal panic and chaos.” – Jen Easterly, Director, DHS CISA



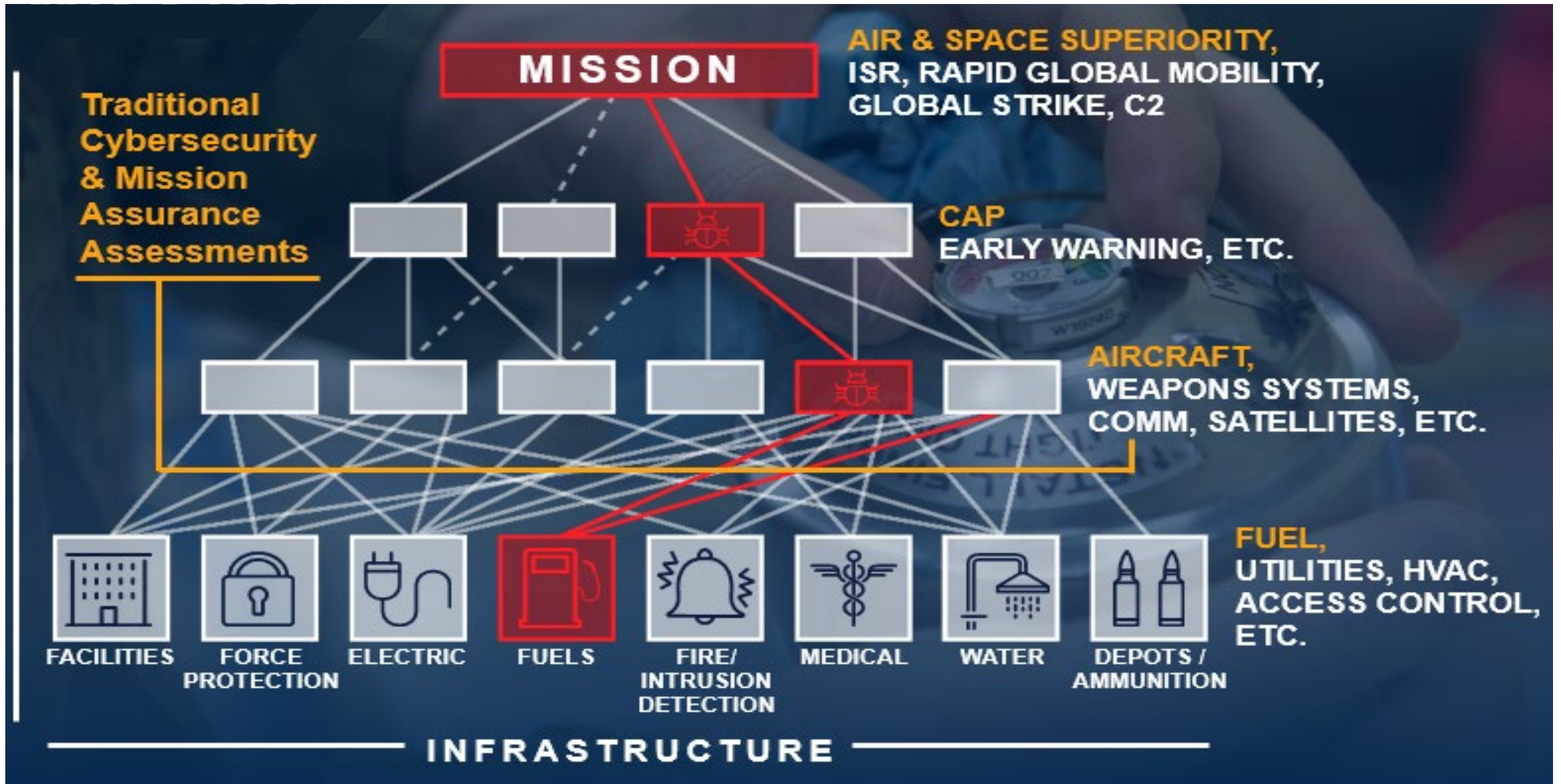
“Volt Typhoon is very focused on targeting **U.S. critical infrastructure** by staying below the radar, and works hard to reduce the signatures we use to hunt them across networks,” Sandra Joyce, VP, Mandiant Intelligence, Google Cloud



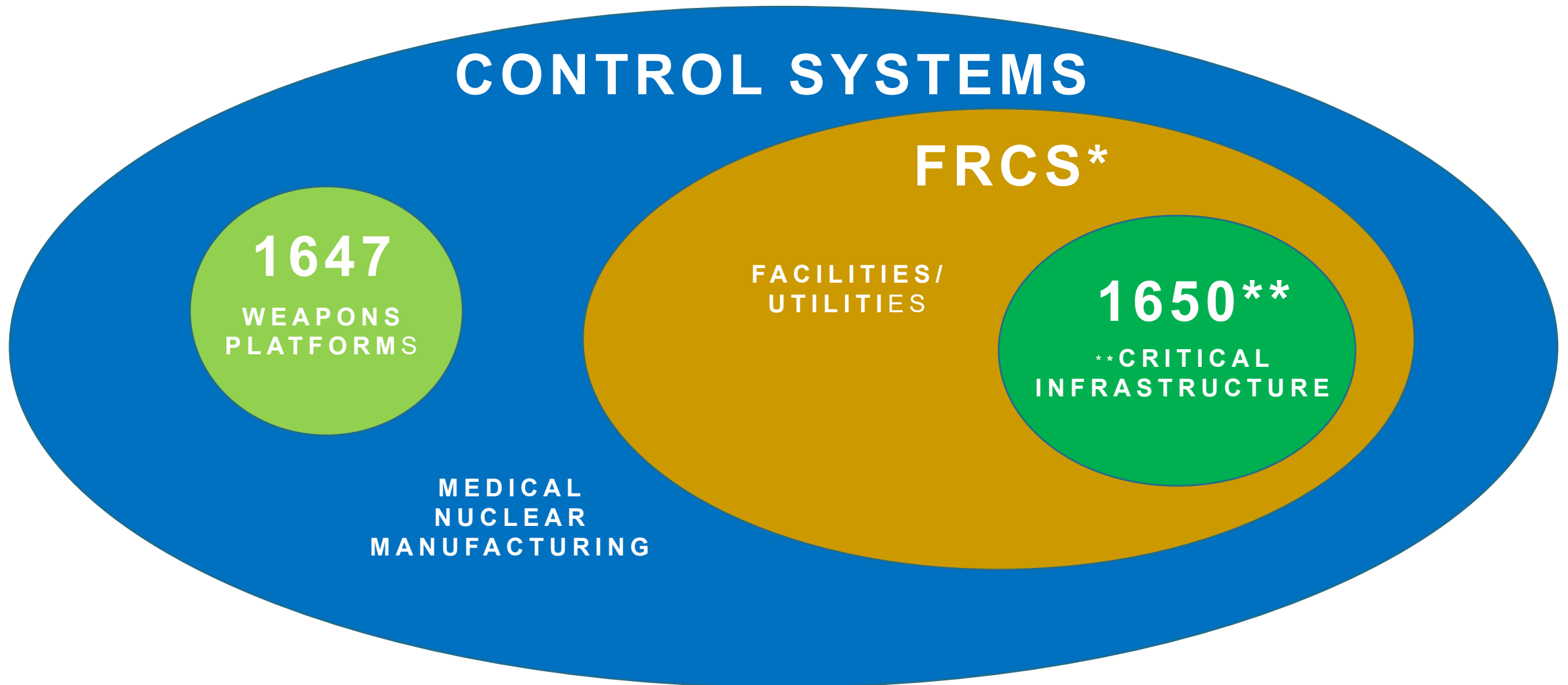
[Hackers], “are positioning on **American infrastructure** in preparation to wreak havoc and cause real-world harm to American citizens and communities, if or when China decides the time has come to strike.” – Christopher Wray, FBI Director



FRCS Vulnerabilities Disrupt Missions



CRITICAL INFRASTRUCTURE & CONTROL SYSTEMS / OT



DOD FRCS Master List

Utility Control

- Compressed gas control systems
- Natural gas control system
- District utility control systems
- Wastewater control and treatment systems
- Potable, sale, gray, and pure water control system
- Oil/water separators control system
- Electrical transmission and distribution control systems
- Cathodic protection systems
- Microgrid control system
- Uninterruptible Power Supply (UPS) control system
- Utility metering control system

Building Control

- Building lighting system
- Electrical distribution (interior)
- Heating, Ventilation, Air Conditioning (HVAC)
- Conveyance and vertical transport systems
- Irrigation and shade control
- Mass notification systems
- Medical control systems
- Meteorological control systems
- Traffic management

Utility Monitoring and Control System

- Telecomm control system
- One or more building control or utility control systems

Airfield Systems

- Aircraft arresting system
- Airfield lighting control system
- Runway ice detection system
- Ramp lighting control systems

Electronic Security Systems

- Access control system
- Electronic security system
- Intrusion detection systems
- Physical access control systems
- Chem/bio/rad monitoring systems
- Residential keyless entry control

Automated Material Handling

- Automated storage/retrieval systems
- Automated weight/offering system
- Ergonomic systems
- Forklift systems
- Packaging systems
- Robotics
- Weigh and span systems

Transportation Systems

- Railroad track control systems

Fire and Life Safety Systems

- Fire pump control system
- Fire suppression system control system
- Fire alarm reporting control system
- Fire detection and alarm control system

Environmental Monitoring

- Environmental water level monitoring systems
- Landfill leachate monitoring systems
- Pollutant discharge monitoring systems
- Water pollution monitoring system
- Water temperature monitoring system

Fueling and Transportation Systems


- Fuel leak detection system
- Petroleum, Oil & Lubricant control system
- Vehicle fueling control system

Pier Systems

Environmental Remediation

Dams, Locks & Levee Systems

DOD Cybersecurity Framework for FRCS



Adaptive	Execute Organizational Change Management	Improve Risk Management & Inventory Processes	Maintain Adaptive Enclave	Intelligence-Informed Detection	Maintain Playbook Response Library	Automated Recovery from Known-Good Resources
Repeatable	Instrumented FRCS Metrics, Reporting, & Analysis	Execute Risk Management Framework	Implement Enclave Architecture & Technical Standards	Instrumented Detection	Instrumented Security Operations	Instrumented Recovery
Risk Informed	Published FRCS Cyber Strategy & Policy	Complete System Component-Level Inventories	System Security Management	Aggregate & Analyze Log Data	Perform Security Operations	Execute Manual Recovery
Partial	Define Roles, Responsibilities & Stakeholders	Inventory Portfolio	Training and Credential Management	Publish Security Operations Plan and Policy	Publish Incident Response SOPs	Publish Recovery Plan
NIST CSF 2.0	Govern	Identify	Protect	Detect	Respond	Recover

DOD Cybersecurity Exercises for FRCS

Control System Resilience Readiness Exercise: What is it?

- The CRRE is a first-of-its-kind, “**live-fire**” cyber resilience exercise that combines real world cyber threat intelligence with **actual physical impacts**, resulting in an unprecedented simulation of how a **cyber event would cause tangible operational impact** to mission-enabling FRCS.
- This exercise is an **evolution in cybersecurity simulation, education, and training** for FRCS Owners and Operators. It provides a hands-on experience of working through the **physical disruption** to an installation that results from a cyberattack.
- The CRRE allows FRCS Owners and Operators to “train like they fight” by **combining intelligence-driven threat injects with system outages**, demonstrating the destructive potential of a cyberattack on control systems, and crucially, what Operators can and should do to **mitigate damage and restore functionality**.

Next Steps

DOD Cybersecurity Framework for FRCS is the foundation for:

- Partnering with Industry
- Implementing Zero Trust (EO 14028)
- Deploying MOSAICS
- Updating Military Construction Unified Facilities Criteria
- Standardizing FRCS Cybersecurity Commissioning and Retro-Commissioning
- Ensuring Mission Accomplishment
- Protecting Health, Life and Safety