CYBER STATECRAFT
INITIATIVE

DFRLab

#ACcyber

ISSUE BRIEF

APRIL 2023

Critical Infrastructure Cybersecurity Prioritization:

A Cross-Sector Methodology for Ranking Operational Technology Cyber Scenarios and Critical Entities

DANIELLE JABLANSKI

The **Cyber Statecraft Initiative** works at the nexus of geopolitics and cybersecurity to craft strategies to help shape the conduct of statecraft and to better inform and secure users of technology. This work extends through the competition of state and non-state actors, the security of the internet and computing systems, the safety of operational technology and physical systems, and the communities of cyberspace. The Initiative convenes a diverse network of passionate and knowledgeable contributors, bridging the gap among technical, policy, and user communities.

The mission of the **Digital Forensic Research Lab (DFRLab)** is to identify, expose, and explain disinformation where and when it occurs using open-source research; to promote objective truth as a foundation of government for and by people; to protect democratic institutions and norms from those who would seek to undermine them in the digital engagement space; to create a new model of expertise adapted for impact and real-world results; and to forge digital resilience at a time when humans are more interconnected than at any point in history, by building the world's leading hub of digital forensic analysts tracking events in governance, technology, and security.

EXECUTIVE SUMMARY

"Cyber policy today has created a world in which seemingly everything non-military can be held at risk—hospitals, trains, dams, energy, water—and nothing is off limits."[1]

Policy experts have long looked to other fields to gain a better understanding of cyber issues—natural disasters, terrorism, insurance and finance, and even nuclear weapons—due to the "always/never" rule. The always/never concept stipulates that weapons must always work correctly when they are supposed to and never be launched or detonated by accident or sabotage. The application of the always/never rule to process control systems across an increasingly digitized critical infrastructure landscape is incredibly difficult to master.

Threading the tapestry of risk across critical infrastructure requires a more granular and purposeful model than the current approach to classifying critical infrastructure can deliver. Failing to contextualize the broad problem set that is critical infrastructure cybersecurity jeopardies increasing the cost of compliance-based cybersecurity to the extent that small- and medium-sized businesses cannot afford the expense and/or expect the government to provide managed

[1] Danielle Jablanski, "Why Cyber Holds the Entire World at Risk," National Interest, April 5, 2022, https://nationalinterest.org/blog/techland-when-great-power-competition-meets-digital-world/why-cyber-holds-entire-world-risk.

cybersecurity services for designated concentrations of risk across multiple sectors—an imprudent, expensive, and unsustainable outcome.

Informing decision-makers requires deeper analysis of critical infrastructure targets through available open-source intelligence, criticality and vulnerability data, the degradation of operations by cyber means, and mean time to recover from cyber impacts that does not exist at scale. This paper offers an initial step to focus on cyber-physical operations, discussing the limitations of current methods to prioritize across critical infrastructure cybersecurity and outlining a methodology for prioritizing scenarios and entities across sectors and local, state, and federal jurisdictions.

This methodology has two primary use cases:

1. It provides a way for asset owners to rank relevant cyber scenarios, enabling a single entity, organization, facility, or site in scope to prioritize a tabletop exercise scenario that maps cyber-physical impacts from control failures to localized cascading impacts.

2. It generates a standardized priority score, which can be used by government and industry stakeholders to compare entities, locations, facilities, or sites within any jurisdiction (by geography, sector, regulatory body, etc.)—e.g., to compare 1,000 entities in a single sector or to compare a prison to a water utility or a rail operator to a hospital.

INTRODUCTION

The Department of Homeland Security's National Incident Management System includes five components: plan, organize and equip, train, exercise, and evaluate and improve.[2] Cybersecurity conversations are stuck in a limited cycle of buy a product, run a tabletop exercise, and check compliance boxes, often skipping key steps for organization, failing to exercise function-specific responsibilities, and almost never exercising to failure like a real emergency might require. Collectively, cyber-physical security requires new strategic and tactical thinking to better inform decision-makers in cyber policy, planning, and preparedness.

Critical infrastructure sectors and operations depend on equipment, communications, and business operations to supply goods, services, and resources to populations and interdependent commercial industries each day around the clock. Over the last decade, distributed operations, including manual and analog components that were originally not accessible via the internet, have increasingly become digitized and connected as networked technology connects systems to systems, sites to sites, and people to everything.

Owners and operators of critical infrastructure are responsible for securing their operations and processes from the inside out according to assorted regulatory and compliance requirements within and across each sector. The U.S. government is responsible for protecting citizens, national security, and the economy. Despite the tactical understanding of critical infrastructure equipment, communications, and business operations, critical infrastructure cybersecurity remains ambiguous. Several agencies across the U.S. government are working together to develop cybersecurity performance standards, baseline metrics, incident reporting mechanisms, information sharing tools, and liability protections.

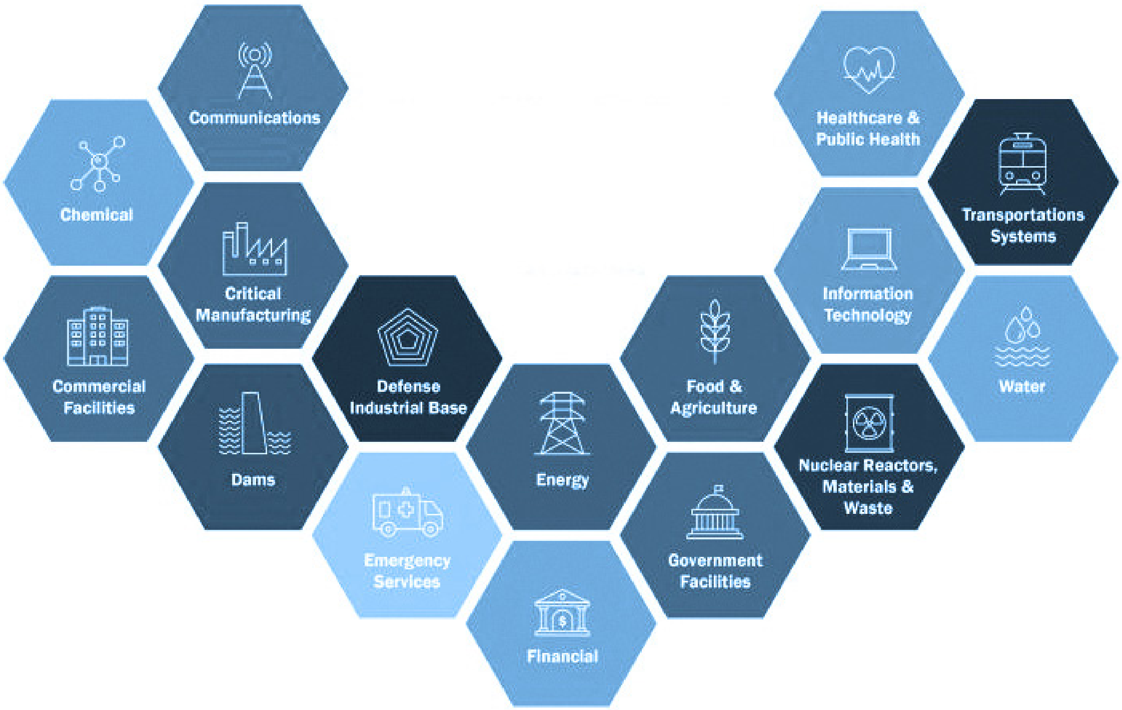
Nevertheless, critical infrastructure cybersecurity presents a massive needle in a haystack problem. Where information technology (IT) sees many vulnerabilities, likely to be exploited in similar ways across mainstream and ubiquitous systems, operational technology (OT) security is often a proprietary ,case-by-case distinction. The oversimplification of their differences leads to a contextual gap when translating roles and responsibilities into tasks and capabilities for government and business continuity and disaster recovery for industry.

What is eating critical infrastructure is not a talent gap, the convergence of IT and OT, or even the lack of investment in cybersecurity products and solutions. It is the improbability of determining all possible outcomes from single points of dependence and the failure that exists between and beyond business continuity, physical equipment, and secure data and communications.

One consistently repeated recommendation from high-level decision-makers is that organizations, entities, and/or facilities carry out tabletop exercises and scenario planning to prepare for cyber situations that could have disruptive and devastating outcomes, especially those that threaten human life and national and economic security. However, there is no standardized way to develop or run these exercises or to decide which scenarios to simulate for teams based on size, location, scope, operational specifics, security maturity, and resource capacity.

[2] "National Preparedness Cycle," Homeland Security Emergency Management Center of Excellence, https://www.coehsem.com/emergency-management-cycle/.

Essential Critical Infrastructure Sectors



SOURCE: cisa.gov

ALL OF IT IS CRITICAL, SO WHAT MATTERS?

"Systems of economic exchange that promote patterns of civil society depend on the sustainable availability and equitable use of natural and social resources necessary for constructing a satisfying and 'satisficing' life by present and future generations."[3]

Critical infrastructure is critical not only because the disruption, degradation, or destruction of entities/operations will impact life, the economy, or national security, but also because critical infrastructure sectors form the backbone of U.S. civil society. Some critical infrastructure sectors are also transactionally dependent on one another. The water sector depends heavily on operations and outputs from the energy, transportation, finance, and manufacturing sectors. Transportation depends on operations and outputs from the energy, finance, communications, and manufacturing sectors, and so on.[4]

There are indicators to suggest that government will likely continue tasking industry with cybersecurity requirements. Recent European Commission legislation sheds light on the due diligence of cybersecurity activities. The Network and Information Security 2 directive suggests that entities assess the proportionality of their risk management activities according to their individual degree of exposure to risks, size, likelihood and severity of incidents, and the societal and economic impacts of potential incidents.

According to retired National Cyber Director Chris Inglis, the Biden administration's National Cybersecurity Strategy drills into "affirmative intentionality," asking industry to raise the bar on cyber responsibility, liability, and resilience building. This comes at a time when best practices are numerous but implementation specifics are scarce. The strategy is positioned to expand mandated policies at sector risk management agencies and to double down on broader information sharing, combined with international law enforcement, to quell undeterred cyber criminals and threat-actor groups.

The U.S. Cybersecurity and Infrastructure Security Agency (CISA) uses the National Critical Functions Framework to define and assess critical functions across sectors. Critical functions, including the fifty-five published by CISA, are defined as "vital to the security, economy, and public health and safety of the nation."[5] Critical assets are prioritized as those which "if destroyed or disrupted, would cause national or regional catastrophic effects."[6]

[3] Benjamin R., Barber, *A Place for Us: How to Make Society Civil and Democracy Strong* (New York: Hill and Wang, 1984).

[4] Tyson Macaulay, *Critical Infrastructure: Understanding Its Component Parts, Vulnerabilities, Operating Risks, and Interdependencies* (Boca Raton: CRC Press, 2009).

[5] "Critical Infrastructure Protection: CISA Should Improve Priority Setting, Stakeholder Involvement, and Threat Information Sharing," U.S. Government Accountability Office, March 1, 2022, https://www.gao.gov/products/gao-22-104279.

[6] "Critical Infrastructure Protection," 2022.

According to a review by the U.S. Government Accountability Office, this approach has fallen short in three major ways: Stakeholders found it difficult to prioritize the framework given competing planning and operations considerations, struggled with implementing the goals and strategies, and required more tailored information to use the framework in a meaningful way. As a result, only fourteen states out of fifty-six have provided updates to the National Critical Infrastructure Prioritization Program since 2017.[7]

Entities determined to be the most essential of all critical infrastructure are categorized as Section 9 entities, defined as "critical infrastructure where a cybersecurity incident could reasonably result in catastrophic regional or national effects on public health or safety, economic security, or national security."[8] A recommended definition of *systemically important critical infrastructure* (SICI) in proposed legislation suggests the secretary of the U.S. Department of Homeland Security could declare a facility, system, or asset as "systemically important critical infrastructure" if the compromise, damage, and/or destruction of that entity would result in the following:

- The interruption of critical services, including the energy supply, water supply, electricity grid, and/or emergency services, that could cause mass casualties or lead to mass evacuations.

- The perpetuation of catastrophic damage to the U.S. economy, including the disruption of the financial market, disruption of transportation systems, and the unavailability of critical technology services.

- The degradation and/or disruption of defense, aerospace, military, intelligence, and national security capabilities.

- The widespread compromise or malicious intrusion of technologies, devices, or services across the cyber ecosystem.[9]

Regardless of scoping for SICI, there is a lack of understanding about the inventory of industrial assets and technologies that are in use across critical sectors today and the configuration contingencies for risk management for that inventory. There is a similar absence of holistic awareness about the realistic, cascading impacts or the fallout analysis for entities with varying characteristics and demographics.

OPERATIONAL TECHNOLOGY

Operational technology (OT) and industrial control system (ICS) technologies include a wide range of machines and equipment, such as pumps, compressors, valves, turbines and similar equipment, interface computers and workstations, programmable logic controllers, and many diagnostics, safety, and metering and monitoring systems that enable or report the status of variables, processes, and operations.

Supervisory control and data acquisition (SCADA) systems encompass operations management and supervisory control of local or physical OT controls and are programmed and monitored to direct one or more processes operating at scale—i.e., machines and devices command process controls that are involved in directing and manipulating physical sensors and actuators.

Sectors operating OT and ICS on a daily basis include oil and gas, power and utilities, water treatment and purification facilities, manufacturing, transportation, hospitals, and connected buildings. OT devices tend to be legacy devices with fifteen- to twenty-year lifecycles and beyond, operating 24-7 with rarely scheduled or available maintenance windows for software patches and updates. These devices often lack robust security controls by design and feature proprietary communication protocols and varying connectivity and networking requirements.

OT cybersecurity aims to prevent attacks that target process control equipment that reads data, executes logic, and sends outputs back to the machine or equipment. However, IT cybersecurity practices, analytics, forensics, and detection tools do not match the unique data and connectivity requirements and various configurations of OT environments.

A single operation or location might have more than a dozen different types of vendor technologies—SCADA, distributed control systems, programmable logic controllers, remote terminal units, human-machine interfaces, and safety instrumented systems—running with proprietary code and industry specific protocols. Prioritizing availability and data in motion, each asset and system will have unique parameters for identification and communication on a network, making it nearly impossible to manually log granular session- and packet-level details about each asset or system.

Attacks involving OT and ICS come predominately in two forms. Some are tailored specifically for a single target with the intent of establishing prolonged, undetected access to manipulate view and/or control scenarios that could result in physical disruption or destruction. Others involve "living off the land" techniques that target common denominators across organizations based on opportunistic activities, such as using established social engineering; tactics, techniques and procedures (TTPs); credential harvesting; and the purchase of intelligence and access from threat actors and groups conducting continuous reconnaissance and acting as initial access brokers.

[7] "Critical Infrastructure Protection," 2022.

[8] Executive Order 13800, Strengthening the Cybersecurity of Federal Networks and Critical Infrastructure, May 8, 2018.

[9] Tasha Jhangiani and Graham Kennis, "Protecting the Critical of Critical: What Is Systemically Important Critical Infrastructure?" Lawfare, June 15, 2021, https://www.lawfareblog.com/protecting-critical-critical-what-systemically-important-critical-infrastructure.

RISKS AND VULNERABILITIES IN OPERATIONAL TECHNOLOGY AND CRITICAL INFRASTRUCTURE

It is increasingly difficult to contextualize critical infrastructure both operationally—based on specific products, services, resources, processes, and technologies—and functionally—based on centralized versus distributed risks, dependencies, and interdependencies. Attempts to at contextualization have led to a debate between asset-specific (things, such as technologies, systems, and equipment) versus function-specific (actions, such as connecting, distributing, managing, and supplying) cybersecurity prioritization. This dichotomy is also characterized as "threats from" a threat actor and their capabilities to impact functions, instead of "threats to" specific assets as explained in product-specific vulnerability disclosures.[10]

Today there are thousands of known product vulnerabilities in OT and ICS systems from each vendor that produces machines and equipment in those categories. While each vulnerability is published with an associated common vulnerability score, it is impossible to immediately understand how severe that vulnerability will be in context for a single entity or organization's risk profile based on the designated severity of the vulnerability. Vulnerabilities must be compared with operational status to understand their significance and to prioritize the actions and procedures that will reduce the severity of the vulnerability's potential impacts.

Unfortunately, "threats from" actors cannot easily be mapped to the exploitation of threats to OT and ICS. The assets versus functions distinction that is commonplace in the current debate over critical infrastructure typically leads to a hyper focus on either systems impact analysis (asset-specific) or business continuity (function-specific) outcomes and limits holistic fallout analysis for four main reasons:

1. The plethora of existing product vulnerabilities in critical OT do not translate directly into manipulation of view or manipulation of control scenarios.

2. The severity scoring for vulnerabilities is too vague to determine cascading impacts or relevant fallout analysis for a specific facility or operation.

3. The loss of function outcomes and consequences are often not well scoped in terms of realistic cyber scenarios that would lead to and produce cascading impacts.

4. Cyber incidents that impact physical processes are less repeatable than IT attacks and accessible cyber threat intelligence for threat actors and TTPs that specifically target OT and ICS is less widely available, as there are fewer known and analyzed incidents.

Many OT and ICS systems have known vulnerabilities and unsophisticated, yet complex, designs; the security complexity is in the attack path or "kill chain," targeting simplistic systems that can be configured in a myriad of ways. Critical infrastructure entities can be targeted by threat actors to exploit and extort their IT and OT or ICS systems, but OT and ICS systems—traditionally designed with mission state and continuity in mind—also risk having their native functionality targeted and hijacked in cyber scenarios.[11]

Risks to cyber-physical systems include:

- the use of legacy technologies with well-known vulnerabilities

- the widespread availability of technical information about control systems

- the connectivity of control systems to other networks

- constraints on the use of existing security technologies and practices

- insecure remote connections

- a lack of visibility into network connectivity

- complex and just-in-time supply chains

- human error, neglect, and accidents.

If the core of cybersecurity is a calculation of threats, vulnerabilities, and likelihood, critical infrastructure sectors and technologies represent an exponential number of probabilistic outcomes for cyber scenarios with physical consequences. Despite increased awareness, pressure, and oversight from governments, boards, and insurance providers, the scale and complexity of the problem set quickly intensifies given the entanglement of

- similar, but not identical, industries and technologies

- inconsistent change management and documentation

- reliance on third-party systems and components

- external threat actors and TTPs

- risk management and security best practices

- compensating controls and security policy enforcement

- compliance, standards, and regulations.

[10] Tyson Macaulay and Bryan Singer, *Cybersecurity for Industrial Control Systems: SCADA, DCS, PLC, HMI, and SIS* (Boca Raton: CRC Press, 2012), 57.

[11] Michael J. Assante and Robert M. Lee, "The Industrial Control System Cyber Kill Chain," SANS Institute, October 2015, https://na-production.s3.amazonaws.com/documents/industrial-control-system-cyber-kill-chain-36297.pdf.

ADVERSARY → INTENTIONAL → OBJECTIVES MET WITHIN SCOPE	ADVERSARY → ACCIDENTAL → UNINTENDED CONSEQUENCES BEYOND SCOPE
OPERATOR → INTENTIONAL → MALICIOUS INSIDER THREAT WITHIN SCOPE	OPERATOR → ACCIDENTAL → CYBER INCIDENT TO TRIAGE

This complexity results in four types of *general* OT and ICS cyber scenarios in critical infrastructure. The two most commonly discussed, but not necessarily the most commonly experienced, are if/when an adversary accesses an OT environment and intentionally causes effects within the scope of their objectives or causes unintended consequences beyond the scope of their objectives. These general scenarios can be further dissected and understood by referencing the specific attack paths and impacts outlined in the MITRE Corporation's ATT&CK Matrix for ICS.[12]

A SCORING METHODOLOGY FOR CROSS-SECTOR ENTITY PRIORITIZATION

Today, critical infrastructure cyber protection correlates sixteen different sectors, with no way to compare a standardized risk metric from a municipal water facility in Wyoming with a large commercial energy provider in Florida or a rural hospital in Texas with a train operator in New York. This section proposes a scoring methodology for cross-sector entity prioritization using qualitative scenario planning and quantitative indicators for severity scoring, assessing the potential for scenarios to cause public panic and to stress/overcome local, state, and federal response capacity.

Prioritizing critical infrastructure cybersecurity requires robust planning—comprehensive in scope, yet flexible enough to account for contingencies. Tasha Jhangiani and Graham Kennis note that "a risk-based approach to national security requires that the U.S. must prioritize its resources in areas where it can have the greatest impact to prevent the worst consequences."[13] Owners and operators of critical infrastructure have relayed to the U.S. government a need for more "regionally specific information" to address cyber threats.[14]

A recent report on the ownership of various utilities in the United States found that "a better indicator of how to approach [cyber] regulations is to look at how many people a utility services," a direct indicator for fallout analysis when OT systems are impacted.[15] Where progress should start can be determined by expanding fallout analysis to identify the most at-risk environments across any given jurisdiction regardless of sector, location, ownership, or cybersecurity policy enforcement.

Scoring entities according to the prioritization methodology outlined below requires a well-executed thought exercise. The results are a way to determine the most consequential scenarios for facilities and operations, as well as the most at-risk facilities and operations within a given jurisdiction. The scoring can be performed at a local, state, or federal level. This type of prioritization offers an accessible way for entities to grapple with cybersecurity concerns in a local and regional context. The ranking also allows prioritization from an effects-based (impacts), rather than a means-based (capabilities), approach.

This methodology has two primary use cases:

1. The scoring matrix provides a way to rank and prioritize relevant cyber scenarios for a single entity, organization, facility, or site in scope.
    a. The ranking, based on weighted scores, will allow any entity, organization, facility, or site to choose scenarios to exercise based on a choice of two real-world impacts (impact A, impact B) or to assess both impacts when choosing a tabletop scenario.
        i. This ranking has the potential to prioritize scenarios that will cause public panic and/or overwhelm response resources over scenarios that simply have a higher cyber severity rating (see Table 1).
2. The standardized priority score provides an overall priority score for the entity, organization, facility, or site.
    a. This score can be used to compare and rank different entities, locations, facilities, or sites within a given jurisdiction—city or local, state, federal, sector-specific, etc.

This methodology can be incorporated into assessments, training, and tabletop exercises in the planning phase of cyber risk mitigation and incident response. It can also be used by leaders to prioritize multiple critical infrastructure sectors or locations in their jurisdiction from a cybersecurity perspective.

[12] "MITRE ATT&CK Matrix for ICS," MITRE Corporation, last modified May 6, 2022, https://attack.mitre.org/matrices/ics/.

[13] Jhangiani and Kennis, 2021.

[14] "Critical Infrastructure Protection," 2022.

[15] Jacob Azrilyant, Melissa Sidun, and Mariami Dolashvili, "Fact and Fiction: Demystifying the Myth of the 85%," capstone project, George Washington University, May 6, 2022, https://www.scribd.com/document/575971848/Fact-and-Fiction-85-and-Critical-Infrastructure.

HOW TO USE THE METHODOLOGY

Prioritizing cybersecurity efforts across critical infrastructure can borrow from the suggested fallout analysis applied to the public and local response capacity of a given target. When a weapon of mass destruction is used as an act of terror, according to the 2002 Federal Emergency Management Agency's Interim Planning Guide for State and Local Governments, "Managing the Emergency Consequences of Terrorist Incidents," there are two additional possible outcomes:[16]

- Impact A—the creation of chaos, confusion, and public panic
- Impact B—increased stress on local, state, and federal response resources.

Weighting cyber severity scores for scenarios based on impact A and impact B is essential, as each scenario will impact the level of public panic and available resources differently depending on the sector and that sector's assets and functions, location, and region. For example, a hospital ransomware attack in an urban area may not cause widespread public panic, but it may have the ability to overwhelm response resources in rural areas. Conversely, an attack on the financial sector may result in public panic, but it may be less likely to overwhelm response resources.

An IT system interruption might cause business disruptions and downtime that results primarily in public panic, while manipulation of control at a water facility could have major impacts on both public panic and response resources. The 2021 Colonial Pipeline ransomware incident inadvertently shut down OT and ICS systems and led to unforeseen local and regional impacts. The scoring methodology used here works to manage uncertainty, identifying four essential components in consultation with informed cybersecurity experts, owners and operators, and local and regional stakeholders.

1. Scenario planning: Six scenarios will be outlined according to their potential to result in either manipulation of view (three scenarios) or manipulation of control (three scenarios) outcomes for OT.17

2. Severity scoring: The scoring will be based on cybersecurity severity (see Tables 1 and 2).

3. Weighting and ranking scenarios: The scenarios will be weighted and ranked based on their potential to cause public panic and/or to stress or overwhelm response capacity.

4. Final scoring: The standardized priority score will be calculated for the entire entity/operation.

The methodology compliments the SICI definition of critical infrastructure outlined above and can also be used to enhance the following concerted CISA recommendations:[18]

- develop primary, alternate, contingency, and emergency plans to mitigate the most severe effects of prolonged disruptions, including the ability to operate manually without the aid of control systems in the event of a compromise
- ensure redundancies of critical components and data systems to prevent single points of failure that could produce catastrophic results
- conduct exercises to provide personnel with effective and practical mechanisms to identify best practices, lessons learned, and areas for improvement in plans and procedures.

The resulting scenarios could further be compared using CISA's National Cyber Incident Scoring System, designed to provide a repeatable and consistent mechanism for estimating the risk of an incident. In the future, this methodology can potentially be used together with a Diamond Model of Intrusion Analysis applied to cyber-physical incidents to better understand how adversaries demonstrate and use certain capabilities and techniques against critical infrastructure targets. This may allow for better nation-state level analysis and more robust information for decision-makers who struggle to understand the likelihood of attacks against specific operations or facilities today.

[16] "Managing the Emergency Consequences of Terrorist Incidents: Interim Planning Guide for State and Local Governments," Federal Emergency Management Agency, July 2002, https://www.fema.gov/pdf/plan/managingemerconseq.pdf.

[17] View and/or control cannot be recovered automatically or remotely from manipulation. The potential for sabotage can come through misinformation delivered to control room personnel or through malicious instructions sent to production infrastructure. Macaulay and Singer, 2012.

[18] "Sector Spotlight: Cyber-Physical Security Considerations for the Electricity Sub-Sector," Cybersecurity and Infrastructure Security Agency, https://www.cisa.gov/sites/default/files/publications/Sector%20Spotlight%20Cyber-Physical%20Security%20Considerations%20Electricity%20Sub-Sector%20508%20compliant.pdf.

ANALYSIS AND CALCULATIONS

STEP 1: Scenario planning: Six scenarios will be outlined for their potential to result in either manipulation of view (three scenarios) or manipulation of control (three scenarios) outcomes for OT.[19]

Scenarios can include incidents in which the threat, vulnerability, or exploitation originate in the IT/corporate or enterprise side of operations. First, the top three most realistic manipulation of view scenarios for a target are identified based on impacts to OT, with severity indicators outlined in Table 1. Then, the top three most realistic manipulation of control scenarios for a target are identified based on impacts to OT, with indicators outlined in Table 1.

Table 1: Severity Indicators—Qualitative Assessment to Determine Severity Score in Table 2

Emerging Threat	Vulnerability	Exploit
Is the threat novel or unique?	Is a widespread OT vulnerability exposed?	What are the methods and speed of propagation/ scope of impact?
Do current monitoring tools detect and defend against the threat?	Will exploitation of vulnerability trigger incident response?	What protocols and ports are affected?
Is the threat a repeat of prior attacks or parts thereof?	Does access require lateral movement from a corporate network?	Payload—what is the level of destruction?
Does the threat defeat segmentation efforts?	How many OT systems are at risk?	How many OT systems are known to be affected?
Does the threat establish novel access to OT systems?	How sophisticated are the required exploits/ capabilities?	How important/critical are the affected systems?
Has the threat impacted similar systems/sectors?	Does exploitation require interaction with the target?	How complicated is the attack method?
Is there wide press coverage/widespread knowledge of threat?	Is there wide press coverage/widespread knowledge of vulnerability?	What are the localized and residual impacts of exploitation?

SOURCE: Adapted from the Center for Regional Disaster Resilience "Washington Cybersecurity Situational Awareness Concept of Operations (CONOPS)" guidance document.[20]

[19] View and/or control cannot be recovered automatically or remotely from manipulation. The potential for sabotage can come through misinformation delivered to control room personnel or through malicious instructions sent to production infrastructure. Macaulay and Singer, 2012.

[20] Washington Cybersecurity Situational Awareness Concept of Operations (CONOPS)," Center for Regional Disaster Resilience, https://www.regionalresilience.org/uploads/2/3/2/9/23295822/washington_cybersecurity_situational_awareness_conops.pdf.

STEP 2: Severity scoring: The scoring will be based on cybersecurity severity indicators (see Table 1). Each scenario is scored based on a severity rating in Table 2 (scores for each scenario range from 10 to 50).

Table 2: Severity Rating
(does not have to equal 100)

Severity	Rating	Description
Minimal	10	Negligible impact on the organization
Low	20	Very low impact on the organization, unlikely to affect other organizations
Medium	30	Poses a potential impact on the organization, minimal possibility of impact to other organizations
High	40	Will impact the organization, likely to impact other organizations
Crisis	50	Will have a severe impact on the operational capacity of the organization, known or expected impacts to other organizations

SOURCE: Adapted from the Center for Regional Disaster Resilience "Washington Cybersecurity Situational Awareness Concept of Operations (CONOPS)" guidance document.[21]

STEP 3: Weighting and ranking scenarios: The scenarios will be weighted and ranked based on their potential to cause public panic and/or to stress or overwhelm response capacity.

The scenarios will be ranked based on impact A and impact B. All six scenarios will be ranked separately by both likelihood of causing public panic and ability to overwhelm local response resources (see Table 3).

Table 3: Weighting Likelihood to Cause Public Panic and to Overwhelm Resources
(total weights must = 1)

Panic	Weight	Resources	Weight
Most likely to cause public panic	.25	Most likely to overwhelm response resources	.25
Most likely to cause public panic	.25	Most likely to overwhelm response resources	.25
Potential to cause public panic	.15	Potential to overwhelm response resources	.15
Potential to cause public panic	.15	Potential to overwhelm response resources	.15
Least likely to cause public panic	.10	Least likely to overwhelm response resources	.10
Least likely to cause public panic	.10	Least likely to overwhelm response resources	.10

STEP 4: Final scoring: The standardized priority score will be calculated for the entire entity/operation. The weighted scores for both impact A and impact B are combined and the standardized priority score is calculated (see Figure 4).

[21] "Washington Cybersecurity Situational Awareness," Center for Regional Disaster Resilience.

CASE STUDY: PRISON OT CYBERSECURITY

In November 2022, the Atlantic Council's Cyber Statecraft Initiative brought together cybersecurity experts to apply this scoring methodology to a mock tabletop exercise focused on a prison. A prison environment includes many functional OT and ICS systems and helps illustrate the utility of cybersecurity scenario planning beyond what is traditionally considered critical infrastructure. U.S. prisons also offer a real-world environment where experts who specialize in OT and ICS cybersecurity for any Section 9 entities or existing critical infrastructure sectors can address the problem set on equal footing, without speaking directly to any sector they serve or have worked in or with.

Prisons, often referred to as correctional facilities, operate across the United States. Twenty-six states and the Federal Bureau of Prisons rely heavily on private facilities to house incarcerated inmates.[22] These facilities depend on a myriad of IT and OT systems for safe, healthy, and continuous 24-7 operations. Examples of IT systems in prisons include telephone and email, video, telemedicine, radios, and management platforms (i.e., access to computers or tablets for entertainment, education, job skills, and reentry planning). Examples of OT systems include security platforms, surveillance cameras, access control points, perimeter intrusion detection, cell doors, and health and safety platforms, such as fire alarms and heating, ventilation, and air conditioning (HVAC) systems.[23] These OT and ICS systems are exposed to the threats and vulnerabilities that were previously discussed.

Consider one potential OT scenario in which a threat actor gains access to the system that controls the cell doors, which are programmed not to open or close simultaneously. Access to the controllers that incrementally open and close the cell doors could be achieved and a threat actor could override the incremental interval, directing all doors to move at once, potentially surging the power and/or destroying electronics and components of the cyber-physical system. Researchers have discovered prison control rooms with internet access and commissaries connected to OT networks where programmable logic controllers are operating.[24] This scenario represents a potential manipulation of control that would likely produce some level of public panic, but may not necessarily overwhelm local response capabilities.

Tabletop participants conducted a 90-minute exercise to develop six potential scenarios—three specifying manipulation of view impacts to OT and three specifying manipulation of control impacts to OT. The guidelines specified that each scenario must be realistic, technically feasible, worst-case scenarios based on cyber-physical impacts. The scenarios could not be duplicative and must be considered irrespective of network segmentation and best practice compensating controls. Scenarios could have initial access vectors in traditional information technologies, directly or indirectly impacting OT.

The prison specifics indicated that the facility opened in 1993 as a supermax prison in upstate New York. The mock facility housed 300 male inmates and had about 500 employees. Visiting hours were reportedly weekends and holidays between 9:00am and 3:15pm. The facility was said to be located five miles outside of a city of 27,000 people. The immediate town had twenty-seven police officers and fourteen civilian support staff. The nearest hospital, with 125 beds, was five miles away and in similar proximity to two large elementary schools. The facility itself was described as a hub-and-spoke model for operations, with a central command center monitoring and operating the facility and control systems located on premise but removed from the command center.

Access vectors were potentially numerous, including technicians with equipment and inventory access, universal serial bus (USB) drive and other transient devices, internet-connected control systems and networks, software updates, remote access, and remote exploitation, leading to the example scenarios outlined below. The scenarios and scoring that follow are a snapshot of this mock exercise and the application of the methodology in this paper. The example demonstrates bounded knowledge of a simulated exercise and is meant to showcase how an organization or facility might use the methodology for an entity or operation. Participants were cybersecurity experts, however, the scenario planning and thought exercise is meant to include all relevant stakeholders.

[22] Mackenzie Buday and Ashley Nellis, "Private Prisons in the United Sates, The Sentencing Project, August 23, 2022, https://www.sentencingproject.org/reports/private-prisons-in-the-united-states/.

[23] Teague Newman, Tiffany Rad, and John Strauchs, "SCADA & PLC Vulnerabilities in Correctional Facilities," Wired, July 30, 2011, https://www.wired.com/images_blogs/threatlevel/2011/07/PLC-White-Paper_Newman_Rad_Strauchs_July22_2011.pdf.

[24] Newman, Rad, and Strauchs, 2011.

MOCK PRISON EXAMPLE SCENARIOS: MANIPULATION OF VIEW AND MANIPULATION OF CONTROL

Scenario	Description
MOV 1	Camera systems accessed and controlled by external party, used to cause embarrassment and question integrity of organization
MOV 2	Scheduling and operational logistics manipulation, to include badging, medical deliveries, food systems, personnel requirements, transportation, etc., disrupted or degraded
MOV 3	Ransomware targets the organization with the ability to impact OT networks, no ability to control process control systems or OT devices
MOC 1	Third-party access and takeover of OT systems except cell block doors (safety, fire, HVAC, commissary equipment, radio signal in patrol vehicles, etc.)
MOC 2	Communications distributed denial-of-service, internally and externally, with capacity/threat to manipulate, modify, and disrupt process control systems
MOC 3	Third-party access to takeover process control systems of cell block doors only

MOV = manipulation of view, MOC = manipulation of control.

Figure 1. Priority Based on Severity Rating Alone (Table 1)

Scenario	Severity
MOV 1	30
MOV 2	10
MOV 3	40
MOC 1	40
MOC 2	40
MOC 3	50

NOTE that based on cybersecurity severity alone, MOC 3 ranks highest as a cyber scenario worth preparing and executing a tabletop exercise for.

Figure 2. Weighted Priority for Impact A (panic)

Scenario	Severity	Panic	Score	Rank
MOV 1	30	0.15	4.5	4
MOV 2	10	0.10	1	6
MOV 3	40	0.10	4	5
MOC 1	40	0.15	6	3
MOC 2	40	0.25	10	2
MOC 3	50	0.25	12.5	1

FORMULA: Score = Severity * Panic

NOTE that based on the cybersecurity severity score and the ability to cause public panic, MOC 3 still ranks highest as a cyber scenario worth preparing and executing a tabletop exercise for.

Figure 3. Weighted Priority for Impact B (resources)

Scenario	Severity	Resources	Score	Rank
MOV 1	30	0.25	7.5	2
MOV 2	10	0.10	1	5
MOV 3	40	0.10	4	4
MOC 1	40	0.15	6	3
MOC 2	40	0.25	10	1
MOC 3	50	0.15	7.5	2

FORMULA: Score = Severity * Resources

NOTE that based on the cybersecurity severity score and the ability to overwhelm local response capacity, MOC 2 now ranks highest as a cyber scenario worth preparing and executing a tabletop exercise for.

Figure 4. Weighted Priority for Impact A and B (both panic and resources)

Scenario	Severity	Panic	Resources	Score	Rank
MOV 1	30	0.15	0.25	7.5	2
MOV 2	10	0.10	0.10	1	5
MOV 3	40	0.10	0.10	4	4
MOC 1	40	0.15	0.15	6	3
MOC 2	40	0.25	0.25	10	1
MOC 3	50	0.25	0.15	7.5	2

FORMULA: Score = Severity * Panic * Resources

Manipulation of control scenario two—communications distributed denial-of-service, internally and externally, with capacity/threat to manipulate, modify, and disrupt process control systems—became potentially more impactful than manipulation of control scenario three—third-party access to takeover process control systems of cell block doors only—as a cyber scenario worth preparing for. Planning and training for a scenario that cuts off internal and external communications and includes uncertainty surrounding cyber-physical impacts is a more robust scenario than direct access to a limited OT/ICS asset or a potential ransomware situation that has limited cascading impacts.

Standardized Priority Score = 6.51

The standardized priority score can be used to compare entities from various sectors based on likely real-world scenarios, expected severity, and impacted populations. Another entity with different severity and impact calculations may have a total score of 4.35, for example. It is scalable; a company can compare different facilities and a city or sector or agency can work to enhance protections for the top 10 percent of entities in their purview of responsibility or scope, creating a starting point for addressing the most critical of critical targets and building cross-sector resilience.

FORMULA **Standardized Priority Score** = (Sum Panic) * (Sum Severity) / Sum Severity **OR** (38)*(36)/210

CONCLUSION

When considering whether assets or functions are more important, the answer is concretely somewhere in between—it always depends on the operation, product, or service. Evaluating entities and sectors against how well they implement cybersecurity requirements and best practices is abundant in complexity but limited in scope. Meanwhile, focusing on technology regulation leads to time-consuming and expensive audits and standardizing unrelated sectors yields vague guidance that becomes difficult to implement and enforce. Hypothetical cyber-physical scenarios quickly become convoluted with technical contingencies, competing priorities, overlapping authorities and analysis gaps.

Like the CARVER Target Analysis and Vulnerability Assessment tool, a similar way to standardize and prioritize what is most important from a cyber perspective is needed and must include impact analysis that goes beyond the cyber incident itself to consider scenarios that also impact public panic and the ability to overwhelm local response capabilities.[25] The methodology proposed in this paper is a simple scoring system that provides a repeatable mechanism that is suitable for prioritization based on real-world cyber scenarios, cyber-physical impacts, and fallout analysis.

Some sector-specific target and attack data exists, but there is still too much fear, uncertainty, and doubt driving tabletop exercises. Hopefully in the future, cyber policy and preparedness will have processes akin to the Homeland Security Exercise and Evaluation Program, with the key ingredient being a common approach.[26] This methodology will not resolve all critical infrastructure cybersecurity and systemically critical infrastructure debates. It will take widespread adoption to be most useful, offering a strategic way to scope and prepare for effective tabletop exercises and to compare entities across various sectors and jurisdictions.

[25] "What is the CARVER Target Analysis and Vulnerability Assessment Methodology?" SMI Consultancy, https://www.smiconsultancy.com/what-is-carver.

[26] "Homeland Security Exercise and Evaluation Program," Federal Emergency Management Agency, https://training.fema.gov/programs/nsec/hseep/.

ABOUT THE AUTHOR

Danielle Jablanski is a nonresident fellow at the Cyber Statecraft Initiative under the Atlantic Council's Digital Forensic Research Lab (DFRLab) and an OT cybersecurity strategist at Nozomi Networks, responsible for researching global cybersecurity topics and promoting operational technology (OT) and industrial control systems (ICS) cybersecurity awareness throughout the industry. Jablanski serves as a staff and advisory board member of the nonprofit organization Building Cyber Security, leading cyber-physical standards development, education, certifications, and labeling authority to advance physical security, safety, and privacy in public and private sectors. Since January 2022, Jablanski has also served as the president of the North Texas Section of the International Society of Automation, organizing monthly member meetings, training, and community engagements. She is also a member of the Cybersecurity Apprenticeship Advisory Taskforce with the Building Apprenticeship Systems in Cybersecurity Program sponsored by the US Department of Labor.

ACKNOWLEDGEMENTS AND SPECIAL THANKS TO

David Batz
Edison Electric Institute

Chris Blask
Cybeats

Bryson Bort
SCYTHE

Ron Brash
Adolus

Ron Fabela
Synsaber

Daryl Haegley
United States Air Force

Trey Herr
Atlantic Council

William Loomis
Atlantic Council

Steve Luczynski
Accenture

Jen Pedersen
Cybersecurity and Infrastructure Security Agency

Bob Kolasly
Exiger

Megan Samford
Schneider Electric

Keenan Skelly
Shadowbyte

Emma Stewart
National Rural Electric Cooperative Association

Nik Urlaub
MITRE

Munish Walther-Puri
Exiger

Tiffany Strauchs Rad
Anatrope, Inc.

Atlantic Council

Board of Directors