Measuring Defense:

Prioritizing Security Solutions by Efficacy and Adversary Growth

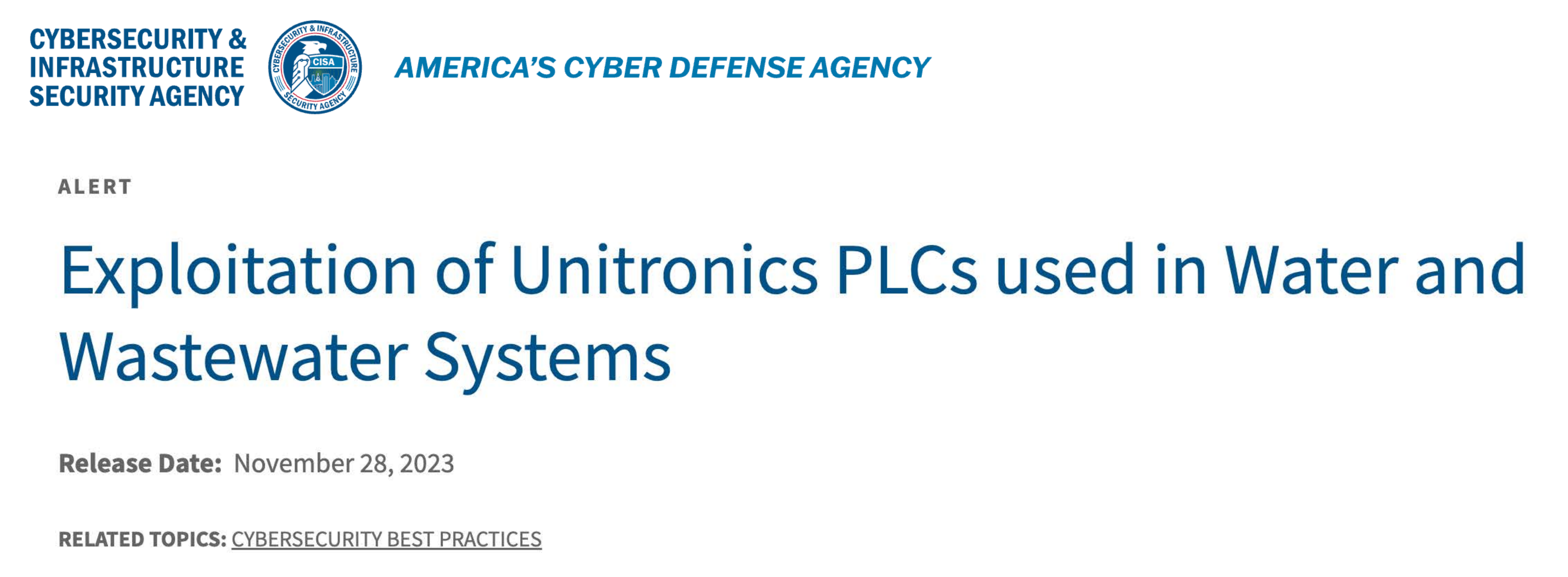
Sarah Freeman

5 December 2023

“A record 26,448 software security flaws were reported in 2022,

with the number of critical vulnerabilities up 59% on 2021 to 4,135…”

- Analysis of CVEs reported in 2022 by The Stack



CYBERSECURITY & INFRASTRUCTURE SECURITY AGENCY

AMERICA'S CYBER DEFENSE AGENCY

ALERT

Exploitation of Unitronics PLCs used in Water and Wastewater Systems

Release Date: November 28, 2023

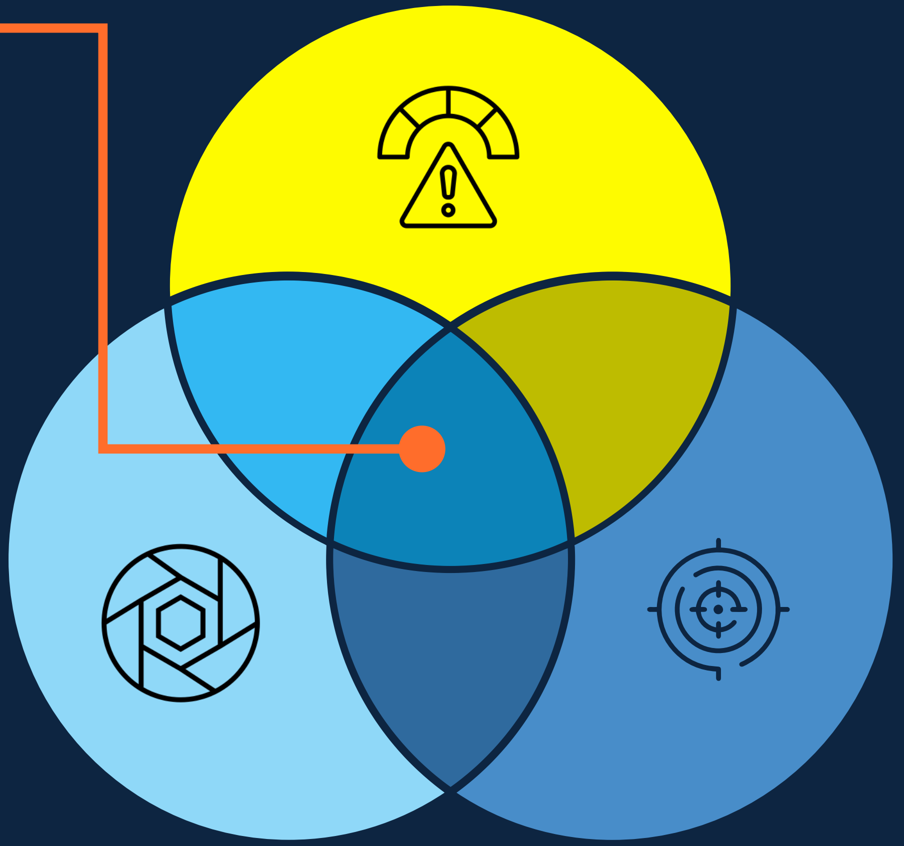
RELATED TOPICS: CYBERSECURITY BEST PRACTICES

Defensive Inefficiencies

- Prioritization of security resources remains a challenge
- Current security programs focus on vulnerability mitigation
  - What do we fix first?
- ODNI Assessments (2020-2023) noted both China and Russia targeting critical infrastructure
  - At a minimum have the capability cause localized, temporary disruptions to critical infrastructure within the United States.

> *The number of vulnerabilities disclosed in the first half of the year [2022] topped 11,800, forcing companies to determine the impact of an average of 90 security issues per weekday.*
>
> *- Dark Reading*

Re-evaluating Effective Cyber Defense



Critical DEFENSE

Understand Risk

Including tolerable risk, and potential adverse outcomes.

Understand Exposure

Can also be described in terms of "Susceptibility," and considers existing protections.

Understand Threat

Ability and willingness of an actor to cause harm.

Defining Cyber Risk

*Risk of **financial loss, operational disruption, or damage**, from the failure of the digital technologies employed for informational and/or operational functions introduced to a manufacturing system via electronic means **from the unauthorized access, use, disclosure, disruption, modification, or destruction of the manufacturing system**.*

-Cybersecurity Framework Manufacturing Profile, NISTIR 8183

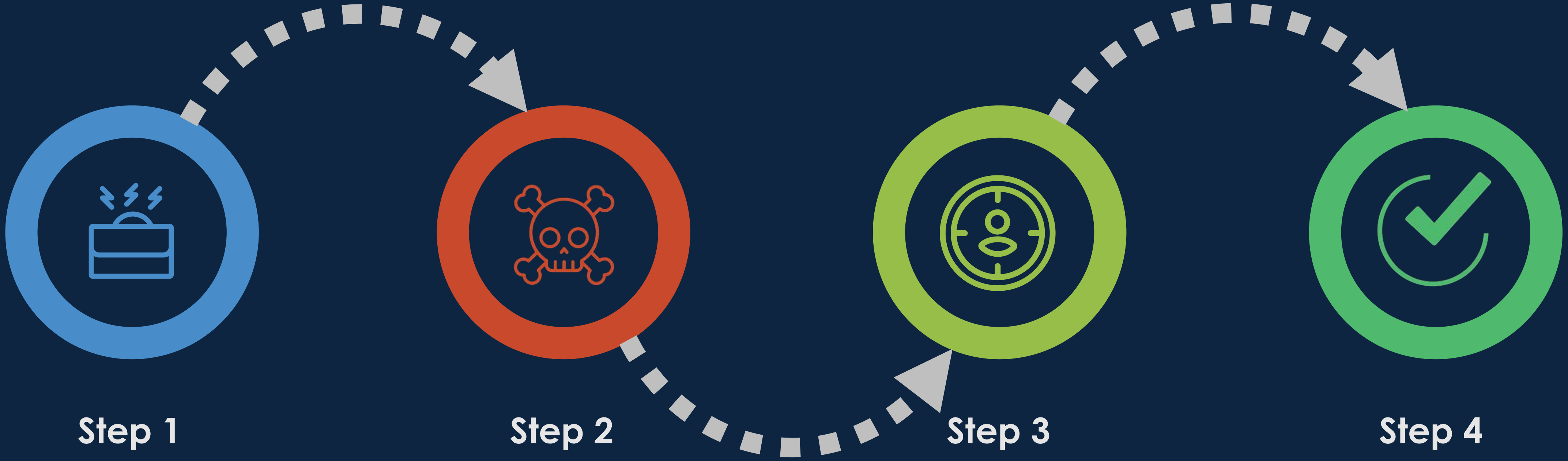
Defining Cyber Risk

*The risk of **depending on cyber resources** (i.e., the risk of depending on a system or system elements that exist in or intermittently have a presence in cyberspace).*

-Developing Cyber-Resilient Systems: A Systems Security Engineering Approach , NIST Special Publication 800-160, Volume 2

Tolerable Risk is the amount of risk deemed acceptable to meet a specific goal or outcome.

High-level Path to Tolerable Risk Identification



Step 1

Define Operational Priorities

Step 2

Calculate Threat

Step 3

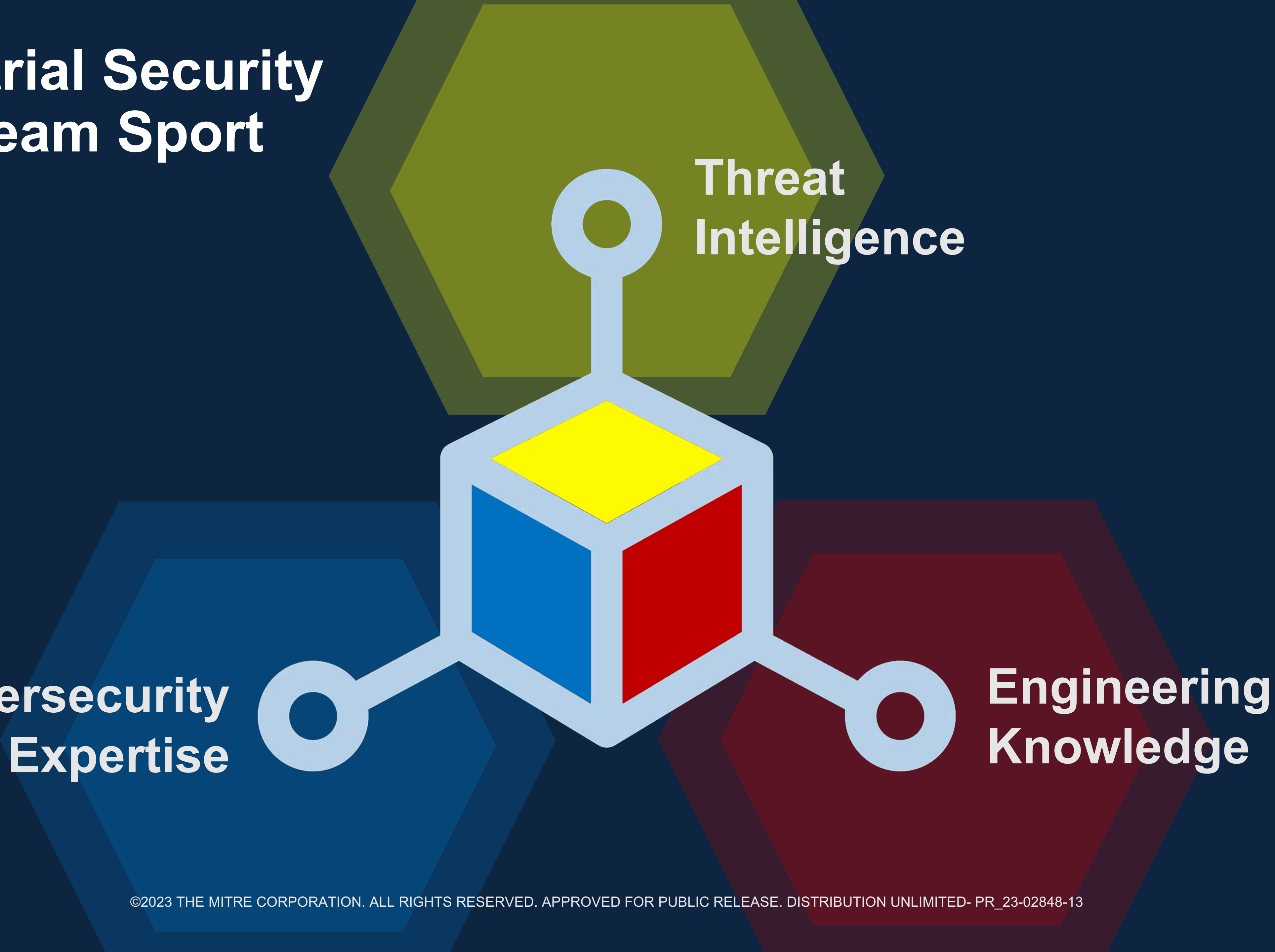
Understand Exposure

Step 4

Determine (and Communicate!) Acceptable Risk

MITRE

Industrial Security as a Team Sport



MITRE

Industrial Security as a Team Sport

Cybersecurity Expertise

- *Resilience Analysis*
- *Crown Jewel Analysis (CJA)*

Engineering Knowledge

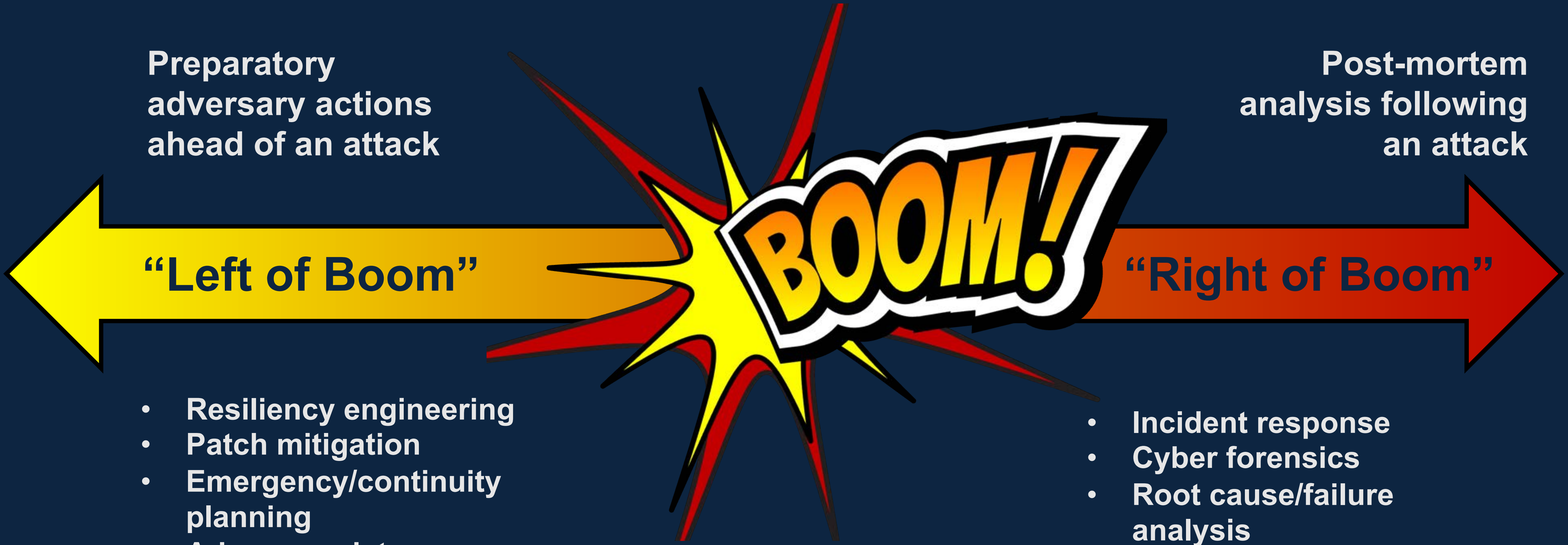
- *Failure Modes and Effects Analysis (FMEA)*
- *Cyber Process Hazard Analysis (PHA)*
- *Safety Analysis*

MITRE

Current Intelligence Approach

Preparatory adversary actions ahead of an attack

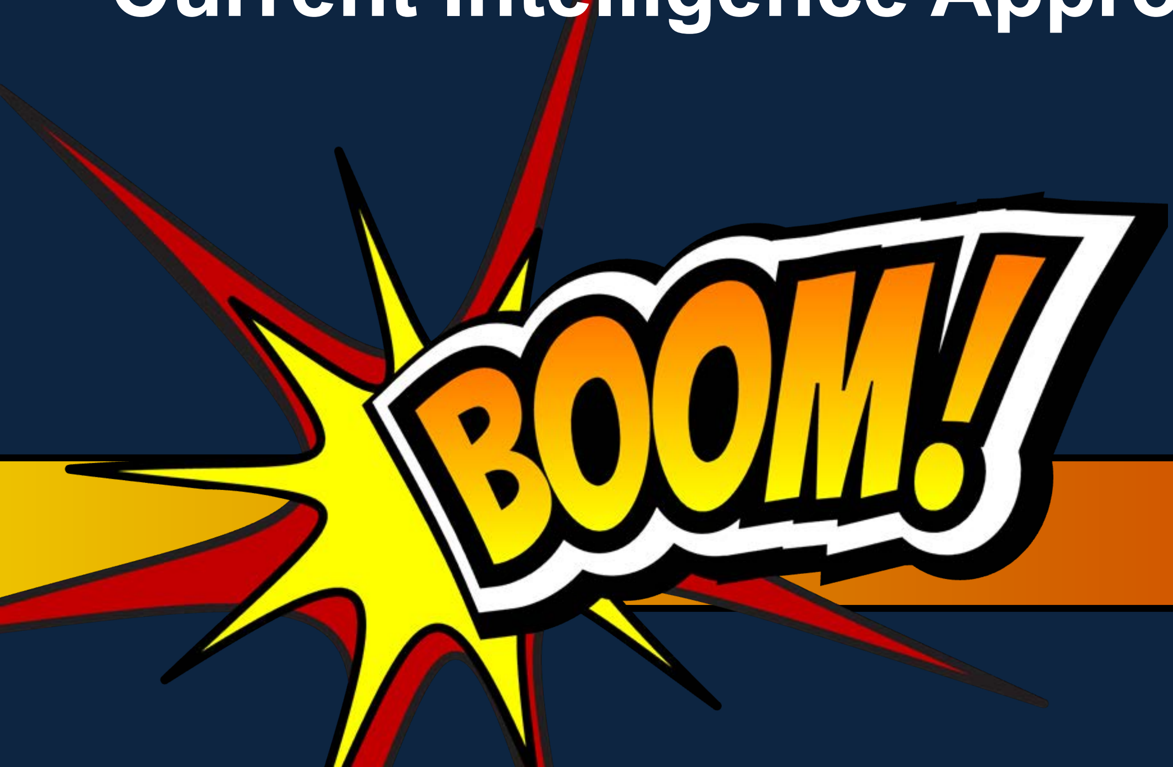
Post-mortem analysis following an attack

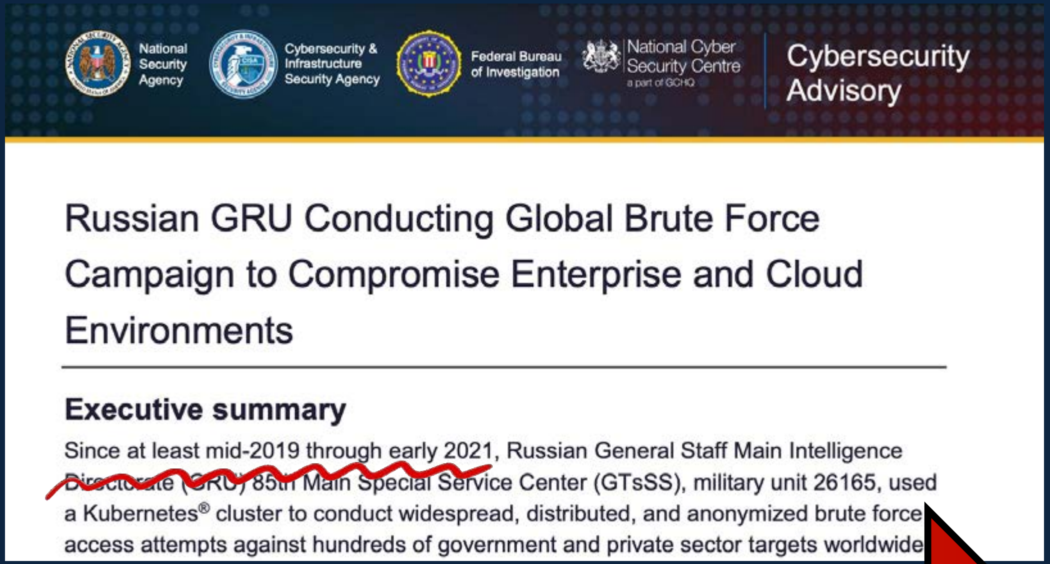


- Resiliency engineering
- Patch mitigation
- Emergency/continuity planning
- Adversary deterrence
- Etc.

- Incident response
- Cyber forensics
- Root cause/failure analysis
- Etc.

Current Intelligence Approach



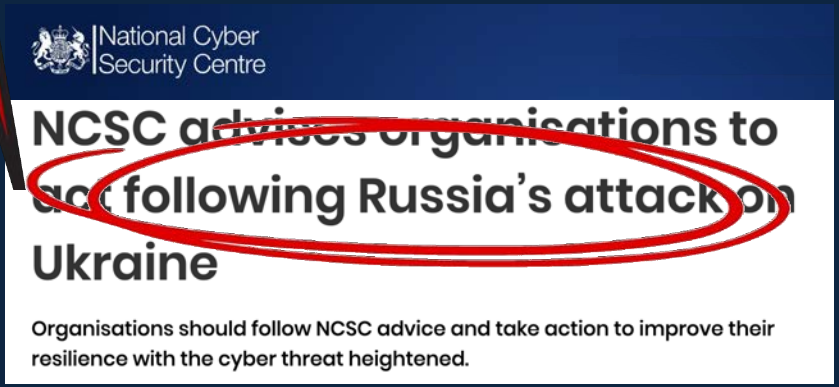


National Security Agency | Cybersecurity & Infrastructure Security Agency | Federal Bureau of Investigation | National Cyber Security Centre a part of GCHQ | Cybersecurity Advisory

Russian GRU Conducting Global Brute Force Campaign to Compromise Enterprise and Cloud Environments

Executive summary

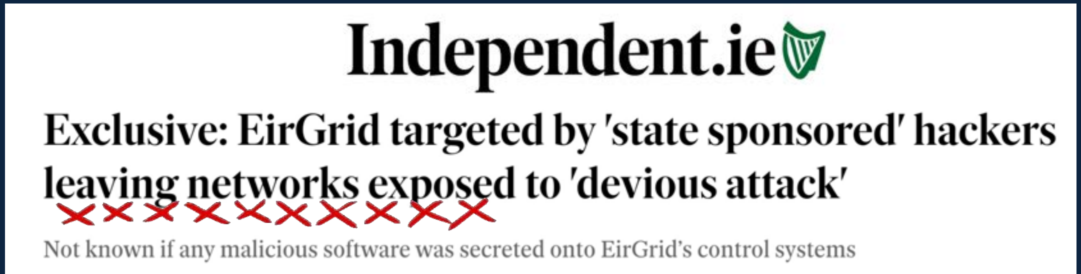
Since at least mid-2019 through early 2021, Russian General Staff Main Intelligence ~~Directorate (GRU) 85th Main Special Service Center~~ (GTsSS), military unit 26165, used a Kubernetes® cluster to conduct widespread, distributed, and anonymized brute force access attempts against hundreds of government and private sector targets worldwide



National Cyber Security Centre

NCSC ~~advises organisations~~ to ~~act~~ following Russia's attack ~~on~~ Ukraine

Organisations should follow NCSC advice and take action to improve their resilience with the cyber threat heightened.



Independent.ie

Exclusive: EirGrid targeted by 'state sponsored' hackers leaving networks exposed to 'devious attack'

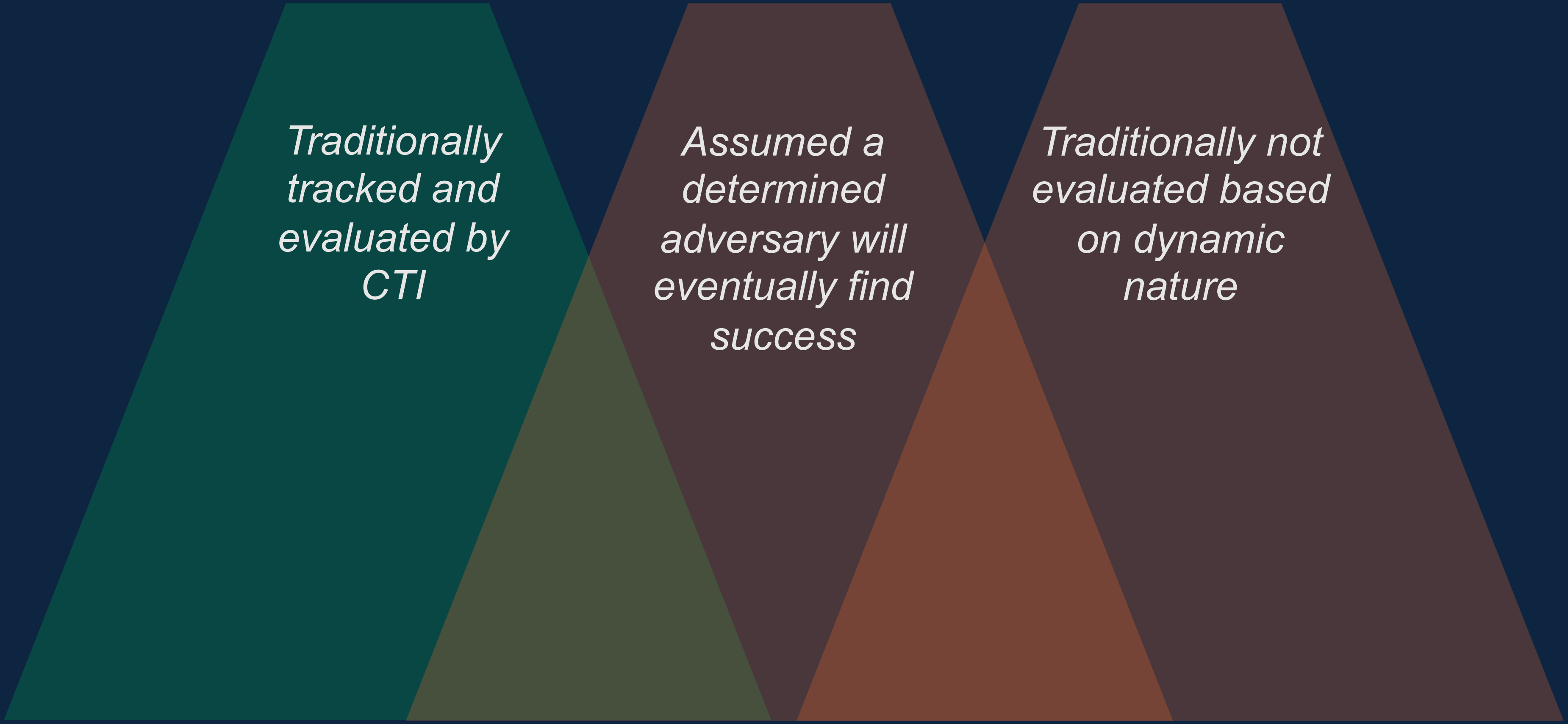
Not known if any malicious software was secreted onto EirGrid's control systems

MITRE

Risk = Probability x Impact

Traditional Cyber Threat Analysis

Threat = Capability x Opportunity x Motivation



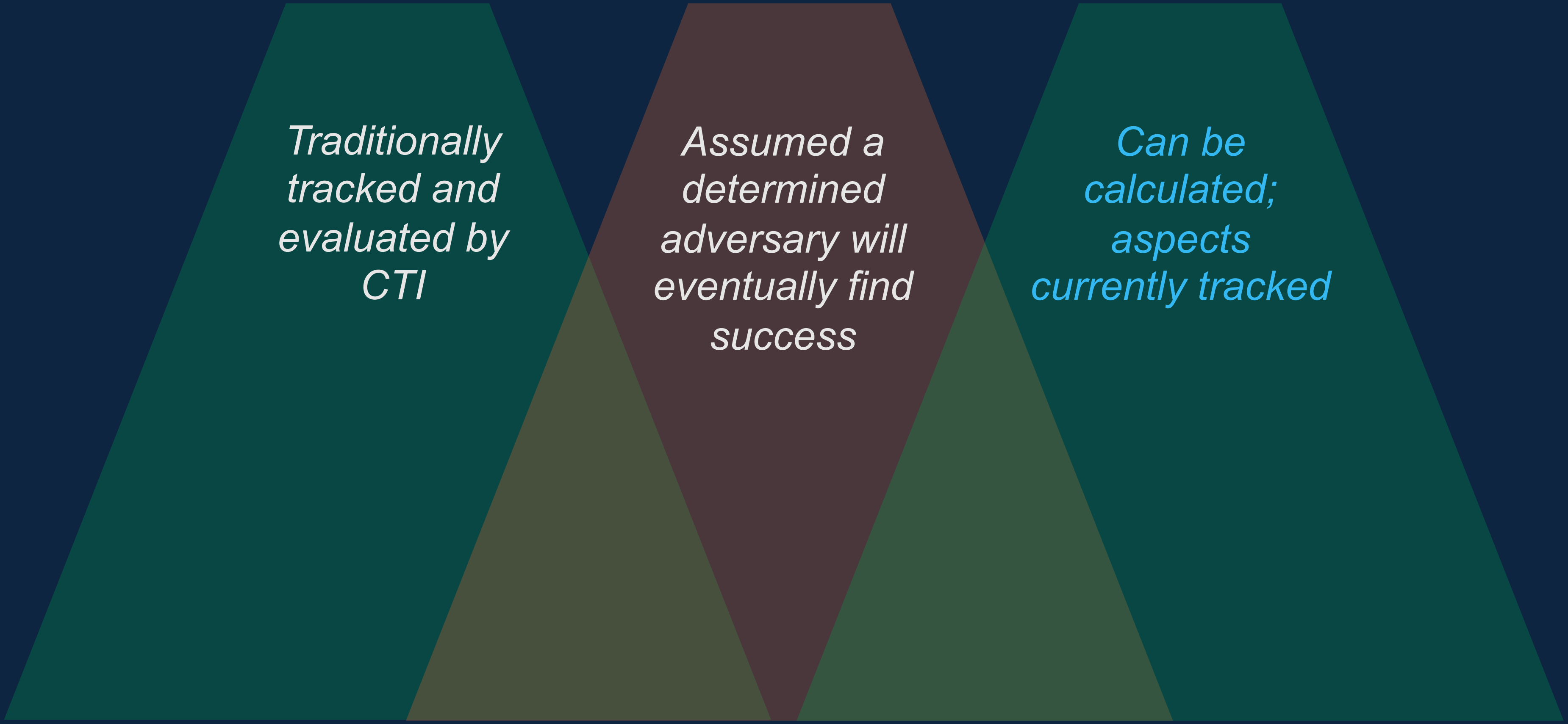
Traditionally tracked and evaluated by CTI

Assumed a determined adversary will eventually find success

Traditionally not evaluated based on dynamic nature

Traditional Cyber Threat Analysis

Threat = Capability x Opportunity x Motivation

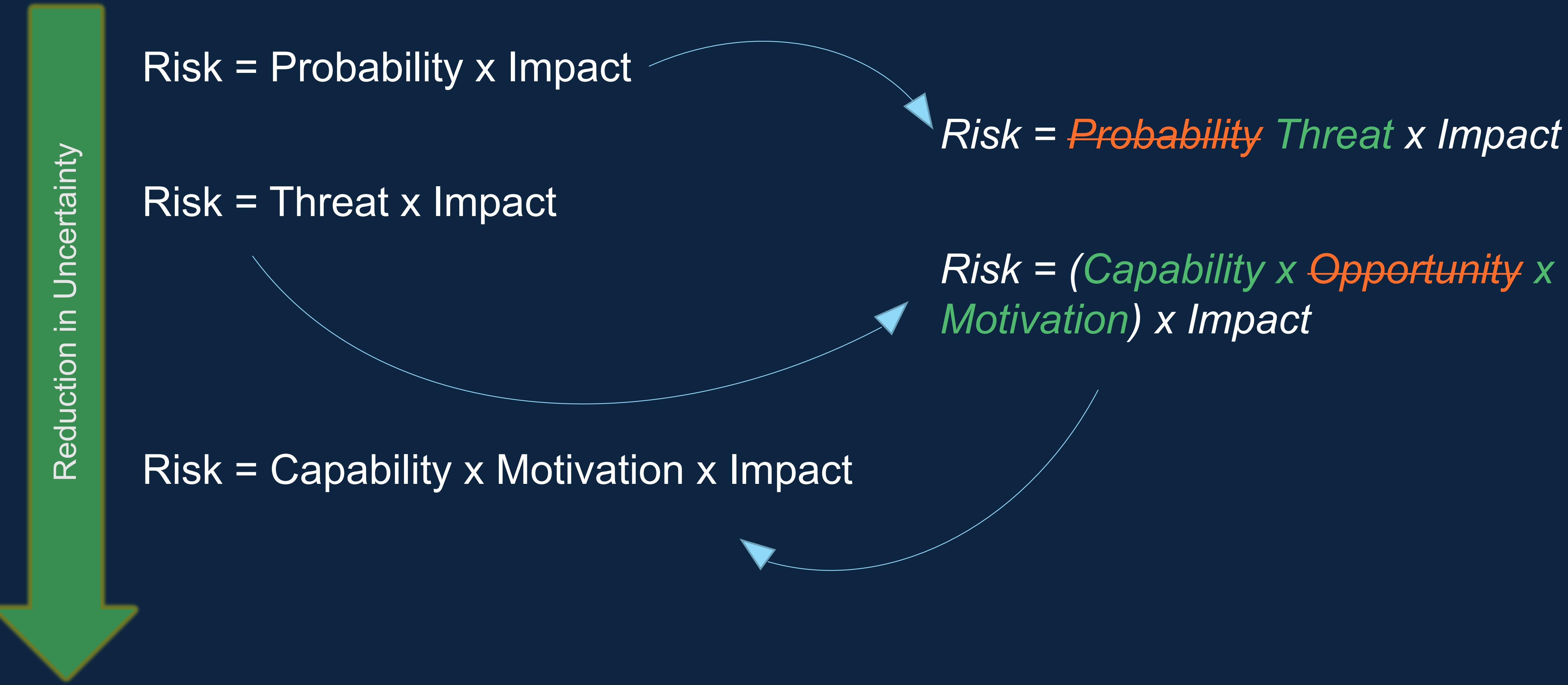


Traditionally tracked and evaluated by CTI

Assumed a determined adversary will eventually find success

Can be calculated; aspects currently tracked

Measuring Risk



Reduction in Uncertainty

Risk = Probability x Impact

Risk = ~~Probability~~ Threat x Impact

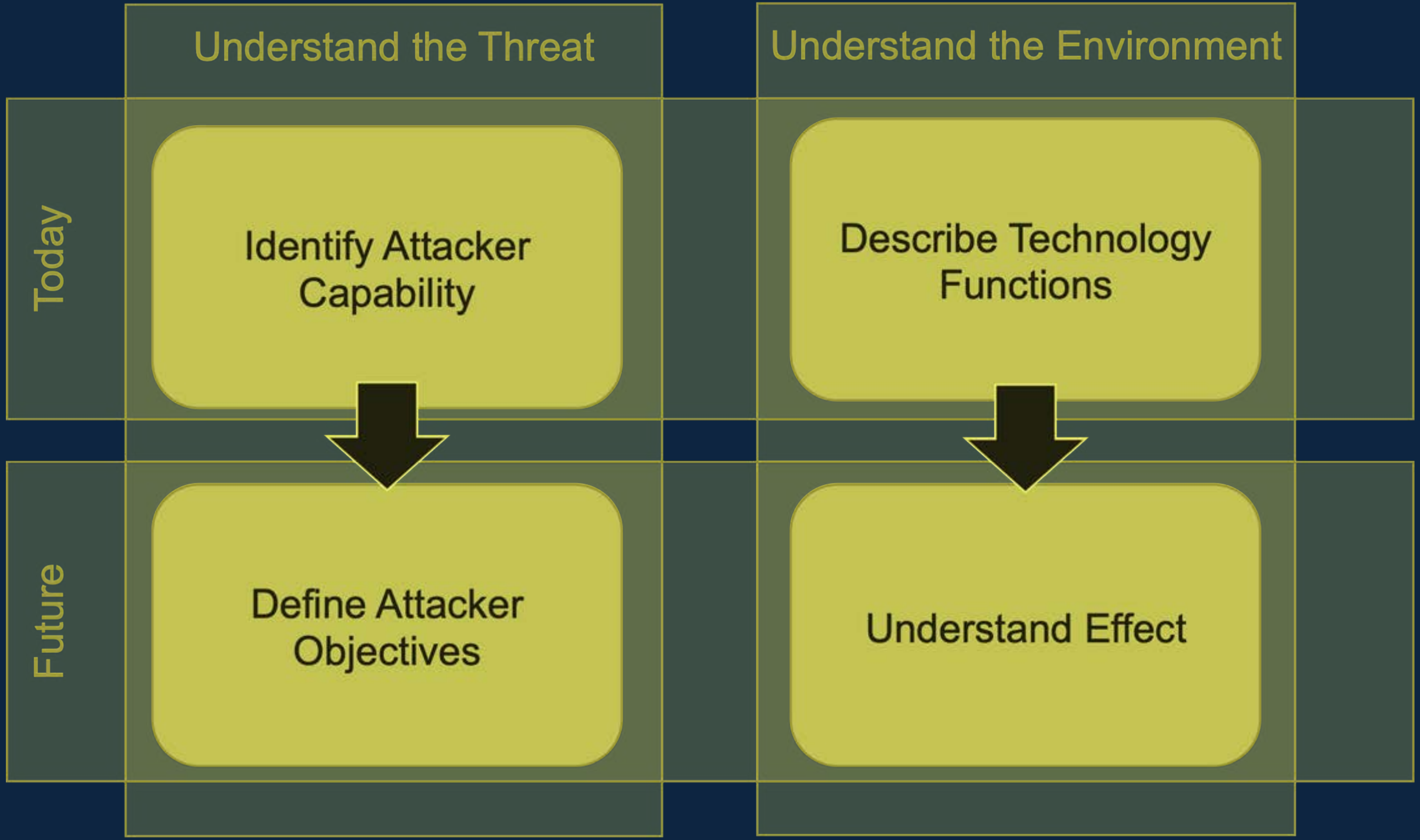
Risk = Threat x Impact

Risk = (Capability x ~~Opportunity~~ x Motivation) x Impact

Risk = Capability x Motivation x Impact

Infrastructure Susceptibility Analysis (ISA) Needs

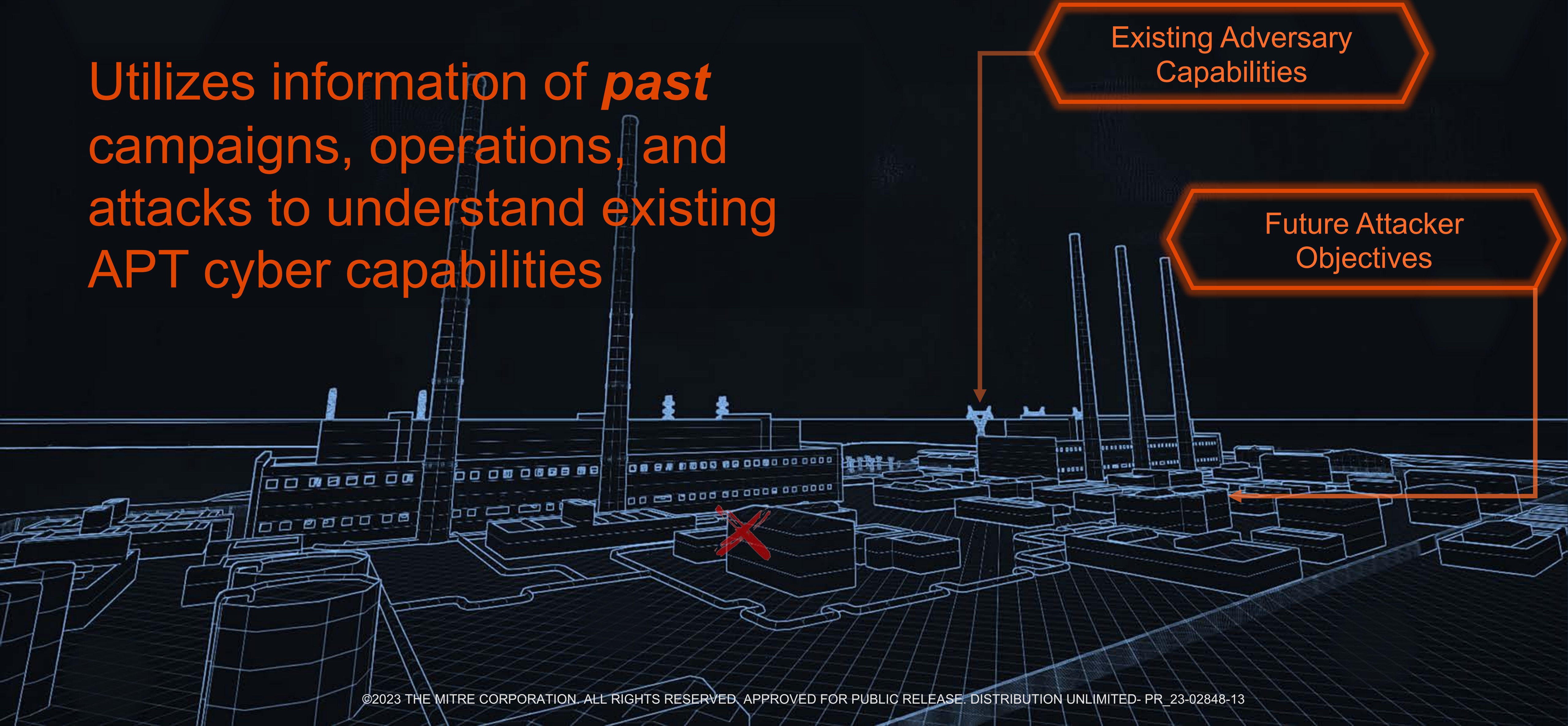
- Systematic, repeatable process
- Leverages cyber threat intelligence and technical targeting approaches
- Enables semi-quantitative analysis (limiting analytic bias)
- Seeks to better define adversary intentions and capabilities
- Identifies the most ***likely*** attacks, in addition to the most damaging


Understand the Threat
Understand the Environment
Today
Future
Identify Attacker Capability
Describe Technology Functions
Define Attacker Objectives
Understand Effect

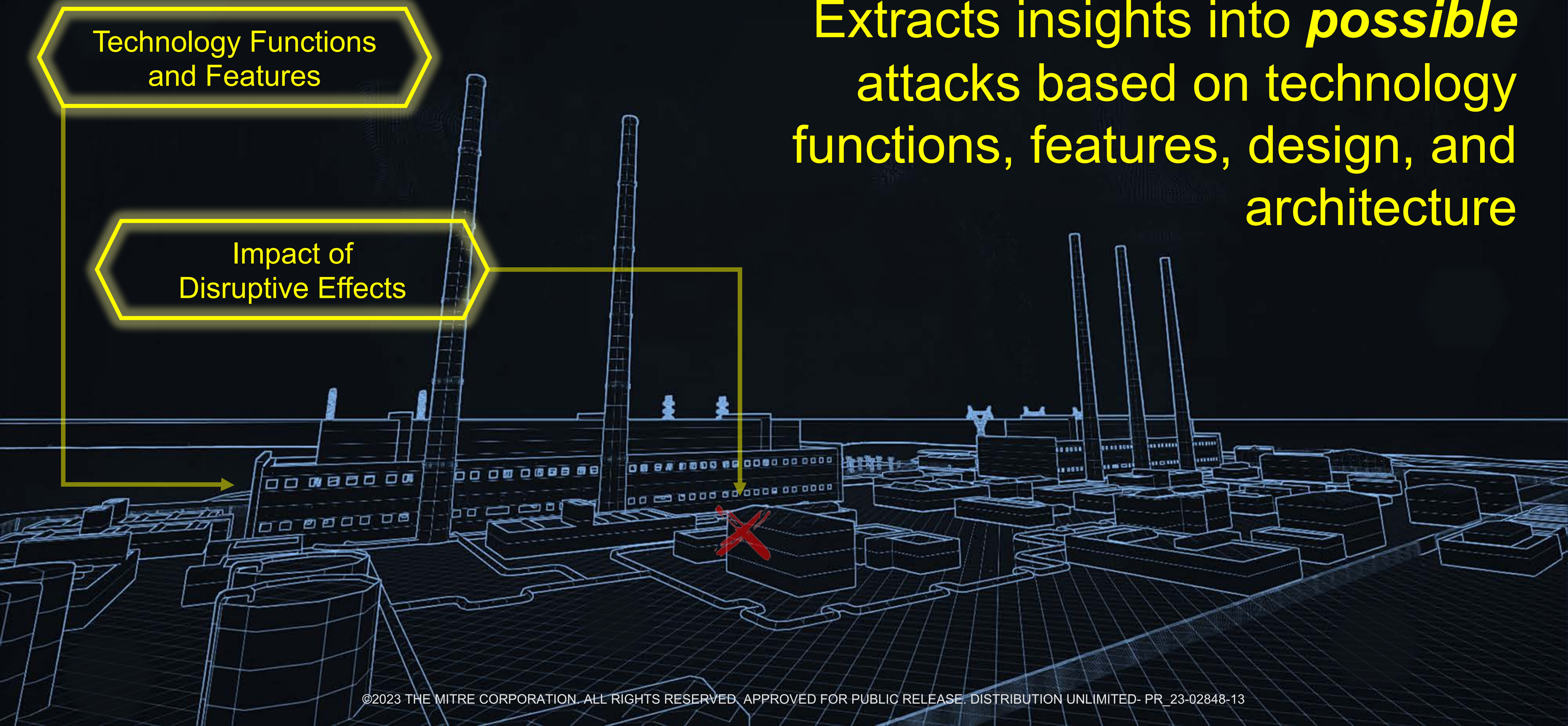
MITRE

Understand the Threat

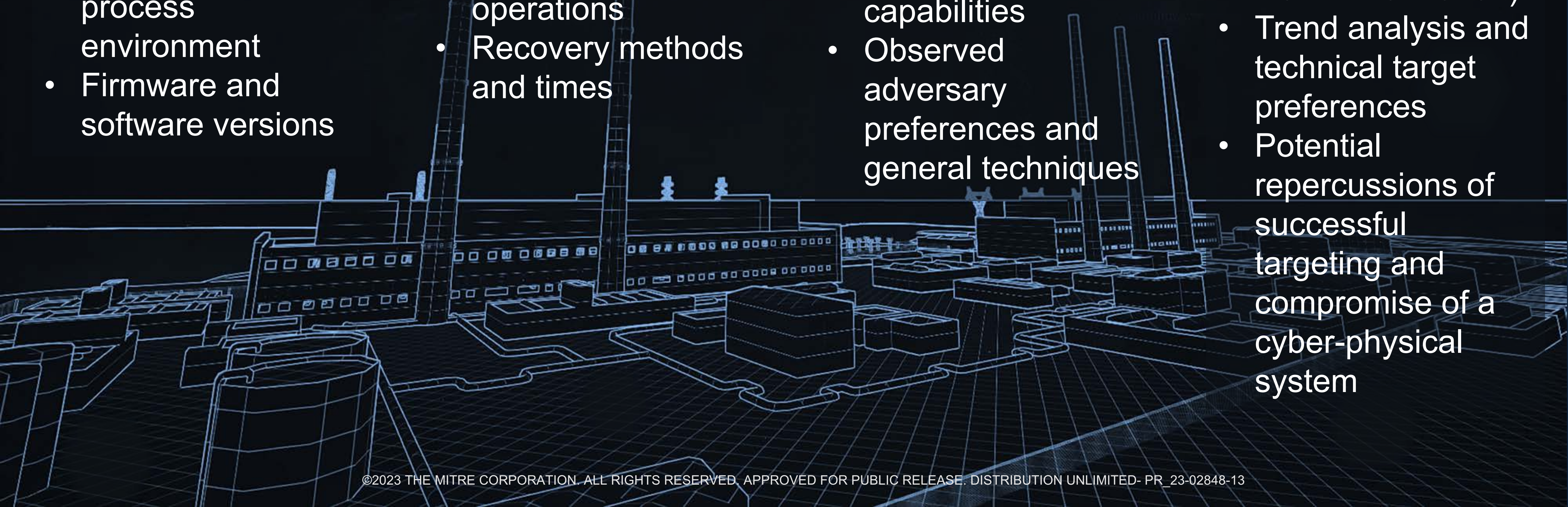
Utilizes information of ***past*** campaigns, operations, and attacks to understand existing APT cyber capabilities



Understand the Technology


Technology Functions and Features
Impact of Disruptive Effects

Extracts insights into ***possible*** attacks based on technology functions, features, design, and architecture



Technology Functions and Features

- Deployed hardware and software within an industrial or process environment
- Firmware and software versions

Impact of Disruptive Effects

- Details of past cyber incidents or system outages
- Impact to operations
- Recovery methods and times

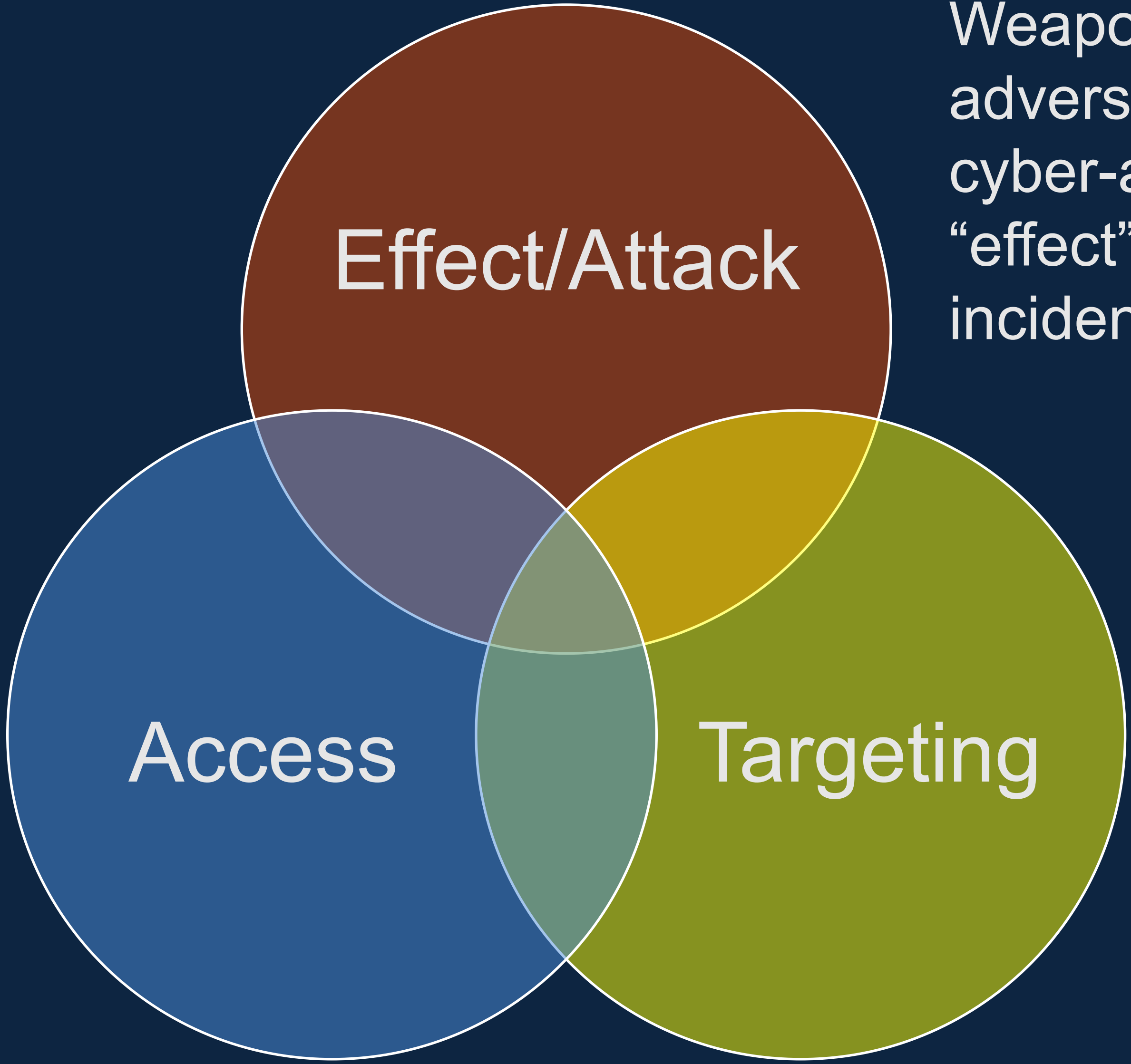
Existing Adversary Capabilities

- Demonstrated Stage I (access) and Stage II (effect) attack capabilities
- Observed adversary preferences and general techniques

Future Attacker Objectives

- Assessed adversary interest areas (collected victim information)
- Trend analysis and technical target preferences
- Potential repercussions of successful targeting and compromise of a cyber-physical system

Areas of Capability Sophistication



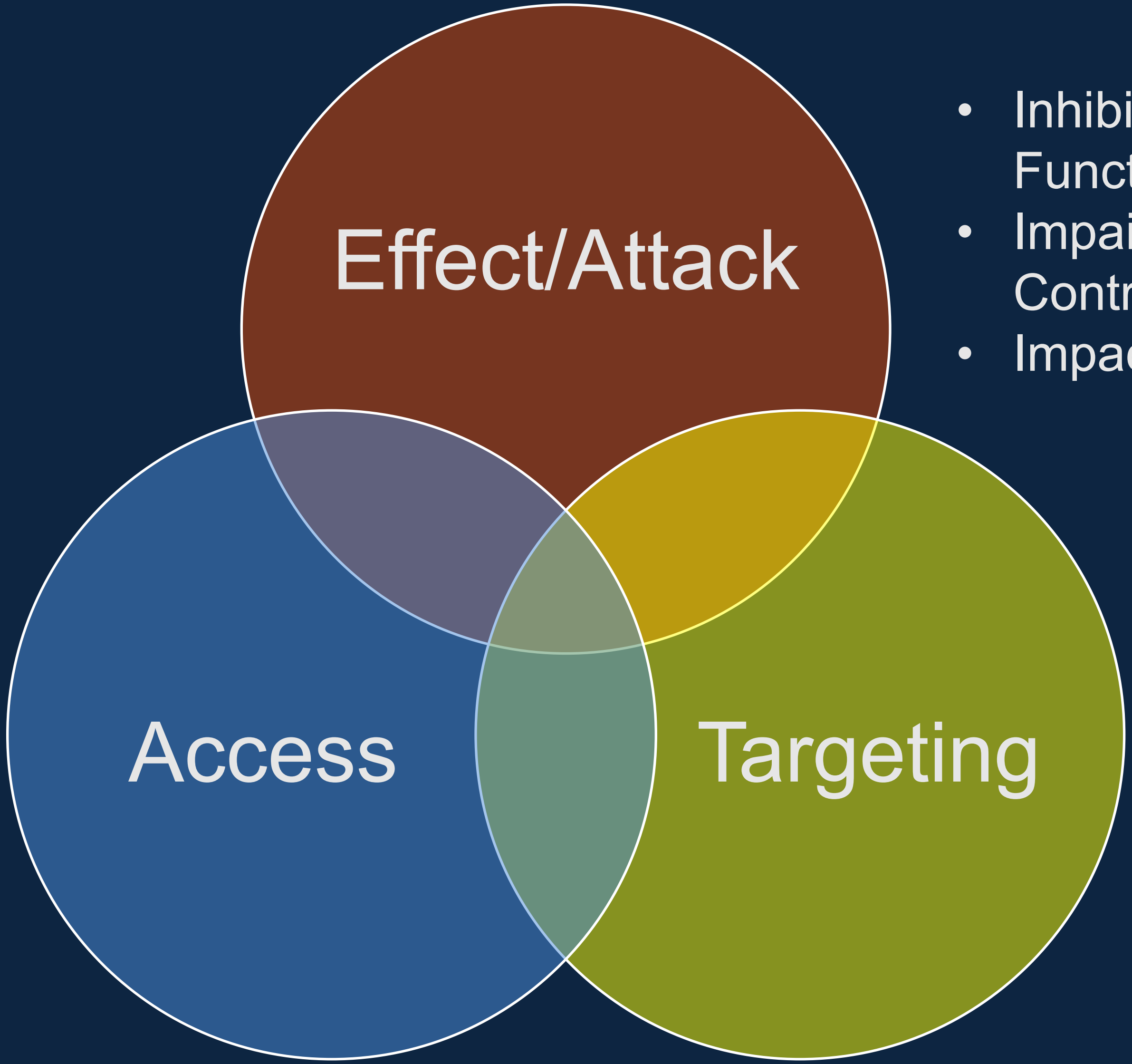
Weapons used by an adversary to conduct a cyber-attack. The end “effect” of a campaign or incident.

Adversary tools, techniques, and methods to gain access to the technical target of a cyber attack.

Tools and techniques leveraged by an adversary to gather the necessary information to support CNO.

MITRE

Sophistication Domains Mapped to ATT&CK for ICS Artifacts

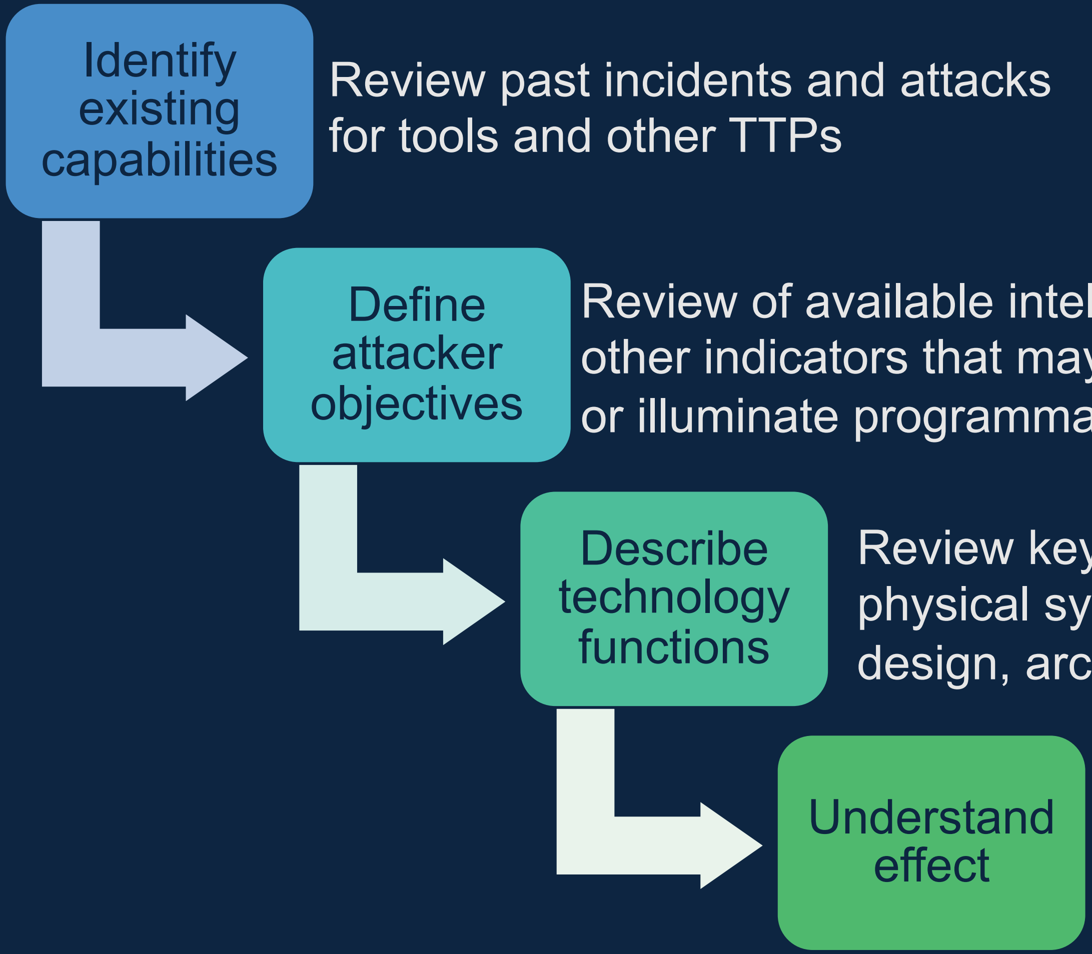


- Inhibit Response Function (TA0107)
- Impair Process Control (TA0106)
- Impact (TA0105)

- Initial Access (TA0108)
- Persistence (TA0110)
- Privilege Escalation (TA0111)
- Evasion (TA0103)
- Lateral Movement (TA0109)
- Command and Control (TA0101)

- Discovery (TA0102)
- Collection (TA0100)

ISA Process Overview – Threat-centric Approach



Identify existing capabilities

Review past incidents and attacks for tools and other TTPs

Define attacker objectives

Review of available intelligence or other indicators that may identify or illuminate programmatic goals

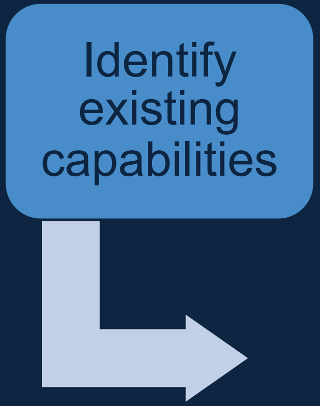
Describe technology functions

Review key technology/cyber-physical systems’ purpose, design, architecture

Understand effect

Define outcome given a system failure or loss of availability

ISA Process Overview – Threat-centric Approach



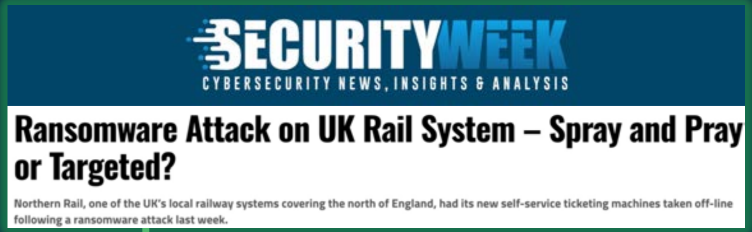
Identify existing capabilities

Review past incidents and attacks for tools and other TTPs

Key Questions:

- *What technical effects/capabilities have been demonstrated against real-world victims (both Stage I and Stage II)?*
- *What vulnerabilities/CVEs are leveraged by the attackers?*
- *What was the result of these access campaigns or attacks?*
- *Etc.*

Rail Example: Major Incidents and Cyber Attacks

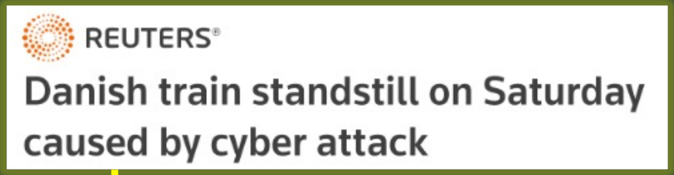


SECURITYWEEK
CYBERSECURITY NEWS, INSIGHTS & ANALYSIS

Ransomware Attack on UK Rail System – Spray and Pray or Targeted?

Northern Rail, one of the UK's local railway systems covering the north of England, had its new self-service ticketing machines taken off-line following a ransomware attack last week.

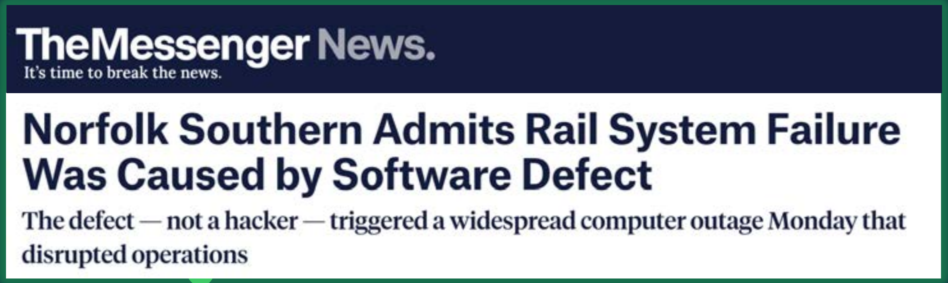
2021
UK



REUTERS®

Danish train standstill on Saturday caused by cyber attack

2022
Denmark

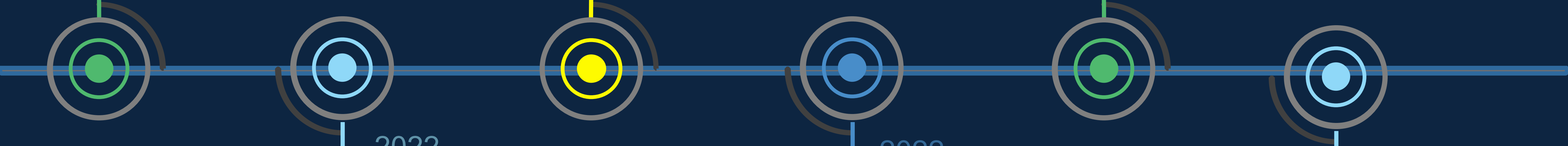


TheMessenger News.
It's time to break the news.

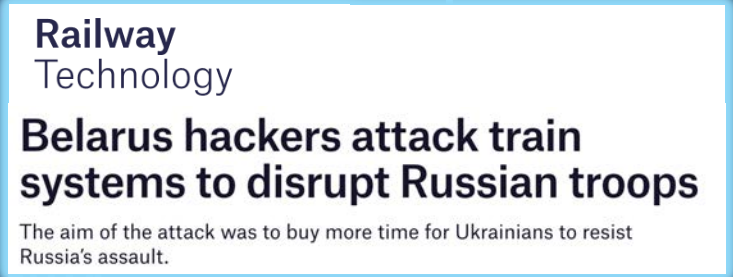
Norfolk Southern Admits Rail System Failure Was Caused by Software Defect

The defect — not a hacker — triggered a widespread computer outage Monday that disrupted operations

2023
US



2022
Belarus

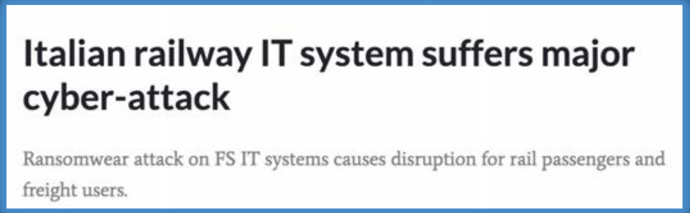


Railway
Technology

Belarus hackers attack train systems to disrupt Russian troops

The aim of the attack was to buy more time for Ukrainians to resist Russia's assault.

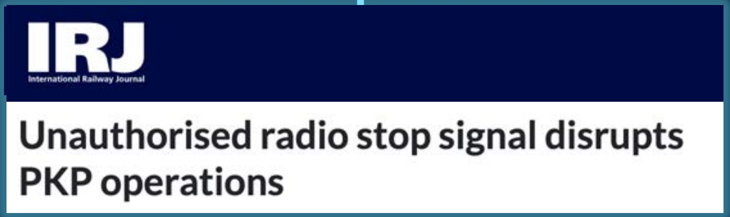
2022
Italy



Italian railway IT system suffers major cyber-attack

Ransomwear attack on FS IT systems causes disruption for rail passengers and freight users.

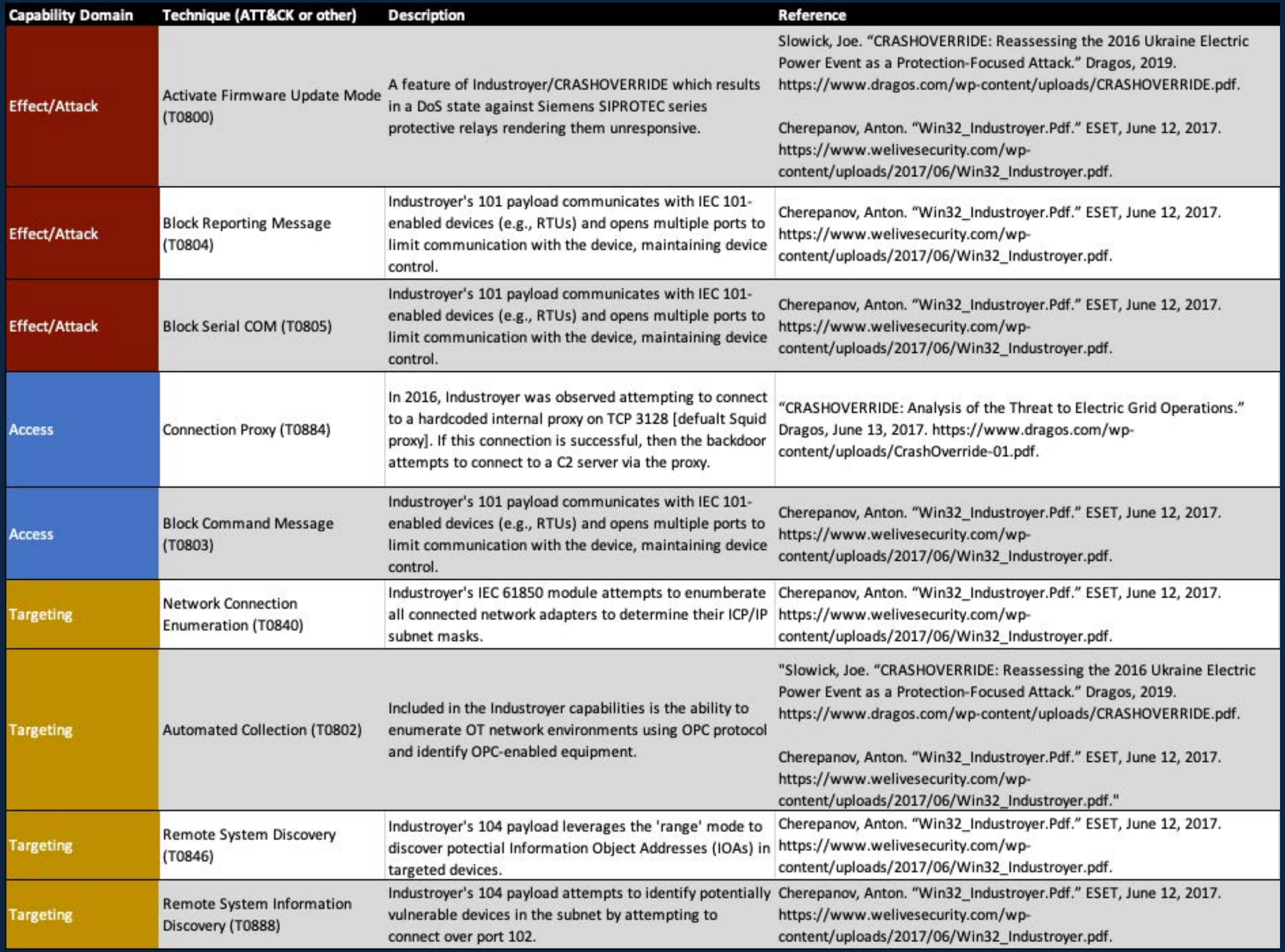
2023
Poland



IRJ
International Railway Journal

Unauthorised radio stop signal disrupts PKP operations

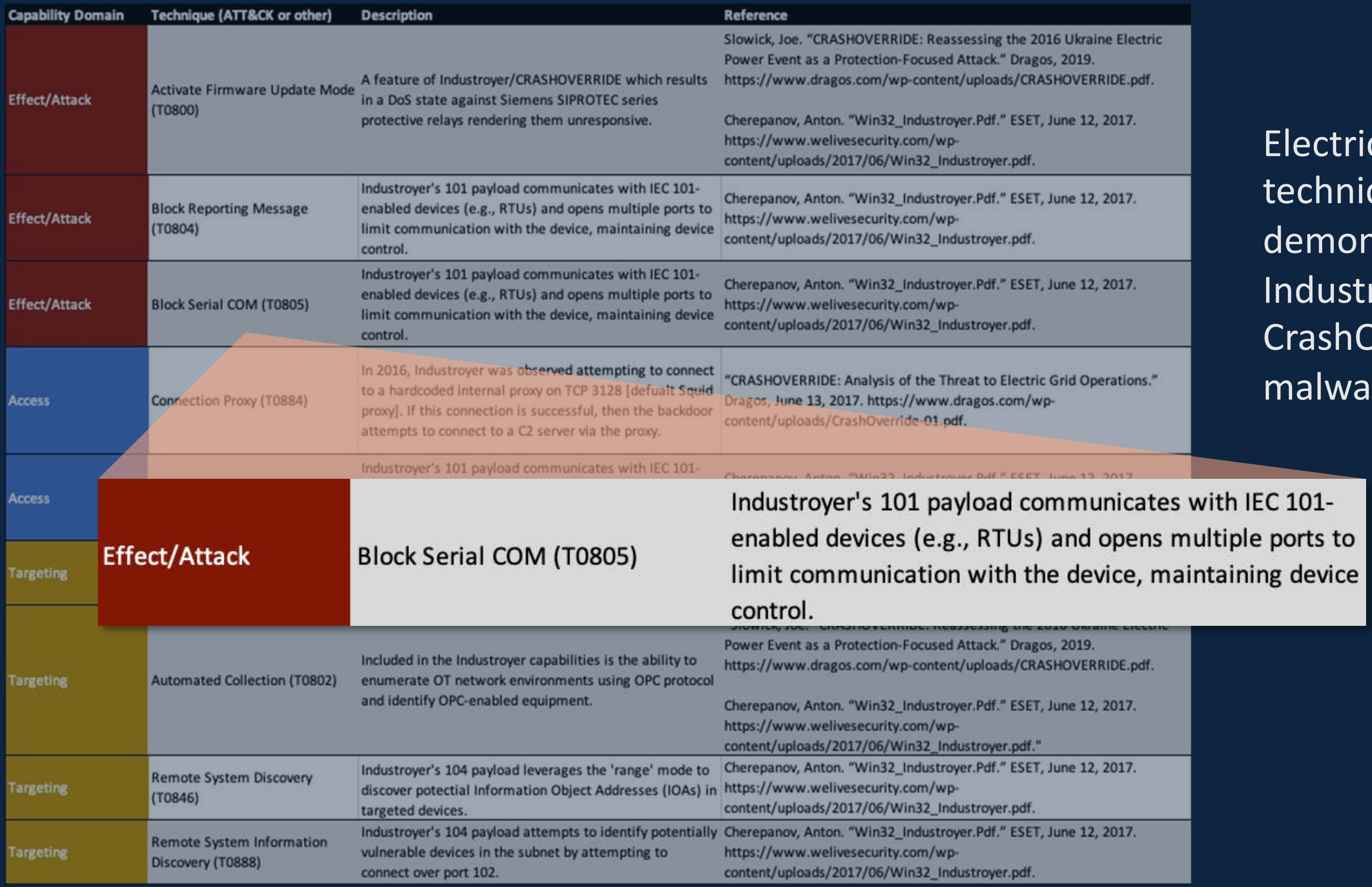
Identify Existing Capabilities



Capability Domain	Technique (ATT&CK or other)	Description	Reference
Effect/Attack	Activate Firmware Update Mode (T0800)	A feature of Industroyer/CRASHOVERRIDE which results in a DoS state against Siemens SIPROTEC series protective relays rendering them unresponsive.	Slowick, Joe. "CRASHOVERRIDE: Reassessing the 2016 Ukraine Electric Power Event as a Protection-Focused Attack." Dragos, 2019. https://www.dragos.com/wp-content/uploads/CRASHOVERRIDE.pdf. Cherepanov, Anton. "Win32_Industroyer.Pdf." ESET, June 12, 2017. https://www.welivesecurity.com/wp-content/uploads/2017/06/Win32_Industroyer.pdf.
Effect/Attack	Block Reporting Message (T0804)	Industroyer's 101 payload communicates with IEC 101-enabled devices (e.g., RTUs) and opens multiple ports to limit communication with the device, maintaining device control.	Cherepanov, Anton. "Win32_Industroyer.Pdf." ESET, June 12, 2017. https://www.welivesecurity.com/wp-content/uploads/2017/06/Win32_Industroyer.pdf.
Effect/Attack	Block Serial COM (T0805)	Industroyer's 101 payload communicates with IEC 101-enabled devices (e.g., RTUs) and opens multiple ports to limit communication with the device, maintaining device control.	Cherepanov, Anton. "Win32_Industroyer.Pdf." ESET, June 12, 2017. https://www.welivesecurity.com/wp-content/uploads/2017/06/Win32_Industroyer.pdf.
Access	Connection Proxy (T0884)	In 2016, Industroyer was observed attempting to connect to a hardcoded internal proxy on TCP 3128 [defualt Squid proxy]. If this connection is successful, then the backdoor attempts to connect to a C2 server via the proxy.	"CRASHOVERRIDE: Analysis of the Threat to Electric Grid Operations." Dragos, June 13, 2017. https://www.dragos.com/wp-content/uploads/CrashOverride-01.pdf.
Access	Block Command Message (T0803)	Industroyer's 101 payload communicates with IEC 101-enabled devices (e.g., RTUs) and opens multiple ports to limit communication with the device, maintaining device control.	Cherepanov, Anton. "Win32_Industroyer.Pdf." ESET, June 12, 2017. https://www.welivesecurity.com/wp-content/uploads/2017/06/Win32_Industroyer.pdf.
Targeting	Network Connection Enumeration (T0840)	Industroyer's IEC 61850 module attempts to enumberate all connected network adapters to determine their ICP/IP subnet masks.	Cherepanov, Anton. "Win32_Industroyer.Pdf." ESET, June 12, 2017. https://www.welivesecurity.com/wp-content/uploads/2017/06/Win32_Industroyer.pdf.
Targeting	Automated Collection (T0802)	Included in the Industroyer capabilities is the ability to enumerate OT network environments using OPC protocol and identify OPC-enabled equipment.	"Slowick, Joe. "CRASHOVERRIDE: Reassessing the 2016 Ukraine Electric Power Event as a Protection-Focused Attack." Dragos, 2019. https://www.dragos.com/wp-content/uploads/CRASHOVERRIDE.pdf. Cherepanov, Anton. "Win32_Industroyer.Pdf." ESET, June 12, 2017. https://www.welivesecurity.com/wp-content/uploads/2017/06/Win32_Industroyer.pdf."
Targeting	Remote System Discovery (T0846)	Industroyer's 104 payload leverages the 'range' mode to discover potectial Information Object Addresses (IOAs) in targeted devices.	Cherepanov, Anton. "Win32_Industroyer.Pdf." ESET, June 12, 2017. https://www.welivesecurity.com/wp-content/uploads/2017/06/Win32_Industroyer.pdf.
Targeting	Remote System Information Discovery (T0888)	Industroyer's 104 payload attempts to identify potentially vulnerable devices in the subnet by attempting to connect over port 102.	Cherepanov, Anton. "Win32_Industroyer.Pdf." ESET, June 12, 2017. https://www.welivesecurity.com/wp-content/uploads/2017/06/Win32_Industroyer.pdf.

Electric grid techniques demonstrated by Industroyer/ CrashOverride malware (2016)

Identify Existing Capabilities



Capability Domain	Technique (ATT&CK or other)	Description	Reference
Effect/Attack	Activate Firmware Update Mode (T0800)	A feature of Industroyer/CRASHOVERRIDE which results in a DoS state against Siemens SIPROTEC series protective relays rendering them unresponsive.	Slowick, Joe. "CRASHOVERRIDE: Reassessing the 2016 Ukraine Electric Power Event as a Protection-Focused Attack." Dragos, 2019. https://www.dragos.com/wp-content/uploads/CRASHOVERRIDE.pdf. Cherepanov, Anton. "Win32_Industroyer.Pdf." ESET, June 12, 2017. https://www.welivesecurity.com/wp-content/uploads/2017/06/Win32_Industroyer.pdf.
Effect/Attack	Block Reporting Message (T0804)	Industroyer's 101 payload communicates with IEC 101-enabled devices (e.g., RTUs) and opens multiple ports to limit communication with the device, maintaining device control.	Cherepanov, Anton. "Win32_Industroyer.Pdf." ESET, June 12, 2017. https://www.welivesecurity.com/wp-content/uploads/2017/06/Win32_Industroyer.pdf.
Effect/Attack	Block Serial COM (T0805)	Industroyer's 101 payload communicates with IEC 101-enabled devices (e.g., RTUs) and opens multiple ports to limit communication with the device, maintaining device control.	Cherepanov, Anton. "Win32_Industroyer.Pdf." ESET, June 12, 2017. https://www.welivesecurity.com/wp-content/uploads/2017/06/Win32_Industroyer.pdf.
Access	Connection Proxy (T0884)	In 2016, Industroyer was observed attempting to connect to a hardcoded internal proxy on TCP 3128 [defualt Squid proxy]. If this connection is successful, then the backdoor attempts to connect to a C2 server via the proxy.	"CRASHOVERRIDE: Analysis of the Threat to Electric Grid Operations." Dragos, June 13, 2017. https://www.dragos.com/wp-content/uploads/CrashOverride-01.pdf.
Access		Industroyer's 101 payload communicates with IEC 101-	Cherepanov, Anton. "Win32_Industroyer.Pdf." ESET, June 12, 2017.
Targeting			
Targeting	Automated Collection (T0802)	Included in the Industroyer capabilities is the ability to enumerate OT network environments using OPC protocol and identify OPC-enabled equipment.	Slowick, Joe. "CRASHOVERRIDE: Reassessing the 2016 Ukraine Electric Power Event as a Protection-Focused Attack." Dragos, 2019. https://www.dragos.com/wp-content/uploads/CRASHOVERRIDE.pdf. Cherepanov, Anton. "Win32_Industroyer.Pdf." ESET, June 12, 2017. https://www.welivesecurity.com/wp-content/uploads/2017/06/Win32_Industroyer.pdf."
Targeting	Remote System Discovery (T0846)	Industroyer's 104 payload leverages the 'range' mode to discover potectial Information Object Addresses (IOAs) in targeted devices.	Cherepanov, Anton. "Win32_Industroyer.Pdf." ESET, June 12, 2017. https://www.welivesecurity.com/wp-content/uploads/2017/06/Win32_Industroyer.pdf.
Targeting	Remote System Information Discovery (T0888)	Industroyer's 104 payload attempts to identify potentially vulnerable devices in the subnet by attempting to connect over port 102.	Cherepanov, Anton. "Win32_Industroyer.Pdf." ESET, June 12, 2017. https://www.welivesecurity.com/wp-content/uploads/2017/06/Win32_Industroyer.pdf.

Effect/Attack	Block Serial COM (T0805)	Industroyer's 101 payload communicates with IEC 101-enabled devices (e.g., RTUs) and opens multiple ports to limit communication with the device, maintaining device control.

Electric grid techniques demonstrated by Industroyer/ CrashOverride malware (2016)

MITRE

ISA Process Overview – Threat-centric Approach

Define attacker objectives

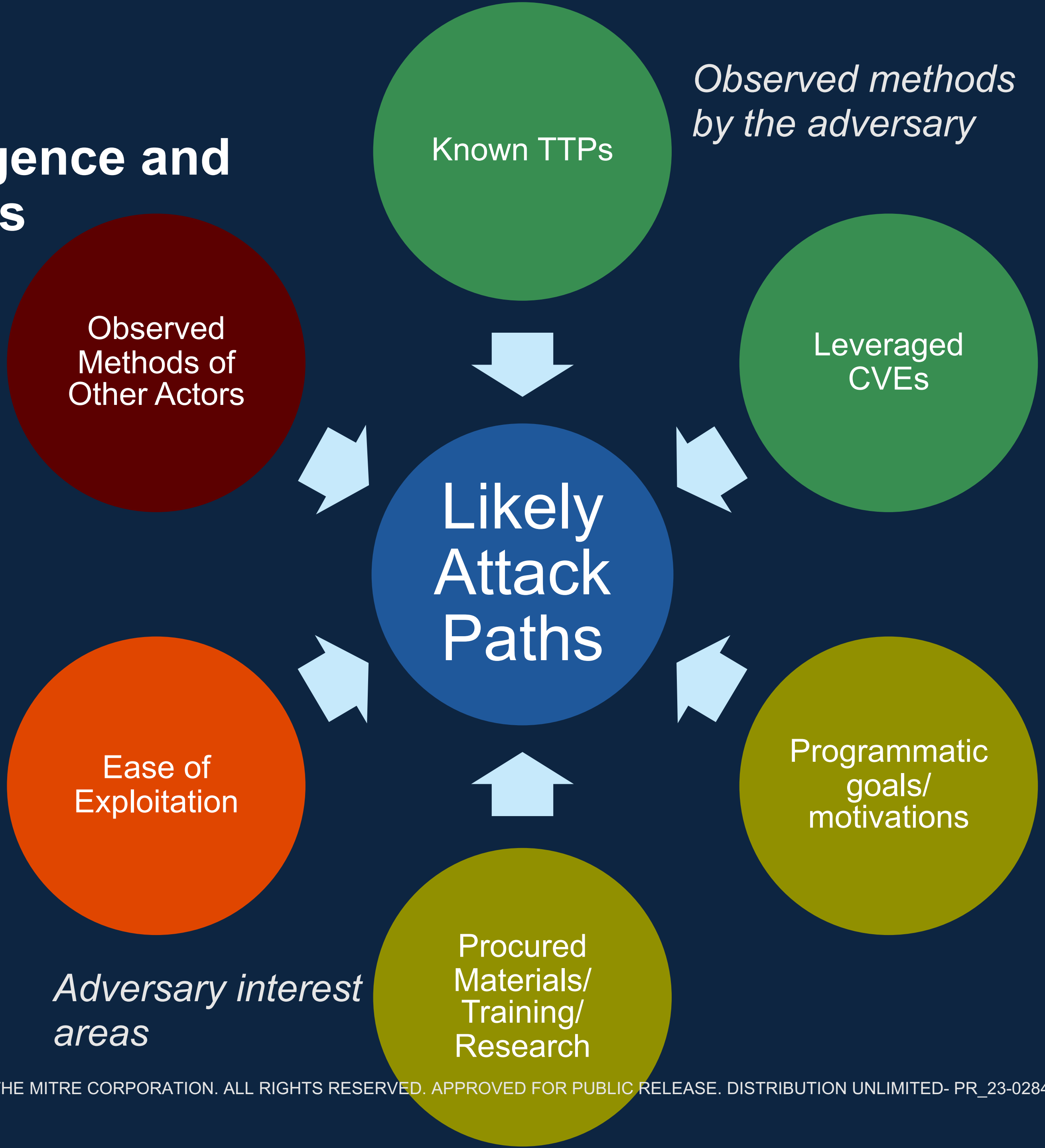
Review of available intelligence or other indicators that may identify or illuminate programmatic goals

Key Questions:

- *Are actors pursuing capabilities against a given sector or technology?*
- *In what sectors is that equipment commonly deployed (e.g., market share by sector or subsector)?*
- *In what countries/regions/companies is that equipment commonly deployed (e.g., market share by region)?*
- *What training have the threat actor pursued?*
- *What are the programmatic goals for groups which are state sponsored?*
- *Etc.*

ISA Inputs

Leveraged Intelligence and Confidence Levels



Likely Attack Paths

Known TTPs

Observed methods by the adversary

Leveraged CVEs

Observed exploitation of adversary vulns

Programmatic goals/ motivations

Information regarding intended effects or consequences of sponsored programs

Procured Materials/ Training/ Research

Adversary interest areas

Ease of Exploitation

Relative difficulty of attack scenario

Observed Methods of Other Actors

Attack scenario leverages third-party TTPs

Confidence Key

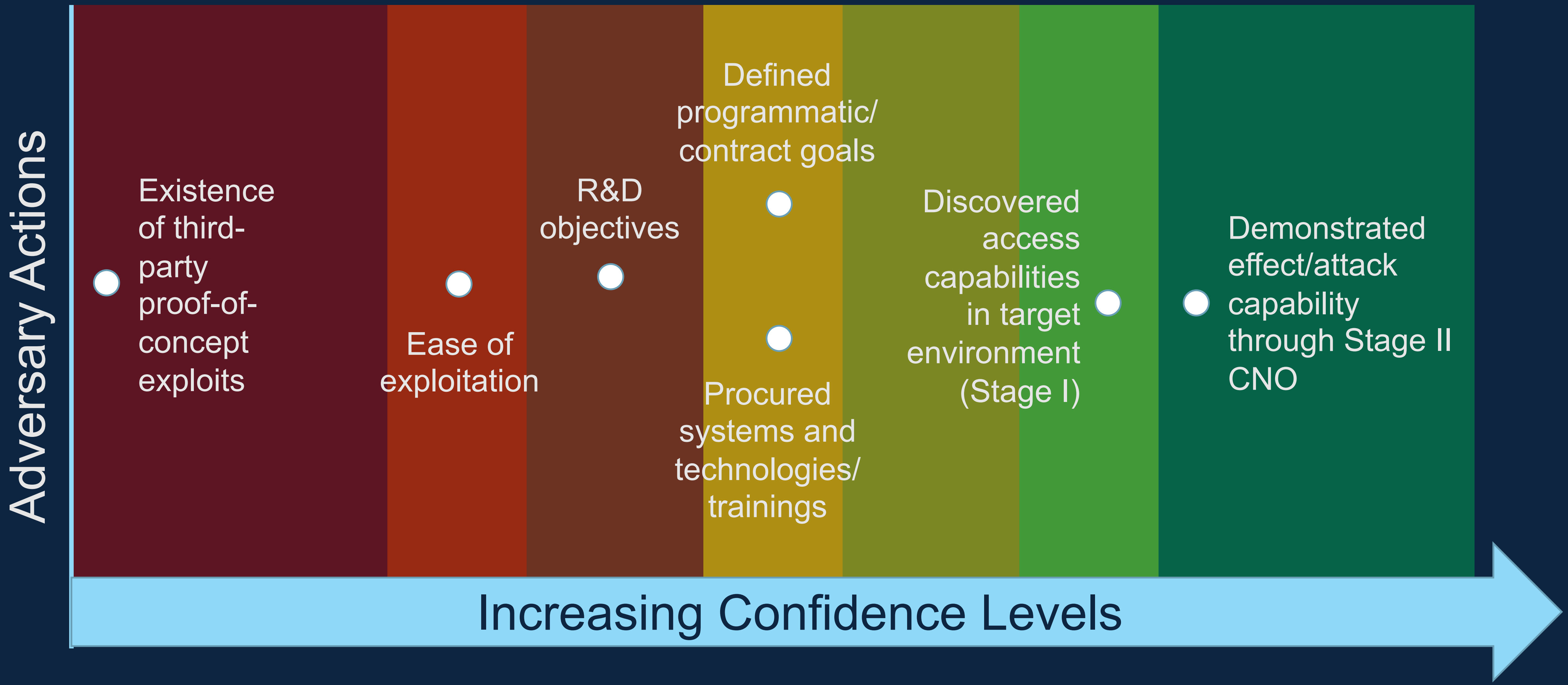
Green – high confidence

Yellow – medium confidence

Orange – medium/low confidence

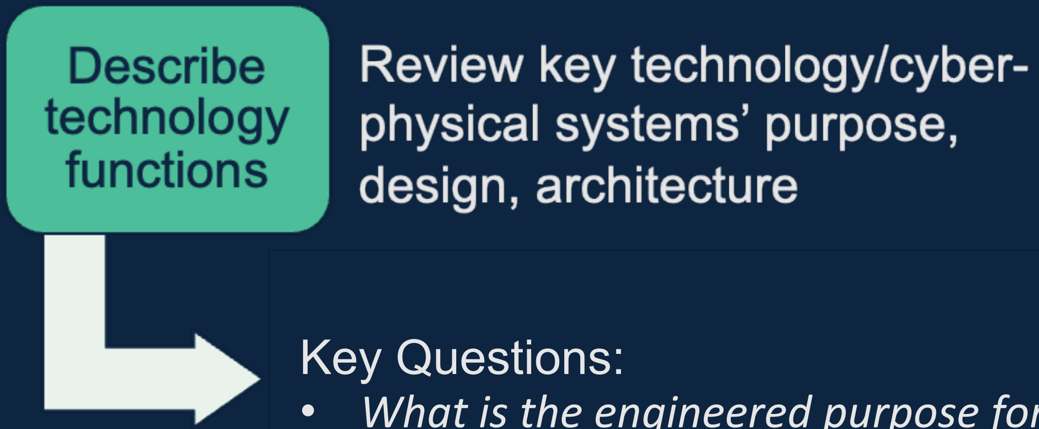
Red – low confidence

Defining Adversary Intention



Adversary Actions
Existence of third-party proof-of-concept exploits
Ease of exploitation
R&D objectives
Defined programmatic/ contract goals
Procured systems and technologies/ trainings
Discovered access capabilities in target environment (Stage I)
Demonstrated effect/attack capability through Stage II CNO
Increasing Confidence Levels

ISA Process Overview – Threat-centric Approach



Describe technology functions

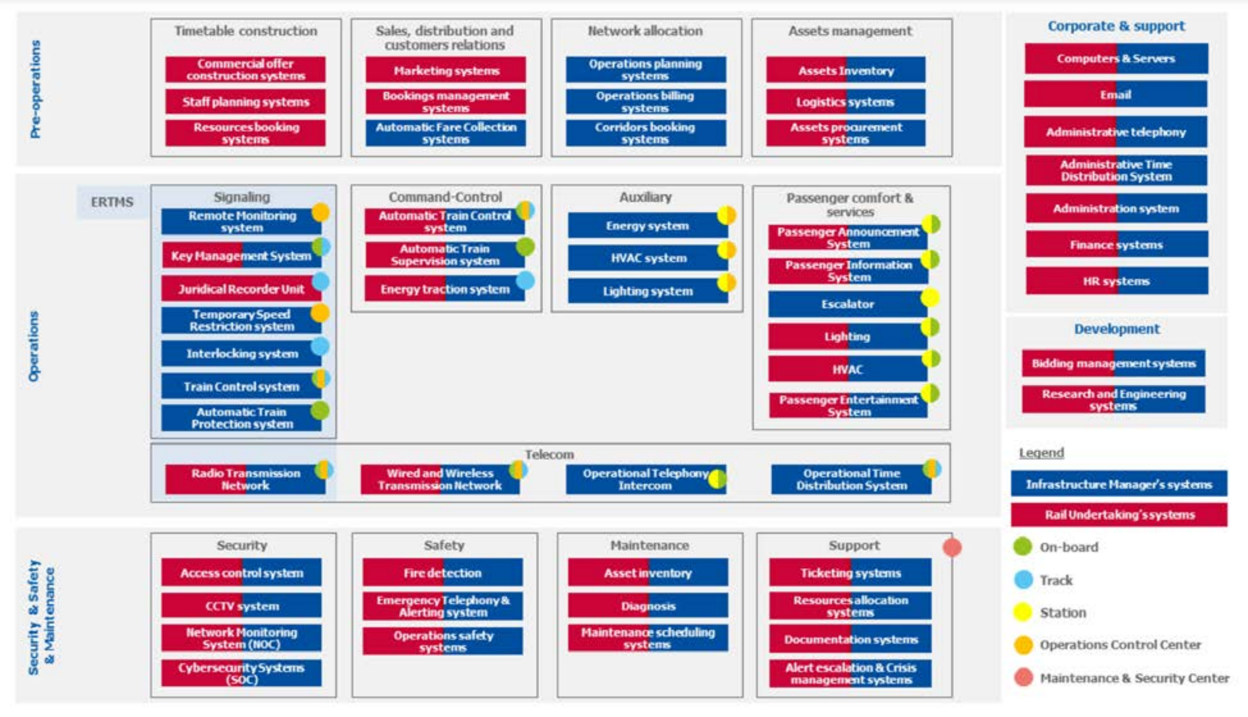
Review key technology/cyber-physical systems' purpose, design, architecture

Key Questions:

- *What is the engineered purpose for a given cyber-physical system (CPS)?*
- *How is a CPS designed, deployed, commissioned, and maintained throughout its lifecycle?*
- *Who are the key players/organizations throughout a CPS lifecycle?*
- *Given a desired outcome, what are the necessary technical targets for an attack?*
- *Etc.*

Function Models and Taxonomies within the Rail Sector

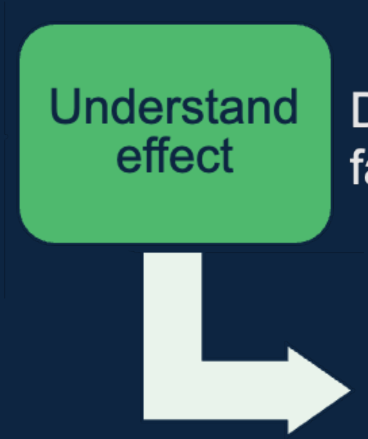
- Past work has identified core functions of rail sector
    - Models are typically high-level and not technology-based
    - More detailed technology-based approaches are limited
- Variation in tech by region and country
- Technology trends influence security
    - Many rail operators are increasingly reliant on digital technologies for normal operation
    - Results → a larger attack surface for adversaries and reduces the need for CPS specialists



Pre-operations
Timetable construction
Commercial offer construction systems
Staff planning systems
Resources booking systems
Sales, distribution and customers relations
Marketing systems
Bookings management systems
Automatic Fare Collection systems
Network allocation
Operations planning systems
Operations billing systems
Corridors booking systems
Assets management
Assets Inventory
Logistics systems
Assets procurement systems
Corporate & support
Computers & Servers
Email
Administrative telephony
Administrative Time Distribution System
Administration system
Finance systems
HR systems
Operations
ERTMS
Signaling
Remote Monitoring system
Key Management System
Juridical Recorder Unit
Temporary Speed Restriction system
Interlocking system
Train Control system
Automatic Train Protection system
Command-Control
Automatic Train Control system
Automatic Train Supervision system
Energy traction system
Auxiliary
Energy system
HVAC system
Lighting system
Passenger comfort & services
Passenger Announcement System
Passenger Information System
Escalator
Lighting
HVAC
Passenger Entertainment System
Development
Bidding management systems
Research and Engineering systems
Telecom
Radio Transmission Network
Wired and Wireless Transmission Network
Operational Telephony Intercom
Operational Time Distribution System
Security & Safety & Maintenance
Security
Access control system
CCTV system
Network Monitoring System (NOC)
Cybersecurity Systems (SOC)
Safety
Fire detection
Emergency Telephony & Alerting system
Operations safety systems
Maintenance
Asset inventory
Diagnosis
Maintenance scheduling systems
Support
Ticketing systems
Resources allocation systems
Documentation systems
Alert escalation & Crisis management systems
Legend
Infrastructure Manager's systems
Rail Undertaking's systems
On-board
Track
Station
Operations Control Center
Maintenance & Security Center

Typical Rail Functions and Operations (ENISA) (2020)

ISA Process Overview – Threat-centric Approach

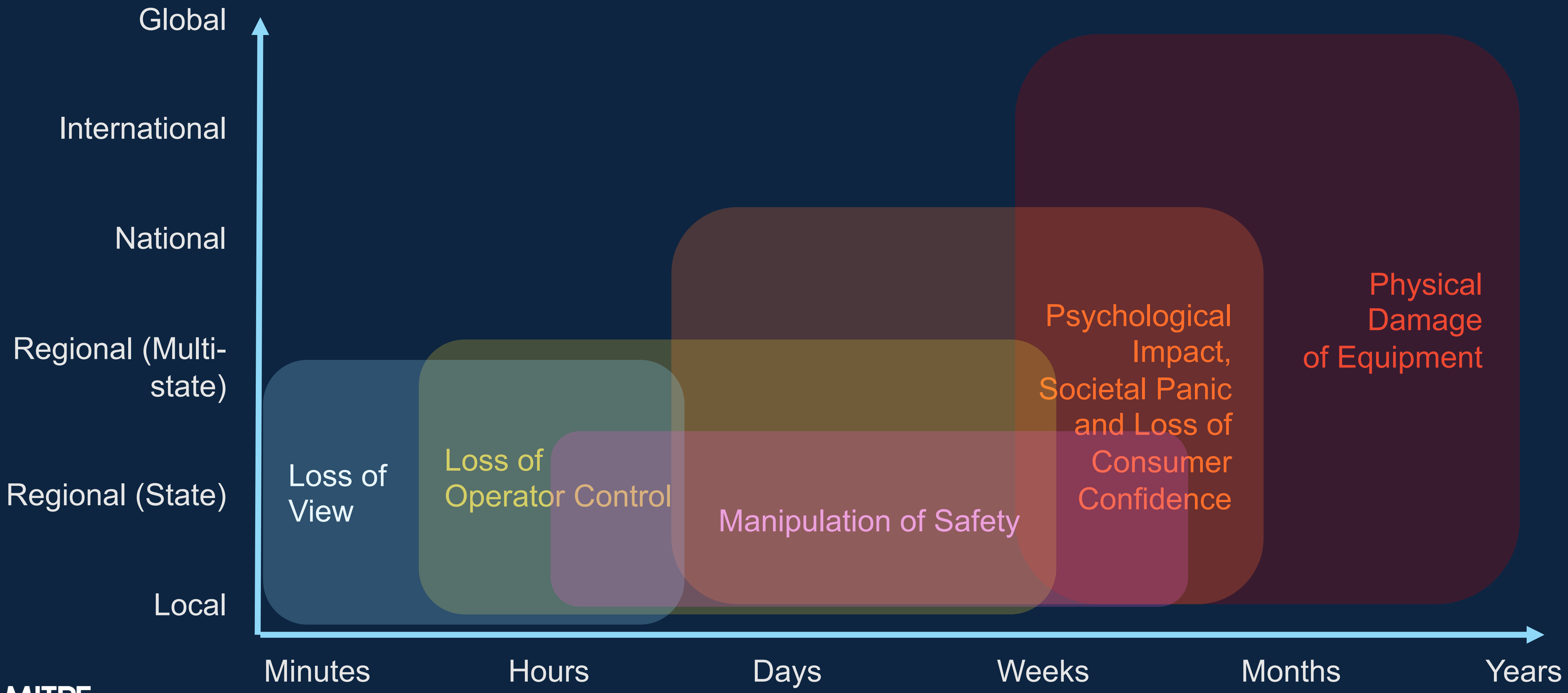


Define outcome given a system failure or loss of availability

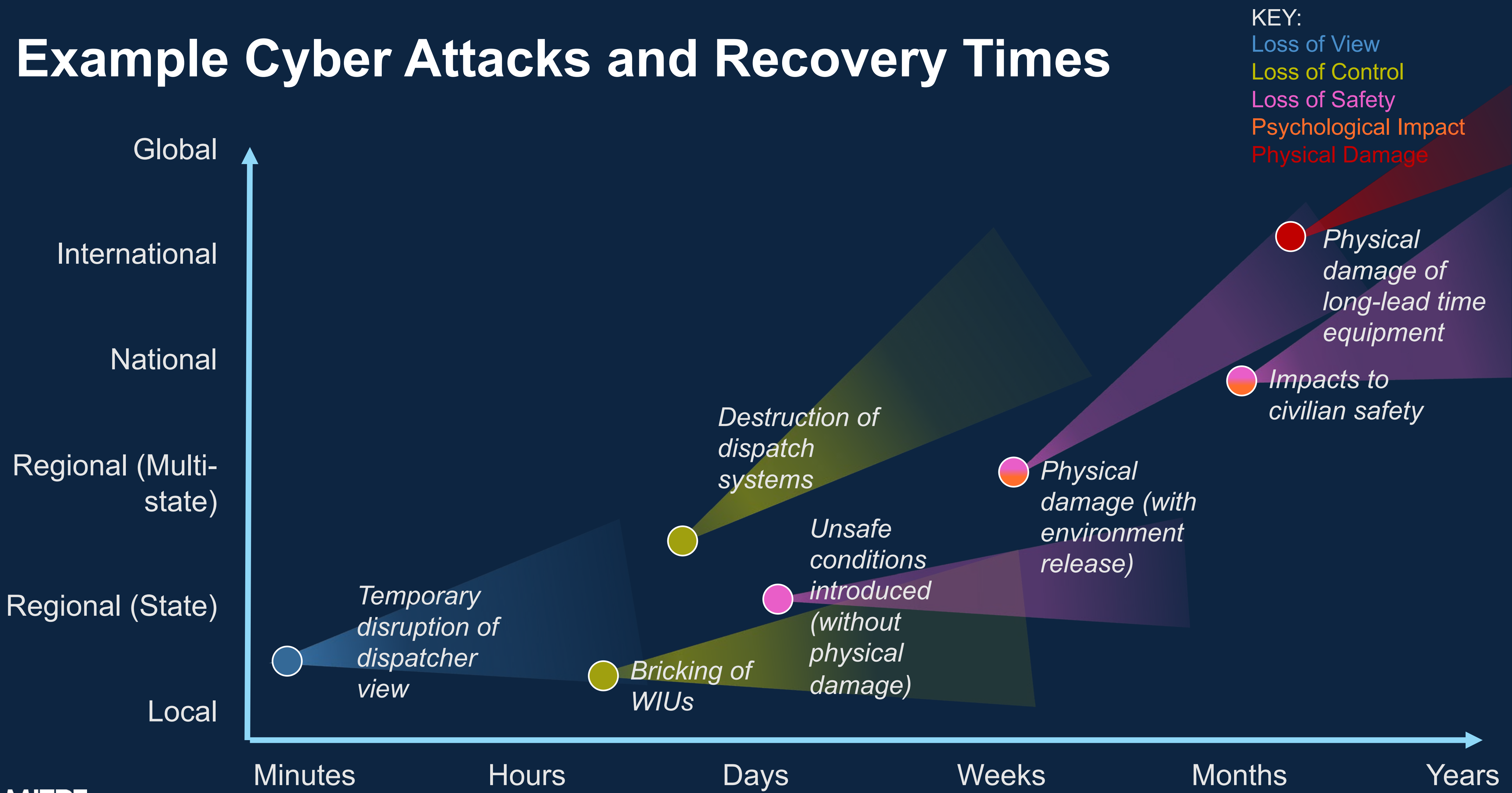
Key Questions:

- *What technology failures have occurred in the past?*
- *What was the result of those technology failures?*
- *What was the cost and process of recovery from those technology failures?*
- *What system or business interdependencies exist?*
- *Etc.*

Severity: Considering Both Impact and Recovery

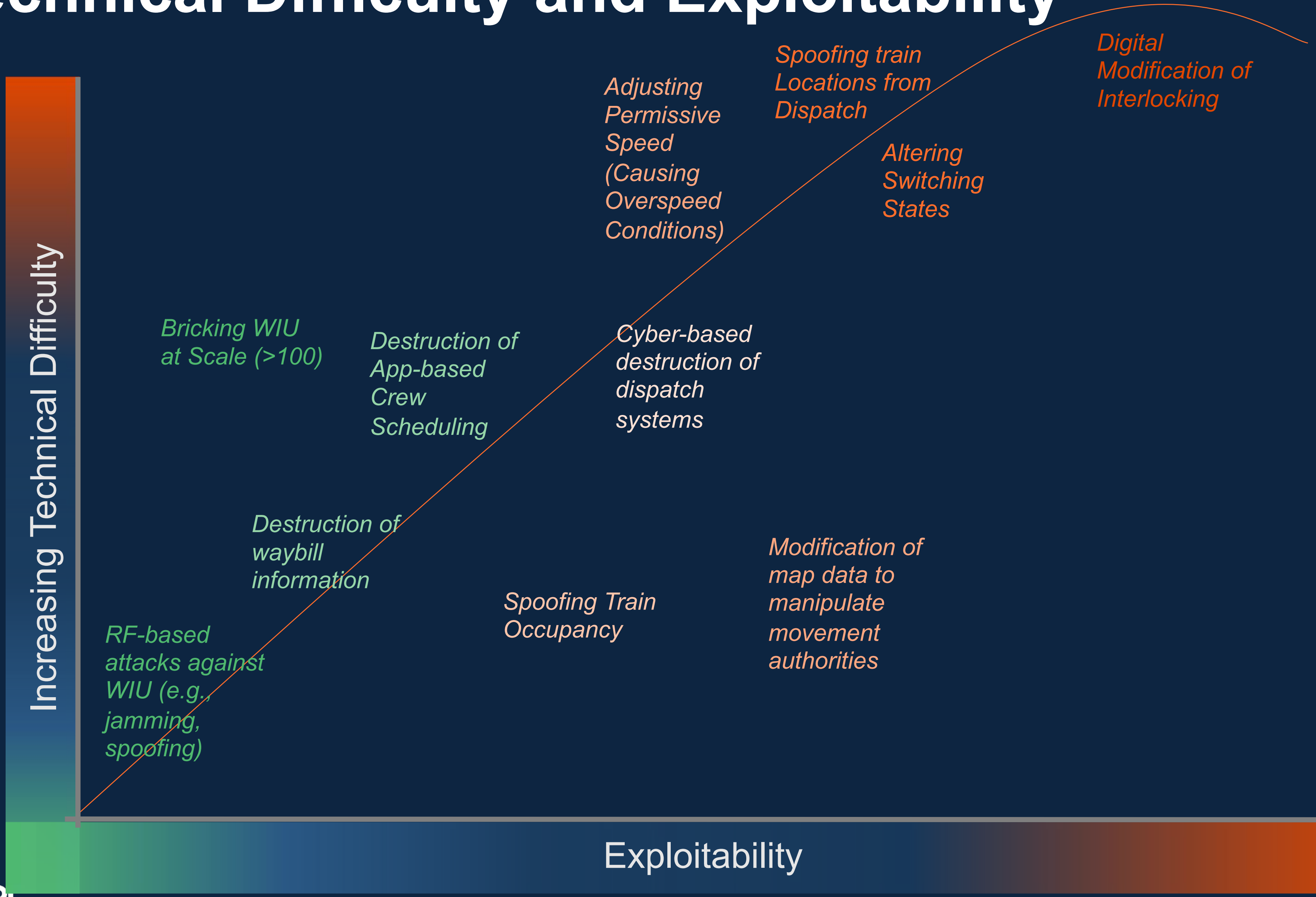


Example Cyber Attacks and Recovery Times



MITRE

Technical Difficulty and Exploitability

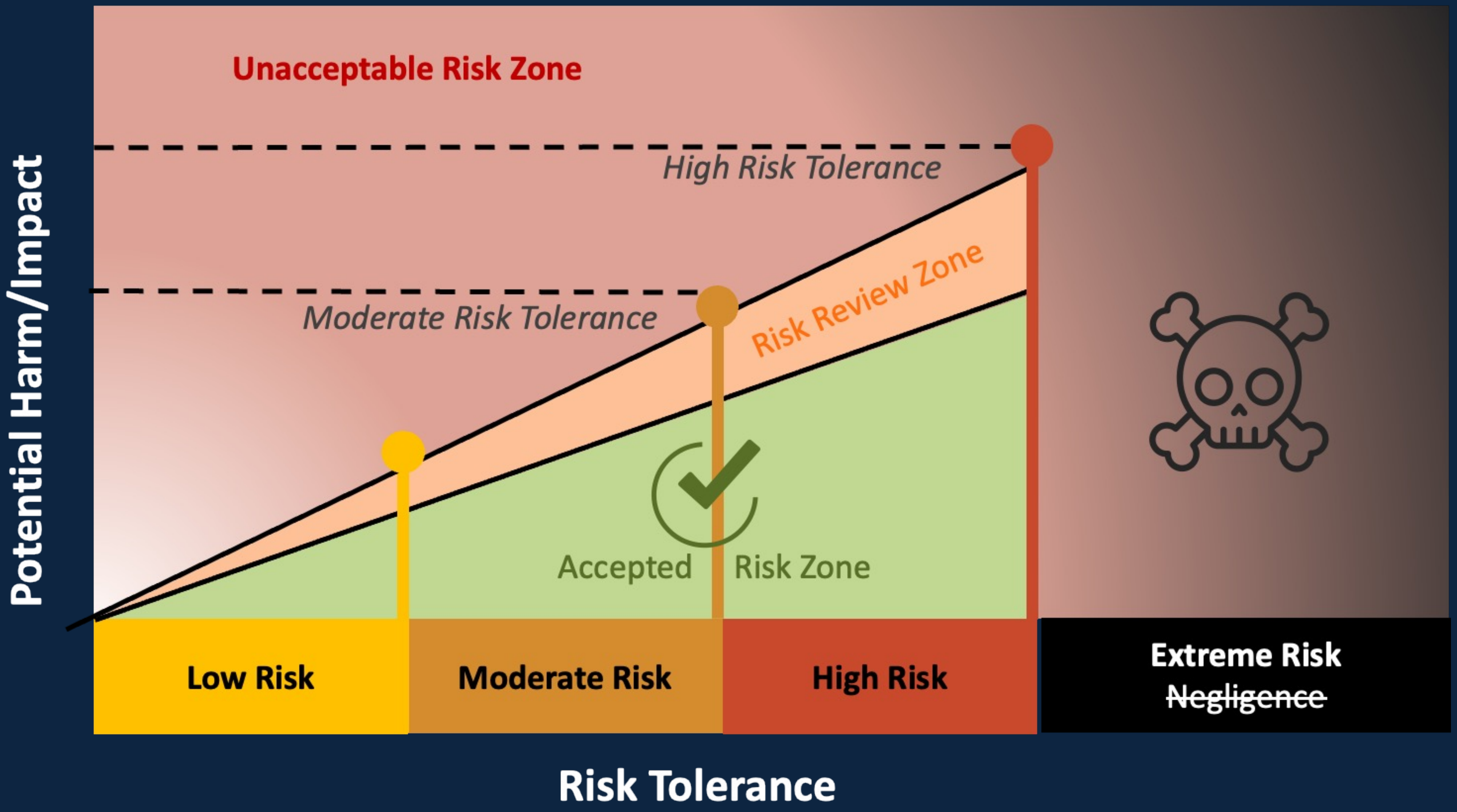


Technical Difficulty: **Skill** required to exploit a vulnerability

Exploitability: **Operational requirements** (e.g., time, money, personnel) required to exploit a vulnerability

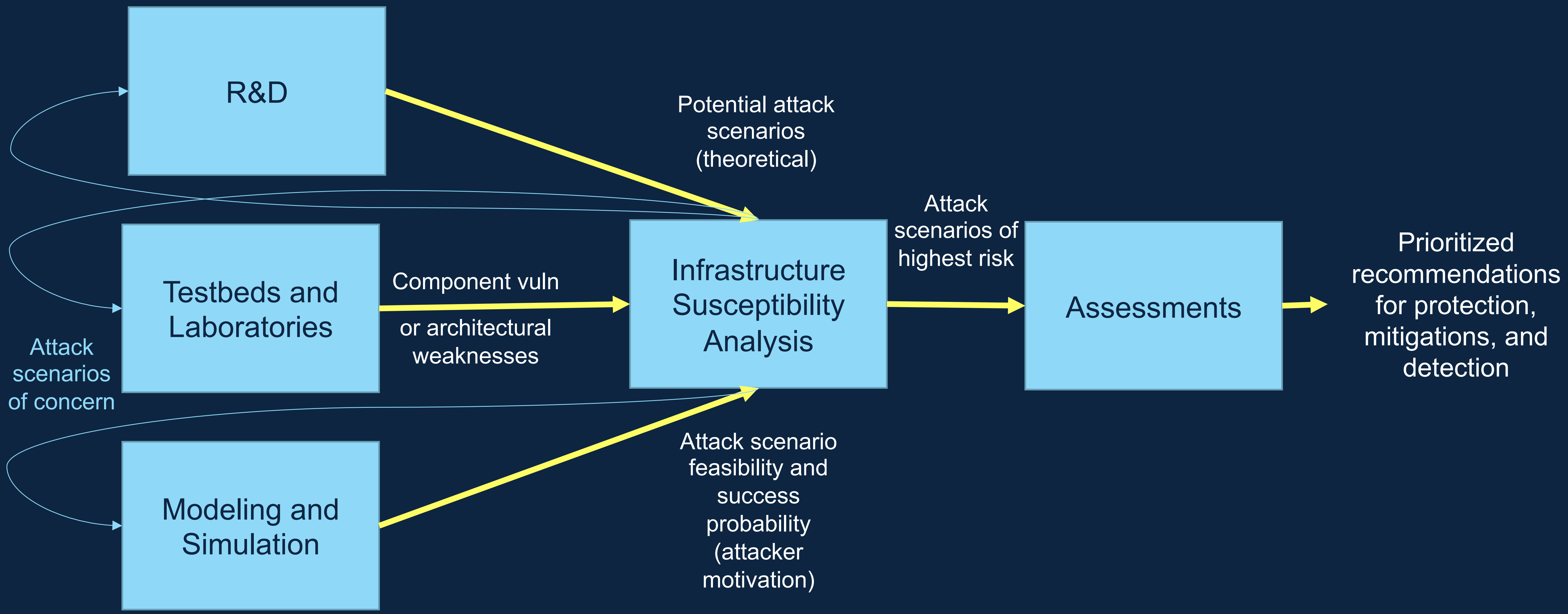
Most concerning attacks are those with low difficulty and high exploitability.

Understanding Threat, Exposure, and Risk Tolerance



MITRE

Future ISA Assessment Process Flow



R&D

Testbeds and Laboratories

Modeling and Simulation

Infrastructure Susceptibility Analysis

Assessments

Potential attack scenarios (theoretical)

Component vuln or architectural weaknesses

Attack scenario feasibility and success probability (attacker motivation)

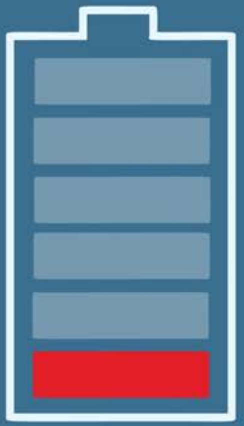
Attack scenarios of highest risk

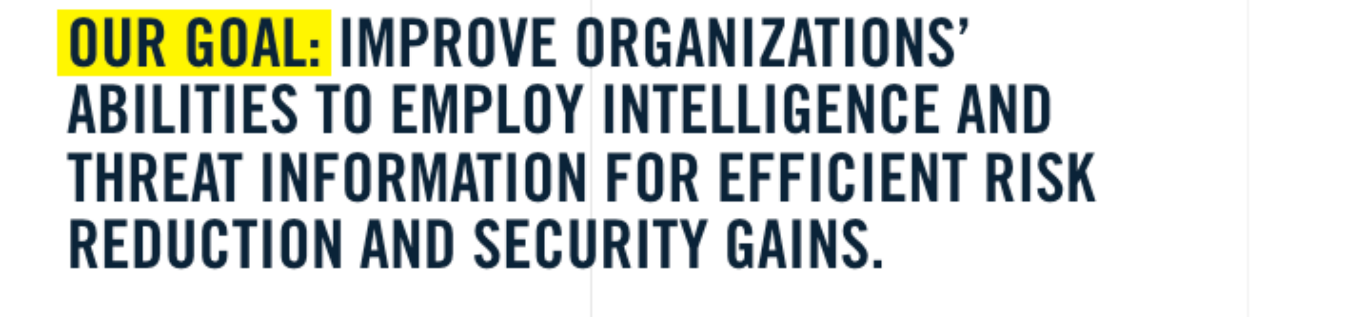
Prioritized recommendations for protection, mitigations, and detection

Attack scenarios of concern

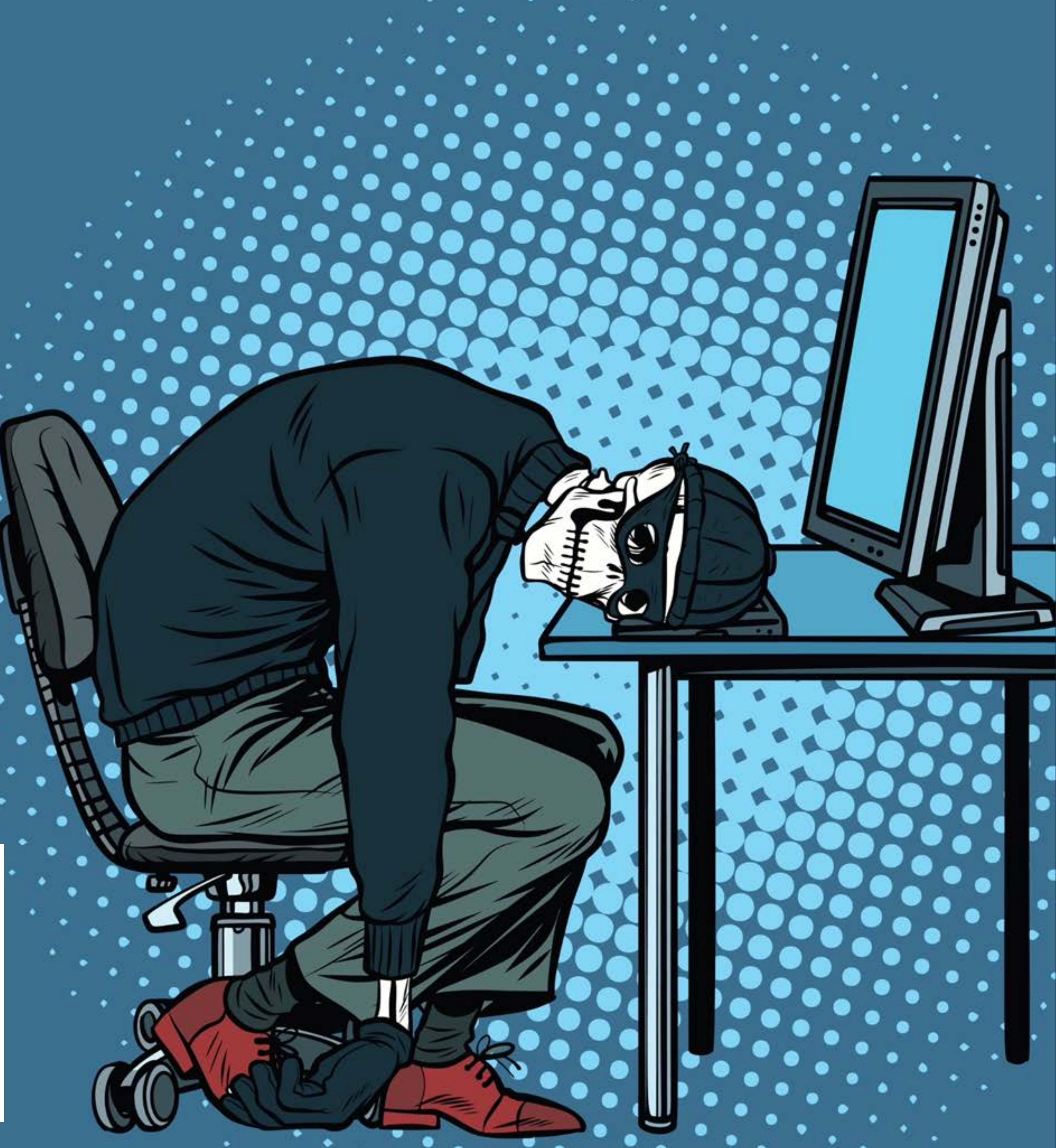
Increasing Adversary Costs

- Scoring approach enables identification of most likely attacks
- Future R&D Focus: calculating defender gains via specific system, procedure, and architecture modifications



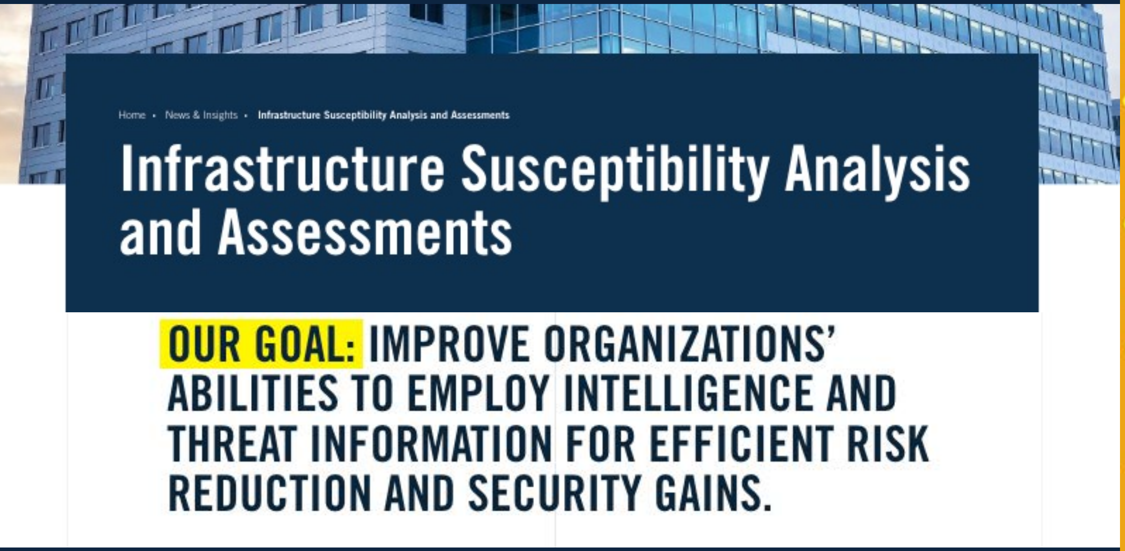


OUR GOAL: IMPROVE ORGANIZATIONS' ABILITIES TO EMPLOY INTELLIGENCE AND THREAT INFORMATION FOR EFFICIENT RISK REDUCTION AND SECURITY GAINS.



Interested in Learning More?

Visit our website (mitre.org/isa) and reach out to the ISA team (isa@mitre.org) - we're continuing to develop resources.



Home • News & Insights • Infrastructure Susceptibility Analysis and Assessments

Infrastructure Susceptibility Analysis and Assessments

OUR GOAL: IMPROVE ORGANIZATIONS' ABILITIES TO EMPLOY INTELLIGENCE AND THREAT INFORMATION FOR EFFICIENT RISK REDUCTION AND SECURITY GAINS.

MITRE

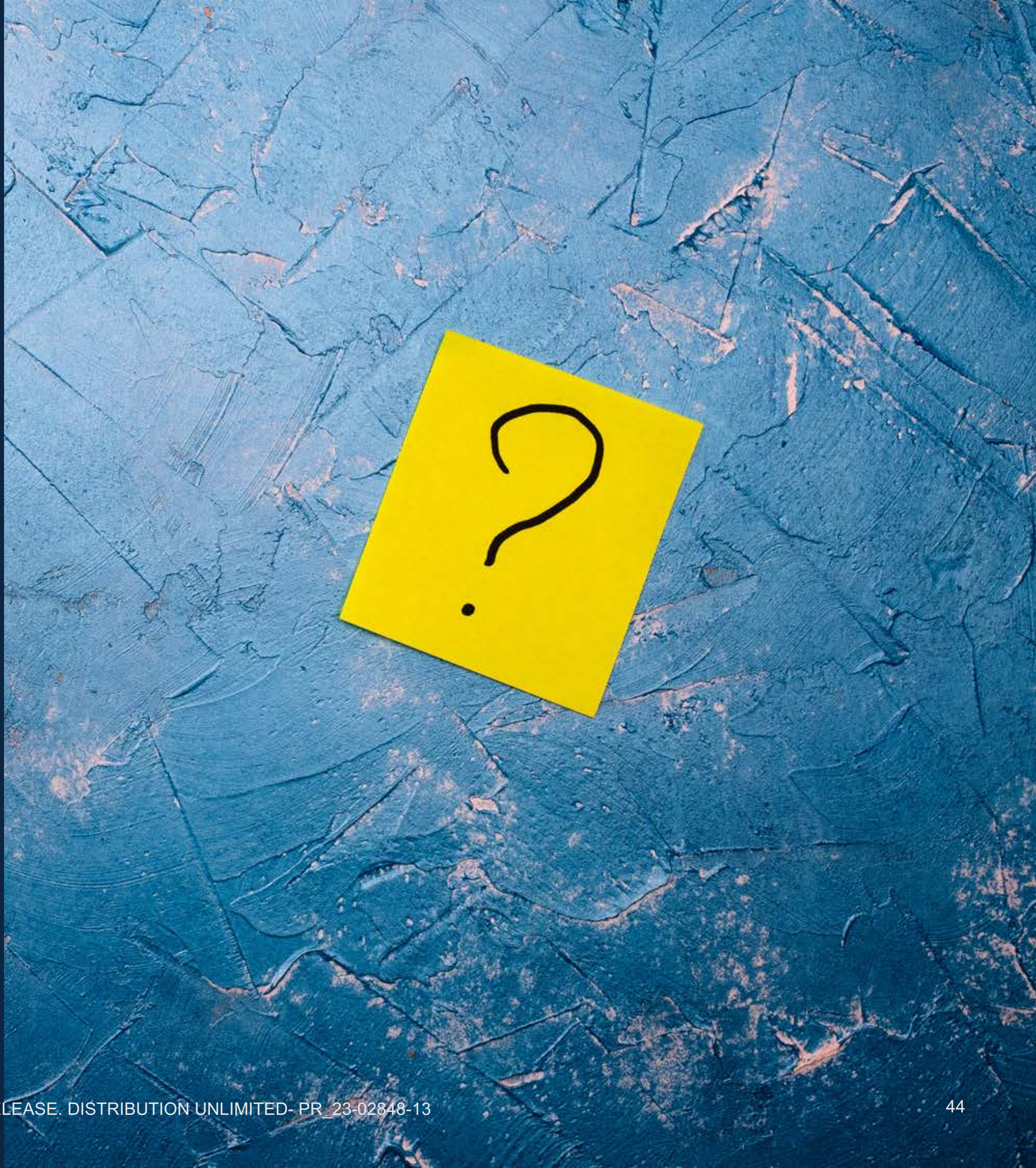
Questions?

Sarah Freeman

Chief Engineer, Intel, Modeling and Simulation

Cyber Infrastructure Protection Innovation Center/MITRE

sfreeman@mitre.org



Resources

- NIST Special Publication 800-160 V2, https://doi.org/10.6028/NIST.SP.800-160v2r1
- Stouffer, Keith, Timothy Zimmerman, CheeYee Tang, Joshua Lubell, Jeffrey Cichonski, and John McCarthy. "Cybersecurity Framework Manufacturing Profile." Gaithersburg, MD: National Institute of Standards and Technology, September 8, 2017. https://doi.org/10.6028/NIST.IR.8183.
- Kertzner, Peter, Cedric Carter, and Adam Hahn. "Crown Jewels Analysis (CJA) for Industrial Control Systems (ICS)," 2022. https://www.mitre.org/sites/default/files/2023-01/PR-22-2824-Crown-Jewels-for-Industrial-Control-Systems.pdf.
- Danzig, Richard. "Surviving on a Diet of Poisoned Fruit: Reducing the National Security Risks of America's Cyber Dependencies." Center for New American Security, July 21, 2014. https://www.cnas.org/publications/reports/surviving-on-a-diet-of-poisoned-fruit-reducing-the-national-security-risks-of-americas-cyber-dependencies.
- Freeman, Sarah G., St. Michel, Curtis P., and Johnson, Nathan Hill. 2020. "CCE Phase 1: Consequence Prioritization". United States. https://doi.org/10.2172/1617458. https://www.osti.gov/servlets/purl/1617458.
- Bochman, Andrew A., and Sarah Freeman. *Countering cyber sabotage: introducing consequence-driven, cyber-informed engineering (CCE)*. CRC Press, 2021.