Research Report

BRIDGET R. KANE, STEPHEN WEBBER, KATHERINE H. TUCKER, SAM WALLACE,
JOAN CHANG, DEVIN McCARTHY, DENNIS MURPHY, DANIEL EGEL, TOM WINGFIELD

Threats to Critical Infrastructure

A Survey

Critical infrastructure in the United States supports the prosperity of the nation and its people. It permeates the daily lives of citizens, underpinning the safety and security of the general public and ensuring the economic well-being of the nation, yet the health of these assets, systems, networks, and facilities is often taken for granted. In 1997, the President's Commission on Critical Infrastructure Protection wrote, "life is good in America because things work . . . we are able to assume that things will work because our *infrastructures* are highly developed and highly effective."[1] But what if things did not work? What points of systems weakness exist, and how do these weaknesses contribute to opportunities for the destruction or disruption of critical resources and essential services?

In this report, we analyze threats and hazards to critical infrastructure and examine the vectors by which an adversary might conduct attacks against the homeland. We also look at the cascading effects of an attack and other impacts resulting from infrastructure age and maintenance and from weather challenges. These threats are demonstrated across critical infrastructures on a daily basis, but it is easy to become desensitized to such risks and vulnerabilities—particularly when not presented as part of a holistic picture of threats in aggregate. Here, we offer characterizations of various types of threat actors and vectors to raise awareness of systemic vulnerabilities and threat environments that can affect our critical infrastructure.

This report provides a foundation for understanding threats against critical infrastructure; it is intended to aid policymakers and related audiences in surveying the threat landscape and understanding (1) challenges related to policies, plans, capabilities, resources, and coordination and (2) information-sharing mechanisms required for response, recovery, and mitigation. Our hope is that this work will contribute to preparedness efforts by providing a foundation for further inquiry into critical issues.

KEY FINDINGS

- Impacts resulting from critical infrastructure attacks or vulnerabilities are often intensified by interdependencies and cascading effects across sectors and geographic boundaries; therefore, singular events are not really singular and will have outsize effects.
- There is a high degree of interdependence in some sectors; the resulting difficulty in isolating the effects of an attack to a single actor or category makes attribution particularly challenging.
- Hesitancy by private organizations to share details about specific threats or threat actors often stems from concerns regarding customer confidence, legal liabilities, or proprietary technology; this hinders information-sharing efforts, planning, response, recovery, and collaboration between affected entities and other stakeholders.
- Infrastructure protection often requires a deep understanding of targeted infrastructure; highly trained individuals are needed to address these mitigations at the system level and work with other sector experts on cross-sector impacts.
- Some sectors have underinvested in much-needed enhancements to infrastructure networks, assets, systems, and facilities; this increases the likelihood of disruption and interruption of services.
- Sector authorities are often decentralized and assets are largely privatized; resulting silos can create challenges in coordination and complicate efforts to maintain and enhance critical infrastructure.

Background Information

What Is Critical Infrastructure?

The definition of *critical infrastructure* varies by source. We focus on two sources for this effort. First, the USA Patriot Act defines the term as "systems and assets, whether physical or virtual, so vital to the United States that the incapacity or destruction of such systems and assets would have a debilitating impact on security, national economic security, national public health or safety, or any combination of those matters."[2] Second, the Cybersecurity and Infrastructure Security Agency (CISA) further identifies 16 critical infrastructure sectors designated in Presidential Policy Directive 21 (PPD-21)[3] that are "part of a complex, interconnected ecosystem"—"their incapacitation or destruction would have a debilitating effect on national security, national economic security, national public health or safety, or any combination thereof."[4]

Further compounding this intricacy are the interdependencies that exist across sectors. Because of the interconnected nature of critical infrastructure systems, it is probable that damage to one system will adversely affect another. These interdependencies are the mainspring of cascading, cross-sector (and, perhaps, cross-geographical) impacts that present challenges for response efforts.

Approach

We first conducted an open-source literature review for each sector to understand possible threats, threat actors, and impacts (both to national defense and socioeconomic well-being). We also conducted interviews with subject-matter experts (SMEs) both within and outside RAND. Our sectors were categorized based on literature related to the original 16 sectors as identified by PPD-21.[5] We narrowed those 16 sectors based on perceived criticality and opportunities for consolidation, and we reorganized our sector analysis into seven categories for conciseness and clarity: energy, transportation, financial services, communications, health care, water, and municipal services.[6] Several sectors were kept as defined by PPD-21. We grouped others under "parent" sectors—for example, we categorized "dams" under "water." A few, such as chemical or commercial facilities, are only briefly noted in terms of relevant sector-related impacts. The resulting high-level categorization allowed us to address larger assets, systems, and networks while retaining the ability to discuss smaller sectors via interdependencies in practice. This approach gave us valuable foundational knowledge for each sector that we could leverage in building out our framework.

Abbreviations

ATM	automated teller machine
CISA	Cybersecurity and Infrastructure Security Agency
COVID-19	coronavirus disease 2019
DDoS	distributed denial of service
DHS	U.S. Department of Homeland Security
DoD	U.S. Department of Defense
EPA	U.S. Environmental Protection Agency
FAA	Federal Aviation Administration
FBI	Federal Bureau of Investigation
GAO	U.S. Government Accountability Office
GPS	Global Positioning System
ICS	industrial control systems
OTS	operational technology systems
PNT	position, navigation, and timing
PPD-21	Presidential Policy Directive 21
SLTT	state, local, tribal, and territorial
SME	subject-matter expert

Threats to critical infrastructure often occur in a cross-sector fashion. Instead of analyzing threat vectors by themselves, we combined our sector-specific research and repackaged those details under a threat-based framework consisting of cyberattacks, physical sabotage, and aging infrastructure and environmental threats. In addition, we draw on reports of recent attacks and vulnerabilities in U.S. critical infrastructure systems to inform both our foundational overviews and our threat vector surveys. These real-world events demonstrate probable effects, interdependencies, and challenges likely to stem from sector disablement or disruption.

Threat actors are diverse and include state actors with sophisticated cyber capabilities, nonstate criminal organizations (often with financial motives), insider threats, and domestic terrorists or other extremist groups.

Threat Actors and Targets

Critical infrastructure threat vectors are the means by which an actor targets critical infrastructure (or the age-related vulnerabilities inherent in critical infrastructure that increase the likelihood of sector disruption or interruption), such as the identification of targets and malicious actors. Infrastructure encompasses systems, assets (whether physical or virtual), and component parts—such as people, structures, facilities, information, materials, and processes; this presents a significant landscape of susceptible targets vulnerable to a variety of threats that can be examined by both defenders and adversaries.[7] In the event of an attack, targets might be selected based on the primary goals of the threat actor, the vulnerability and accessibility of the target, and the attacker's tools and capabilities.

Threat actors are incredibly diverse and include state actors (such as China and Russia—or affiliated organizations) with sophisticated cyber capabilities; nonstate criminal organizations, often with financial motives (such as hacktivists or crime syndicates); insider threats; and domestic terrorists or other extremist groups. The motives of these groups vary. Threat actors conduct cyberattacks for a variety of reasons, such as to make money, to spy or steal information, to sabotage or otherwise disrupt the target, to destroy data, to test cyber tools and/or target vulnerabilities, to draw attention to a cause or issue, or to gain leverage on an unrelated issue.

For example, a crime syndicate might target the networks of a private company with a *ransomware* (malware that blocks file access until a ransom is paid) attack for financial gain; a state actor might disrupt another state's energy grid to influence that state's decisionmaking regarding a border dispute; or a domestic terrorist might physically attack gas lines to sow discord and gain public awareness for their cause. Alternatively, a hacking group might gain access to systems and networks to test whether a particular cyber tool will be effective or to probe the vulnerabilities of the target, or a terrorist group might conduct physical attacks to transportation systems or highly populated facilities with the intent to cause immediate, substantial harm against a civilian populace.

Background on Sectors

To inform the discussion of threats, we first provide some foundational background on each of our seven sectors. Here, we present brief, high-level overviews of each sector with a primary focus on the composition of each (specifically, their key assets, systems, and facilities) and a description of impacts regarding sector interruption and sector dependencies. This information is critical for understanding relationships among threat vectors, actors, and targets. Specific threat vectors and related effects—such as shortcomings related to aging infrastructure or cyberattacks—will be discussed in detail in subsequent sections. These overviews are intentionally broad and intended to provide a holistic familiarity with critical infrastructure. There are an abundance of detailed, sector-specific issues and policies for each sector; future research should continue to leverage this information to further identify interdependencies between each in support of threat mitigation efforts.

Energy

The U.S. population is highly dependent on energy for personal use and to enable economic activity—energy underpins both economic and social stability. CISA categorizes the energy sector's resources and assets into three components: electricity, oil, and natural gas.[8] For the purposes of this overview, we divide the energy sector into two subsectors—(1) electricity and (2) oil and gas—because of key differences in production and distribution facilities.

Electric Power Infrastructure

Assets. Power infrastructure is composed of a large network of power generation plants along with the transmission and delivery lines that connect them with end users across the country. CISA estimates that the United States has more than 6,413 power plants,[9] and the American Society of Civil Engineers reports that the United States has 600,000 miles of backbone transmission lines and 5.5 million miles of local distribution lines.[10] The diverse array of sources fueling the production of electricity creates a wide variety of assets: coal power plants; nuclear power plants; hydroelectric plants; natural gas power plants; and renewable energy infrastructure, such as solar panels and windmills.

Impacts of Disruption. Disruptions and shortages in the supply of electricity have myriad direct ramifications (such as power outages, inefficiencies, and costly repairs), and they create the potential for cascading effects across other critical infrastructure sectors: loss of power to such key facilities as hospitals and banks, internet blackouts, or nonfunctional traffic lights. A prolonged collapse of grid infrastructure could cause conditions that seriously endanger human life. For hospitals, prolonged loss of power means that machines and equipment that keep patients alive cannot run, emergency surgeries cannot occur, and patients lose access to critical care. During weather events, such as extreme heat or extreme cold, prolonged power outages risk vulnerable populations overheating or freezing to death. Prolonged power loss at water purification plants reduces access to clean and safe drinking water. These are a few of many examples of cascading hazards related to prolonged power outages.

Oil and Gas Infrastructure

Assets. Oil and gas infrastructure encompasses a wide variety of assets, including oil refineries, natural gas pipelines, oil rigs, drills, and regulatory systems. Before oil and natural gas reach their end users, they must travel through a series of physical systems. Among these are production wells, import and export facilities, and other key junctures (such as distribution and transmission lines).[11] The United States has more than 190,000 miles of oil pipelines and 2.4 million miles of gas pipelines.[12]

Impacts of Disruption. Disruptions to oil and gas infrastructure have impacts beyond the immediate loss of energy. Acute disruption or damage to pipelines can create environmental disasters, such as oil spills, that could hurt water and food supplies. Sustained disruptions could prevent people from being able to heat their homes or fuel their cars. The degradation of the oil and gas subsector would have significant cascading effects across other critical infrastructures. Dependencies on oil and gas affect much of society; some examples are large-scale transportation, manufacturing, agriculture and the creation of industrial feedstock, and supply chain management.

Transportation

The ability to move physical goods and people from one point on the map to another is contingent on a vast network of infrastructure systems related to transportation. This collective body of transportation infrastructure is one of the 16 critical infrastructure sectors identified by PPD-21.[13] For the purposes of this overview, we divide the transportation sector into four subsectors of critical infrastructure: maritime; air; rail; and roads, bridges, and tunnels. This overview highlights subsector assets and impacts to national defense and socioeconomic well-being in the event of infrastructure disruption or disablement.

Maritime Infrastructure

Assets. Maritime infrastructure encompasses not only the nation's sea ports, merchant shipping (including personnel, companies, and their business operations), and vessels that move cargo but also wind turbines, oil rigs, and undersea cable landings. The United States has more than 300 ports, each of which has additional infrastructure (for example, docks, piers, and channel harbors).[14] Maritime assets remain highly intertwined with other transportation assets because cargo must be transported from ports across the country using road, rail, or air assets.

Impacts of Disruption. The nation's economic dependence on maritime infrastructure means that disruptions to this subsector sector could damage international trade, supply chains, and economic stability. Forty percent of U.S. international trade by value moves over the oceans, which accounted for about 18 percent of gross domestic product as of 2020.[15] Disruptions might also produce cascading disruptions to other sectors, such as the energy and financial sectors. Some ports (and associated shipping capabilities) are key to the oil and gas industry, carrying implications for the energy sector and global markets.[16] Disruption could also limit military capabilities because the military is heavily dependent on the maritime sector to project power around the globe. The majority of the Time Phased Force Deployment Data for most contingencies would move by sea, which is the primary way to move heavy equipment, fuel, and munitions into theater.[17]

Air Infrastructure

Assets. When it comes to the air subsector, the nation's airports, airlines, and heliports are supported by complex systems, such as air traffic control, navigation systems, and airport business operations. Other assets (such as landing strips, fueling facilities, and flight schools) are critical to continuing operations within the sector. CISA estimates that the United States has roughly 19,700 airports, heliports, and landing strips;[18] the Federal Aviation Administration (FAA) reports that there are more than 14,000 air traffic controllers working in 700 FAA facilities.[19]

Impacts of Disruption. Disruption of air assets affects not just passenger air transit but also the supply chain and other sectors. Airlines move many high-end or perishable trade goods into the United States and carry a significant amount of air freight domestically. Disruptions could reduce the movement of goods critical for other sectors, such as food, medicine, chemicals, or raw materials. Like the maritime subsector, disruptions in the air subsector can limit military capabilities. The military conducts most of its day-to-day personnel movements by air (with a heavy reliance on commercial and contracted services) and, in a contingency necessitating rapid deployment, might use air travel to move the majority of personnel into theater.

Rail Infrastructure

Assets. The rail subsector encompasses freight rail, which is essential to the domestic U.S. economy, and commuter rail, which is essential to the functions of many urban centers. Rail assets consist of rail track, rail cars, terminals, and operational systems. CISA estimates that freight rail assets factor in "138,000 miles of active railroad, over 1.33 million freight cars, and approximately 20,000 locomotives."[20] For passenger rail, Amtrak operates routes that cover more than 21,400 miles,[21] and several U.S. cities have subway systems on which they are dependent, such as Boston, New York City, and Washington, D.C.

Impacts of Disruption. Like the other transportation subsectors, disruptions to rail assets hinder supply chains, other critical infrastructure sectors, and military capabilities. Without a functional freight rail system, critical goods cannot be moved across the country. Moreover, the rail carriers, railroad tracks, and trains that make up the rail sector intersect with the nation's networks of bridges and tunnels, which could either facilitate or act as chokepoints to the flow of people and goods. In a military contingency, freight rail would move vital supplies to ports in support of a deployment, meaning that a disruption would degrade military readiness.

Road, Bridge, and Tunnel Infrastructure

Assets. Roads, bridges, and tunnels facilitate movement along the nation's highways, railways, and waterways. CISA reports that the United States has more than 4 million miles of roads, 350 tunnels, and more than 600,000 bridges, creating a large roadway system that covers the entire country.[22] Other assets in this sector are traffic control measures (such as traffic lights), driver licensing systems, operational systems, bus transit, and commercial vehicles.

Impacts of Disruption. Disruption to roadway infrastructure would halt daily life for the millions of Americans who drive or ride to work, school, and life-sustaining shops. Impassible roadways limit access to health care, food, education, and other necessities of life. Disruptions would also halt the movement of goods and cause severe economic impacts because roads, bridges, and tunnels represent facilitators (or, again, chokepoints) to socioeconomic viability or national defense. Like every other transportation subsector, limited movement reduces the military's ability to effectively use supplies and personnel.

Financial Services

Assets. The sector is generally defined by four categories of services provided: (1) deposit, consumer credit, and payment system products; (2) credit and liquidity products; (3) investment products; and (4) risk transfer products.[23] These four categories are highly interdependent; within each of these categories, there are systemically important actors whose size and interconnectedness within the financial sector mean that issues with these institutions would result in significant disruption across the sector.[24] At the individual level, many Americans most commonly engage with the financial services sector via depository institutions and products. They use banks, banking apps, money transfer services, credit card services, and cryptocurrency wallets, which are all important assets within the financial sector. Additionally, mortgages and other forms of lending are dependent on the use of credit and liquidity products.[25] The proliferation of online banking has entangled these assets with communications infrastructure, such as the internet and cellular networks.

Impacts of Disruption. The consequences stemming from the loss or interruption of these products and assets to the U.S. economy and daily life are severe. Quick access to money enables people to earn wages, buy food and other necessary goods, seek medical treatment, and save money for the future; any disruptions to this system endanger these basic services. Furthermore, the financial sector allows for the effective operation of most other critical infrastructure sectors, which need to buy and sell goods and services to operate. Disruptions can also cause sector institutions to suffer reputational and confidence losses from customers, regulators, and society, making them less likely to share details with authorities to help hamper attacks. Thus, the impact of disruptions on systemically important institutions and markets can have a far greater impact than just the immediate monetary losses incurred, which can spread to similar institutions or across the entire sector with negative consequences for the economy.

> Disruptions to the communications sector cascade to all other critical sectors and have the capacity to bring life to a halt given the modern reliance on rapid communications.

Communications

Assets. The diverse mix of wireless, satellite, terrestrial, and legacy wired transmission systems that form communications infrastructure for information transfers has become an essential backbone to modern life in the United States. Communications infrastructure is made up a set of five overlapping networks (broadcasting, cable, satellite, wireless, and wireline) that allow access to different voice, video, and data applications on a single core network.[26] In addition to these networks, assets include global navigation systems (notably the Global Positioning System [GPS]) and position, navigation, and timing (PNT) infrastructure; personal communications devices (such as mobile phones); and fiber-optic cables.

Underinvestment in infrastructure and a lack of funding to mitigate disruptions persist across sectors.

Impacts of Disruption. The increasing sophistication and complexity of the communications sector allows for the rapid transmission of information that is central to the functionality of the U.S. economy, federal government, and other critical infrastructure sectors. The modernization of fiber-optic submarine cable technology alone has enabled financial transactions worth roughly $10 trillion and allowed transmission of substantial quantities of sensitive government and military communications on a daily basis.[27] Disruptions to the communications sector thus cascade to all other critical sectors and have the capacity to bring life to a halt given the modern reliance on rapid communications. In addition to its immense importance for the general public, communications are also key to sustained military readiness. Network-centric warfare, the Internet of Military Things, and other military products of the information age are generally inoperable without reliable communications infrastructure.

Some impacts stemming from the disruption of GPS and PNT infrastructure are civilian frustration, transportation challenges, loss of timing signals required to synchronize both power distribution and financial system transfers, and the inability to track cargo and other materiel; all of these would affect U.S. economic well-being and ability to project force internationally. Additionally, most PNT systems specifically rely on the U.S. GPS with the assumption that assets and networks will always be accessible and functional. Thus, if data from the U.S. system are unavailable or become corrupted, the systems that rely on those data will fall apart quickly because of the lack of a failsafe.[28] To combat this, the U.S. Department of Defense (DoD) is actively working to modernize the GPS and develop surrogate options, such as the U.S. Air Force's Resilient-Embedded GPS/Inertial Navigation System.[29] Alternatively, the proliferation of satellite constellations in low-Earth orbit could provide a failsafe in "instances where GPS is blocked or fails."[30]

Health

Assets. During the coronavirus disease 2019 (COVID-19) pandemic, a vast network of physicians, medical researchers, hospitals, and others were mobilized to safeguard the homeland from a pervasive and deadly threat. Those people and assets are the vanguard of the Healthcare and Public Health Sector, one of the 16 critical infrastructure sectors designated in PPD-21. Health care focuses on localized delivery and management; the public health portion centers on total population health and operates across all levels of government. Assets include public health; government response and program offices; and private services, such as patient care, health IT, health plans and buyers, mass medical emergency management services, medical materials, and laboratories.[31] In this report, we refer to a *health sector*, which corresponds directly with the Healthcare and Public Health Sector outlined by the White House and CISA.

Impacts of Disruption. Disruptions to the health sector can harm the health and well-being of the general public by causing both short-term effects (such as not having enough beds for patients at a hospital) and long-term effects related to the health and longevity of a population. On the one hand, the health sector is highly dependent on other sectors for operations and services, such as emergency services, energy, water and wastewater systems, and information technology; on the other hand, it is also responsible for keeping the employees in these other critical sectors healthy. Because of the nature of this relationship, disruptions to other critical sectors hinder the health sector, and disruptions to the health sector hinder every other sector.

Water

Assets. Many billions of gallons of clean drinking water are distributed daily to the American people. New York City alone consumes more than one billion gallons of water every day.[32] We consider water infrastructure to consist of both water and wastewater—it "includes the infrastructure necessary to transport, treat, store, distribute, and remove drinking water and wastewater and to control water quantity and quality."[33] These networks and assets rely on a complicated cyber infrastructure made up of information technology and operational technology systems (OTS) alongside the matrix of relevant policy authorities, the partnership mechanisms that represent stakeholders, and government entities that interact with these mechanisms.[34]

Impacts of Disruption. When water and wastewater infrastructure is disrupted or dysfunctional, affected communities are at risk of illness, long-term medical effects, lack of clean water, and large economic burdens. Disruption to clean water has significant cascading effects on other critical infrastructure sectors: The health sector relies on clean water for patient care and treatment. Disruptions to the water supply could hamper the ability of hydroelectric powerplants to produce energy. The employees in every critical infrastructure sector (and, of course, the general population) rely on clean water to survive.

Municipal Services

Assets. The municipal services sector includes public services (for example, education, voting, sanitation, schools, food inspection, transportation, safety, welfare, and emergency and emergency preparedness services) that are provided by state, local, tribal, and territorial (SLTT) governments. This sector does not include services tendered by the federal government, such as sheltering and the distribution of emergency supplies by the Federal Emergency Management Agency in the event of a natural disaster. Although some of these systems and assets are addressed in other sectors (water, for example), we retain the distinction of the municipal services sector because of an emphasis on the role of local and regional governments in the running and sustainment of essential services. Municipal governments store private data (such as voter, tax, and social security details) and have the responsibility of ensuring that data sources remain safe and secure.[35] The emergency services subsector consists of first-responder personnel and resources, including such facilities and equipment as police and fire departments and paramedic services.[36] The government facilities subsector consists of buildings owned or leased by national, state, or local governments as a part of the municipal sector.[37]

Impacts of Disruption. Municipalities and the services they provide are essential to health, education, and modern human life, meaning that disruptions to municipal services hamper routine and essential services.[38] Disruptions to police or fire services endanger public safety; disruptions to voting services inhibit the right of citizens to participate in democratic governance; and disruptions to government databases result in privacy breaches of personal identifiable information. Given the importance of operational cities and towns to the resiliency of the nation, the municipal services sector is of major concern not only for the welfare of ordinary citizens but also for U.S. national security.

Challenges in Responses to Disruptions to Critical Infrastructure Sectors

Common challenges hinder stakeholders from preventing and effectively responding to disruptions across critical infrastructure sectors. Some of these challenges are underinvestment in infrastructure, a multiplicity of stakeholders, a lack of communication, a lack of planning, and the under-identification and underreporting of cyber threats.

Underinvestment in infrastructure and a lack of funding to mitigate disruptions persist across sectors. For example, in the water sector, the U.S. Environmental Protection Agency (EPA) has calculated that $472.6 billion is needed to maintain and improve drinking water infrastructure alone over the next 20 years.[39] In the communications sector, more than 30 million Americans live in areas without access to broadband internet infrastructure.[40] In the municipal sector, local governments lack funding to improve their cybersecurity and prevent cyber disruptions.[41] These funding gaps inhibit infrastructure maintenance and the development of new infrastructure designed to mitigate service disruptions.

This multiplicity of public and private critical infrastructure stakeholders—such as owners, operators, regulators, and others—complicates the coordination of infrastructure standards, equipment, disaster response plans, and mitigation and response efforts. For example, in the energy sector, stakeholders include regulatory authorities and geographically dispersed owners and operators of sector-related infrastructure. These stakeholders might have inconsistent policies and procedures for response activities—for example, communications and information-sharing. They would therefore find it difficult to develop and share a common operating picture of an unfolding incident and to coordinate response activities and ensure that those activities are complementary. The diversity of energy stakeholders means that disruption mitigation efforts might be implemented in a piecemeal and uncoordinated manner across the sector, resulting in persistent inconsistencies in the how energy security and other processes are regulated across the country. In the municipal sector, which often functions in siloed organizational components, agencies built to serve one population might not coordinate with similar agencies for other populations: For example, a local senior citizen agency might not communicate with an agency built to monitor public health. The COVID-19 pandemic exemplified some of these compounding challenges, with failures in continuity and coordination of services leaving vulnerable seniors exposed to a rapidly spreading virus.[42]

Finally, cyber threats can be difficult to identify and can spread quickly across network-linked infrastructure; stakeholders also often underreport these threats. In aggregate, these challenges make it more difficult to facilitate a timely response and prevent threats from spreading. Financial sector institutions, like others, underreport cybercrimes for fear of eroding consumer confidence or incurring legal liabilities.[43] These risks grow proportionally with the increased use of technologies connected to the internet within infrastructure. The rise of "smart cities"—municipalities that use "information and communication technologies . . . to increase operational efficiency, share information with the public and improve both the quality of government services and citizen welfare"[44]—and of "smart grid" electric systems also increases vulnerability to cyber disruptions by creating more points of access for cyber threats.

Survey of Threat Vectors and Risks

In this section, we survey two major *threat vectors*, or means by which an actor targets critical infrastructure: cyberattacks and physical sabotage. We also examine other risks to critical infrastructure related to aging and environmental hazards.

Cyberattack Threats and Threat Actors

According to the U.S. Department of Homeland Security (DHS), "Cybersecurity threats to critical infrastructure are one of the most strategic risks for the United States."[45] The United States is increasingly connected to and dependent on the internet, either via individual devices and programs for personal use or as a byproduct of the modernizations of various systems and assets that undergird the operationality of every critical infrastructure sector. In short, technological innovation has resulted in a massive attack surface that provides countless opportunities for nefarious actors to threaten U.S. national security, economic prosperity, public health, and safety.

For example, state actors target infrastructure to collect information and gain access to industrial control systems (ICS) (among other web-based inroads) in the energy, water, and transportation sectors. Sophisticated attacks by these actors against government and private-sector organizations "support espionage, extract intellectual property, maintain persistent access on networks, and potentially lay a foundation for future offensive operations."[46] Alternatively, organized crime syndicates might engage in cybercrime for financial gain by targeting critical networks. These are only a few of countless examples of cyber threats to critical infrastructure.

Infrastructure can also be damaged or destroyed via inadvertent cyber activity: For example, a network operator might accidentally delete or modify software, leading to infrastructure malfunction or disablement. In early 2023, the FAA halted all domestic departures when its Notice to Air Missions system, an outdated system dating back to the 1970s, failed.[47] After a preliminary review, the FAA determined that "contract personnel unintentionally deleted files while working to correct synchronization between the live primary database and a backup database."[48]

This section focuses only on intentional and malicious cyber threats: We address some ways in which these attacks might occur against targets across selected infrastructure sectors as perpetrated by a variety of actors.

Energy Cyberattacks

Cyberattacks by both state and nonstate actors represent a significant threat to the energy sector. In the past few years, there has been an uptick in cyberattacks by both state actors (including backdoor electronics in Chinese-made transformers in 2020) and nonstate actors.[49] The patchwork regulatory nature and technical connectivity of this sector provide myriad opportunities for cyber exploitation. For both the electricity and the oil and gas subsectors, this might include ICS and supervisory control and data acquisition systems linked to operational technology networks.

Cyberattacks to ICS, particularly, are on the rise.[50] Nefarious organizations might lead intrusions into ICS and other industrial networks for reconnaissance and research purposes and might engage in adversarial use of destructive malware, leading to a shutdown of power utilities for a large number of people.[51] In 2023, hackers linked to Russia released a "first ever" malware toolkit, called PIPEDREAM, capable of infiltrating a variety of U.S. ICS (as opposed to being tailored for one specific system) on U.S. systems to try take electric and gas facilities offline, highlighting the "U.S. energy supply's vulnerability to a crippling cyber assault."[52]

To highlight an attack with geopolitical implications, a massive 2020 outage in Mumbai has widely been attributed to Chinese actors in a coordinated cyber campaign intended to push back against border skirmishes in the Galwan Valley, which lies along the western sector of the "line of actual control" between India and China, close to a disputed area that is controlled by China.[53] Power was cut to 20 million people, causing cascading effects across industries—trains shut down, the stock markets closed, and hospitals switched to emergency generators to keep ventilators running during a significant COVID-19 outbreak.[54] Some of the vulnerabilities that increase the likelihood of these attacks might be attributed to the implementation of smart grid electricity networks, which use "digital and other advanced technologies to monitor and manage the transport of electricity from all generation sources to meet the varying electricity demands of end users."[55] The transition to modern power systems assists in bolstering grid resiliency by increasing capacity of the transmission system, preventing faults, and facilitating the integration of grid-edge devices (such as electric vehicles),[56] but the resulting operational connectivity makes the sector increasingly vulnerable to cyberattacks.

Cyber threats can be difficult to identify and can spread quickly across network-linked infrastructure.

For the oil and gas subsector, systems that make up the refining process are vulnerable to similar incursions that target hazardous refining elements and can cause explosions or loss of life. Therefore, petrochemical refineries represent a high-value target for hostile or adversarial actors. This is exemplified by the recent discovery of a Russia-linked malware strain designed to attack industrial facilities, which provided the ability to disrupt electrical power generation and cause physical harm.[57]

Transportation Cyberattacks

Cyber threats to the transportation sector are numerous and, again, often prey on the modernization and

Cyber threats to the transportation sector are diverse in nature. Malign intent varies, but it is often aimed at disrupting supply chains and logistical networks that facilitate such things as air travel and shipping.

connectivity of operational systems and ICS. Transportation companies are also high-value targets for criminal organizations seeking financial gain. For the maritime subsector, cyberspace provides what is perhaps the most prevalent vector. Many ports depend on OTS, specifically ICS, to move cargo and load it onto ships.[58] Ports are also vulnerable to physical sabotage. As a vector for entry into the United States, ports are vulnerable to malicious actors who might wish to move weapons or contraband into the homeland. Vessels themselves often also depend on OTS to function along with a multitude of other digital and automated functions; each of these is vulnerable to cyberattacks and must be taken into consideration when assessing the landscape of threats.[59]

In 2017, the Russia-deployed NotPetya virus (likely intended to target Ukraine's energy infrastructure) disrupted port operations in the United States and around the globe, devastating the business operations of the international shipping company (and DoD contractor) Maersk.[60] In 2014, the U.S. Senate Armed Services Committee found that multiple threat actors linked to the People's Republic of China had penetrated the business networks of key DoD contractors involved in shipping and that they could target U.S. logistics networks in the future.[61] For a sense of how disruption to maritime infrastructure could harm the United States, the Long Beach port strike of 2015 cost the U.S. economy about $1 billion per day.[62]

The air subsector is also vulnerable to cyber threats, which might consist of attacks on navigation systems, air traffic control, or government and civilian IT networks. That vulnerability was partially realized in 2023, when an FAA system outage of unknown cause grounded flights across the country in the first nationwide ground stop since September 11, 2001.[63] State actors have also disrupted the U.S. air subsector. In 2022, Russian hackers caused mild disruption by attacking U.S. airport websites for Los Angeles International and Chicago O'Hare, among others.[64] Although the attack did not result in interruption to internal airline operations, it demonstrates the vulnerability of the cyber infrastructure that undergirds the sector. As with maritime domain, Chinese hackers have penetrated networks of civilian airlines that would contract with DoD to move personnel during a contingency.[65]

Railroads also depend on OTS/ICS, which are often built into much older system architectures not originally designed for that automation (similar to the modernization issues observed in the energy sector).[66] Because of these limitations, these systems often lack the appropriate cybersecurity protections to combat modern cyberattacks, meaning cyberspace is a vector by which train safety, signaling, and switching functions could be disrupted. Recently, a group of dissidents from Belarus targeted Russia's rail networks with cyberattacks to disrupt its ability to supply the invasion of Ukraine.[67] Another area of concern is *railheads*—the points on a railroad at which roads and other transportation routes might begin or terminate—and other key junctures that would be used to move military equipment for loading.[68] Regarding public transportation, it was revealed in 2021 that Chinese threat actors hacked into New York's subway system.[69] This is especially troubling because disrupting commuter or freight rail has immediate implications for essential functions, the viability of domestic supply chains, and the ability to move materiel during a military deployment.

Cyber threats to the transportation sector are diverse in nature. Malign intent varies, but it is often aimed at disrupting supply chains and logistical networks that facilitate such things as air travel and shipping. That said, it would also be possible for an adversary to cause more-immediate and overt harm as a result of tampering with electronic traffic signs or other safety and signaling functions.

Financial Services Cyberattacks

The financial sector is ripe for targeting via cyberattack. Again, this is primarily because of increasing interconnectivity of internet-enabled devices and other connected systems.[70] Worrisome incidents include those that "corrupt the integrity of financial data, such as records, algorithms, and transactions; few technical solutions are currently available for such attacks, which have the potential to undermine trust and confidence more broadly."[71] Threat actors often have common ideological or financial motives. For example, state actors, state-sponsored groups, or terrorist organizations might seek to create societal disruptions by causing permanent data corruption, leaks, or distributed denial of service (DDoS) attacks on financial services infrastructure whereas cybercriminals might target cash or credential theft for financial gain.[72]

According to an IBM report, incidents targeting finance and insurance organizations made up more than 22 percent of all observed cyberattacks in 2021.[73] The nature of cyberattacks continues to change as these actors, particularly criminal organizations, devise methods to successfully penetrate financial institutions. One telling example is the rapid increase in ransomware attacks throughout the early 2020s, with one survey of financial institutions reporting an increase of more than 1,300 percent in ransomware attacks in 2021.[74] The frequency and sophistication of such attacks is likely to continue to increase with the rise of ransomware as a service, which allows for less technologically sophisticated actors to access advanced ransomware tools by paying to deploy ransomware built or managed by someone else.[75] Common methods of cyberattack that target actors in the financial services sector are phishing, malware, web application attacks, vulnerability exploitation, and DDoS attacks.[76]

Another important trend for financial services—though not limited to this sector—is the rise of nation-state attack campaigns and hybrid warfare, which has resulted in a growth of cyberattacks targeting governments, militaries, and the business sector.[77] These attacks can be employed in conjunction with kinetic and nonkinetic attacks against a target nation, as was the case in the Russian invasion of Ukraine in February 2022. Financial, defense, aviation, and IT service organizations in Ukraine and Lithuania were attacked with a novel malware file in the hours preceding the physical invasion of Ukraine, leveraging access that the attackers had acquired in 2021.[78]

Communications Cyberattacks

Despite the emergence of wireless and satellite access networks, the vast majority of data that individuals, businesses, and governments rely on is transmitted through wireline access networks. Access network providers, such as telecommunications and internet service providers, are a particular target of cyberattacks by criminal groups, which can exploit legacy systems, the increasing connectivity of devices (including the Internet of Things), and greater interconnectivity between networks, ultimately seeking access to the important data managed by network providers. These attacks can leverage different methods, such as ransomware, DDoS, and domain name service attacks.[79]

Similar attacks by state or state-affiliated actors also occur and can be coordinated with other kinetic and nonkinetic attacks, such as Russia's major attack on Ukraine's internet service provider Viasat in the hours preceding the military invasion of the country in February 2023.[80] Such attacks offer adversaries a way to conduct *gray zone* or hybrid warfare, as mentioned previously. In May 2021, a DDoS attack targeted Belnet, an internet service provider serving much of the Belgian government and several major businesses in the country. That attack coincided with the expected testimony to the Belgian Parliament of a Uyghur woman on China's detention camps in the Xinjiang province of Western China.[81]

Threats to GPS and PNT infrastructure have also become more widespread as technology has improved. In previous years, the primary threats to these systems were adversarial state actors. However, technology has progressed to the point that "with a few hundred dollars of commercially available hardware and free software, hackers can block or replace GPS signals."[82] This has widened the aperture for other malign actors, such as crime syndicates, to target electronic signals over localized areas, often jamming or spoofing signals as a cover for vehicle theft or drug trading.[83] It is worth briefly expanding on two spoofing mechanisms. Measurement spoofing "introduces RF [radio frequency] waveforms that cause the target receiver to produce incorrect measurements of time of arrival or frequency of arrival or their rates of change."[84] Data spoofing "introduces incorrect digital data to the target receiver for its use in processing of signals and the calculation of PNT."[85] Both of these can be particularly harmful to targeted systems and have such varied implications as the incorrect time-stamping of agricultural goods, interference with financial transactions, and other applications across sectors.

Health Cyberattacks

Cybersecurity threats to health care organizations and patient safety are increasingly common.[86] The modernization and interconnectivity of health care–related data and technology leave systems ever more vulnerable to cyberattacks. These attacks are often implemented for financial gain. According to a *Journal of the American Medical Association* (*JAMA*) Health Forum Study, ransomware attacks against health care organizations have doubled in the past five years, with health clinics as the most common victims.[87] Of those attacks, 44.4 percent disrupted the delivery of health care, with 8.6 percent of the cohort noting operational disruptions of more than two weeks.[88]

In 2022, CommonSpirit Health—one of the nation's largest nonprofit health systems—experienced a ransomware attack, delaying surgeries and medical care; the attack also exposed the personal information of more than 620,000 patients across more than 700 sites and 142 hospitals in 21 states.[89] Attacks such as this can have downstream effects: For example, health care providers might be required to divert patients to other locations and might not be able to access patient records that are essential for care delivery.[90] In the case of CommonSpirit Health, IT systems experienced network outages and unusual activity,[91] which allowed unauthorized third-party access to sensitive personal information for current and former health center patients, thus violating patient privacy.

Water Cyberattacks

Cyberattacks are the most significant threat to water systems because the sector relies heavily on automation. With the rise of new technology, everything from pumps and valves to chemical treatment systems can be operated remotely. The sector's reliance on supervisory control and data acquisition "systems, industrial control systems, and programmable logic controllers has dramatically reduced manpower costs. However, these advances have also introduced significant cybersecurity risks, as these systems are increasingly intertwined with systems connected to the internet."[92] The EPA is attempting to address this problem with the creation of a steering committee of experts that will examine ways to prevent hackers from taking control of elements of infrastructure or providing inaccurate operational and water quality information to water system operators.[93] However, cyberattacks on water infrastructure—such as a March 2019 attack on a utility in Ellsworth County, Kansas, in which a former employee attempted to shut down processes for cleaning and disinfecting water[94]—are still disturbingly common.[95]

Municipal Services Cyberattacks

In 2020, nearly one-half of ransomware attacks in the world targeted municipalities.[96] Municipal databases present significant targets for cybercriminals because of their substantial sensitive data holdings and appealingly vulnerable networks. These attacks are expensive: It is not uncommon for cyberattacks to cost states up to tens of millions of dollars in financial damages and ransom fees.[97] In the United States, from 2018 to 2022, at least 330 cyberattacks struck SLTT government agencies, affecting more than 230 million people and costing $70 billion in downtime.[98] The most-affected states were Texas, Georgia, California, Florida, and Pennsylvania.[99]

Most municipal cyberattacks use ransomware. A majority of these methods rely on obtaining user credentials. In a phishing scam, a trusted source is impersonated by email to obtain information or to install malware; in this way, a single click can expose a database to malicious actors. That said, alternative techniques and procedures are becoming increasingly common, such as brute force attacks and credential stuffing (which target vulnerabilities from inside systems) and password spraying (which also takes advantage of compromised user credentials).[100]

These methods threaten most cyber-physical systems that underpin critical infrastructure sectors across the United States. An example of this threat occurred in 2018, when a ransomware cyberattack took down the city water department website of Atlanta, Georgia. It affected computer systems and encrypted data, blocking database access, postponing court dates, and hindering payments for public services. Employees could not turn on work computers, nor could they access wireless internet. The hackers, later identified as Iranian members of the SamSam group,[101] demanded more than $50,000 in Bitcoin payment to release information.[102]

Municipalities have a particularly difficult time defending against cyber threats because the enhanced security measures to prevent them are costly. Even though there are obvious vulnerabilities and real costs to these attacks, about one-half of states have no line item budget for cybersecurity.[103] More than one-third of those remaining did not increase funding in recent years, either.[104] Each local government is unique, and, to effectively respond to a cyberattack, municipalities must be able to implement best practices in understanding which threats and impacts they are most likely to encounter.[105] Municipalities often lack the training and knowledge required to understand the threat and identify and implement these security measures.[106]

Physical Sabotage and Attack Threats

Malicious actors use sabotage and physical attacks (in addition to cyberattacks) to harm physical assets. CISA defines *physical sabotage* as “taking deliberate actions aimed at harming an organization’s physical infrastructure (e.g., facilities or equipment).”[107] This broad definition includes such actions as destroying power substations, bombing medical clinics, and shooting municipal employees. Attackers commonly use guns, explosives, chemicals, and other weapons to damage or destroy physical infrastructure.

> There is an extensive network of physical infrastructure assets across the country, many of which are vulnerable to potential sabotage and attacks.

There is an extensive network of physical infrastructure assets across the country, many of which are vulnerable to potential sabotage and attacks. A wide variety of malicious actors—foreign terrorist organizations, current and former employees, domestic extremists, criminal organizations, and others—might have the ability to carry out physical attacks on infrastructure systems and assets. In recent years, insiders (including employees and contractors) and domestic extremists have attacked critical infrastructure systems. Insiders are a particularly potent risk because they often have access to physical assets that outsiders do not have. Domestic extremists are also high-risk threat actors. Many domestic extremists have attempted to physically attack critical infrastructure to create an atmosphere of chaos and sow societal discord.[108] These malicious actors can target any number of physical vulnerabilities to threaten critical infrastructure. As with cyber threats, critical infrastructure can also be damaged or destroyed by a physical accident—for example, a train conductor might inadvertently cause a train to derail. This section

> Disruptions to transportation infrastructure, whether caused by a saboteur, an attacker, or nonmalicious incidents or accidents, can cause significant economic losses.

focuses on physical threats from malicious actors: Here, we outline some of these examples and opportunities for each sector.

Energy Physical Threats

Physical attacks on energy infrastructure are becoming more frequent: Physical attacks on electrical systems were up by nearly 80 percent in 2022 compared with the previous year,[109] and the Electricity Information Sharing and Analysis Center tallied 1,700 reports of attacks, vandalism, and suspicious activity against electricity infrastructure in 2022.[110] The significant number of assets in the energy sector present many opportunities for physical attacks and sabotage. Power substations, gas pipelines, and nuclear energy plants all serve as tempting targets for malicious actors attempting to cause chaos, disrupt the economy, or profit off of damaged infrastructure.

Physical attacks are increasingly perpetrated by domestic terrorists and extremist groups.[111] In 2022, three individuals pleaded guilty to terrorism-related charges for a plot to knock out parts of the electric grid in what the Federal Bureau of Investigation (FBI) described as an attempt to attack regional power substations with the expectation that the damage would lead to economic distress and civil unrest.[112] In late 2022 and early 2023, at least nine substations were attacked in North Carolina, Washington state, and Oregon, leaving tens of thousands without power.[113] Environmental activists and ecoterrorists have also sought to tamper with oil and natural gas energy infrastructure. An environmental activist group called the "Valve Turners," known for taking physical action against the fossil fuel industry, has tampered with emergency shutoff valves to close oil pipelines on multiple occasions.[114]

Transportation Physical Threats

Transportation sector assets are susceptible to physical sabotage and attack; aside from roads, shipping, and public transportation, attacks might particularly emphasize the destruction or obstruction of railheads, junctures, bridges, or tunnels. Malicious actors might cause fires, explosions, chemical detonations, leaks, or blazes inside tunnels or other transportation infrastructure, which can have severe effects. Commuter rail and passenger trains in urban centers are soft targets, meaning "locations that are easily accessible to large numbers of people and that have limited security or protective measures in place making them vulnerable to attack."[115] Trains can be physically attacked by malicious actors, which occurred in 2004 and 2005 terrorist bombings in London and Madrid.[116] The air subsector is also vulnerable to physical attack through such methods as (1) hijackings similar to the September 11, 2001, terrorist attacks on multiple aircraft and (2) bombings or strikes with such weapons as shoulder-fired rockets.[117] Experts also worry about the potential of unmanned systems to attack aircraft, airports, or disrupt airspace management.[118] Physical disruption of transportation infrastructure has serious implications for civilians, the economy, and the military. The 2022 conflict between Russia and Ukraine has illustrated the military value of sabotaging strategic transportation infrastructure. The Kerch Strait bridge in occupied Crimea was targeted with explosives in October 2022, presumably to disrupt Russian military operations.[119] The Russia-Ukraine war also highlights the complementary and overlapping nature of the authorities for protecting critical infrastructure: civilian homeland security and military homeland defense.

Disruptions to transportation infrastructure, whether caused by a saboteur, an attacker, or non-malicious incidents or accidents, can cause significant economic losses. For example, the collapse of interstate bridges in Minneapolis, Minnesota; Memphis, Tennessee; and Philadelphia, Pennsylvania (all vital routes for commercial transportation) have strained supply chains.[120] An eight-day strike at ports in Southern California in 2012 cost an estimated $8 billion in economic losses.[121] Although none of these incidents were caused by a saboteur or an attacker, the examples illustrate the costs associated with transportation infrastructure disruption.

Financial Services Physical Threats

Physical attacks are also sources of threats to the financial services sector. Although increasing digitization and dispersal of critical communications infrastructure for the financial sector has decreased this risk over the past decade, physical disruptions to key institutions remain a risk to the sector.[122] Banks, credit unions, automated teller machines (ATMs), and the stock exchange are all appealing targets for a physical attack and represent points of vulnerability. Although there has been a steep decline in the number of bank robberies in the past two decades, the number of ATM crimes has soared, increasing 600 percent from 2019 to 2020.[123] Financial service locations also serve as soft targets for potential shootings and other mass casualty events. A 2023 shooting at a bank in Louisville, Kentucky, left five dead and eight injured.[124]

Communications Physical Threats

Physical attacks on key hardware components of the communications sector could be carried out by a wide variety of actors. One area of vulnerability is the submarine cables that carry the bulk of information between the East Coast of the United States and Europe: Potential peer and near-peer adversaries have the capability to damage or sever these cables,[125] which could lead to partial or complete outages of telephone and internet services across the northeastern United States. On a smaller scale, the accidental damage caused by fishing vessels to two submarine cables running to Scotland's Shetland Islands in October 2022 demonstrated the potential impacts of a physical attack. Many residents were without telephone, internet, and landline services for more than a day, and all network and mobile links to the Islands' airport stopped working.[126]

Communications servers and towers are also vulnerable to attack. In recent years, anti-5G conspiracy theorist extremists have sabotaged 5G technology: In 2020, for example, extremists bombed an AT&T communications facility in Nashville, Tennessee. Anti-5G extremist attacks increased dramatically in 2019 and 2020:[127] Anti-5G attacks in 2020 coincided with conspiracies surrounding the transmission of COVID-19, resulting in dozens of arson attacks against cellular towers in Europe.[128] Industry and government stakeholders are concerned that other extremists will conduct copycat attacks targeting communications infrastructure in the future.[129]

Health Physical Threats

Physical attacks on hospitals and other health care infrastructure endanger the lives of vulnerable patients and employees. The wide variety of medical equipment and medication present in health care facilities remains at risk of sabotage and tampering. Approximately 70 percent of medication tampering, fraud, and theft incidents take place in such health care facilities as hospitals, pharmacies, medical centers, and ambulance services.[130] Furthermore, hospitals are soft targets for shootings and other violent attacks. Between the years 2000 and 2017, there were hundreds of hospital shootings.[131] In 2018, health care workers suffered 73 percent of all nonfatal workplace violence injuries across the United States.[132]

Water Physical Threats

Physical attacks and sabotage directed against water infrastructure have the capacity to immediately endanger lives and create a public health crisis. Attacks against water treatment facilities, water and sewage lines, or pumping stations could disrupt the distribution of potable water. Attacks against dams or large reservoirs could create catastrophic flooding and reduce the water supply. Biological attacks that sabotage the water supply with chemicals or toxins could generate a mass public health crisis.[133]

Despite the numerous points of physical vulnerability in water systems, there have been few physical attacks on water infrastructure. The majority of sabotage occurs in the cyber realm because of the highly automated nature of water infrastructure. That said, insiders—often disgruntled former employees—might leverage both cyber and physical opportunities for attacks. In 2019, a former employee at a water treatment facility in Ellsworth County, Kansas, attempted to shut down water disinfectant and cleaning procedures.[134] In 2021, a former contractor remotely hacked into the water systems for the town of Discovery Bay, California, attempting to uninstall critical software from the main system.[135] Although these attempts at sabotage were cyber-based, the insider threat problem can manifest itself just as well through physical attacks, which would pose a major threat for water facilities.

Municipal Services Physical Threats

Although the main threat vector against municipal infrastructure is cyber incursions, physical attacks on municipal services or personnel do occasionally occur. Municipal targets can include local government buildings, computer equipment, and emergency services infrastructure. A large portion of municipal assets are people—first responders, local government officials, and poll workers. These people present a soft target for physical attacks but often are not protected by physical security measures. Among local officials surveyed by the National League of Cities, 60 percent reported that their office lacked a strategy or action plan to respond to harassment, threats, and violence.[136]

In terms of real-world examples of physical attacks against municipal services, a young man committed a jihad-inspired attack in 2022 using a machete-like knife with which he assaulted three New York police officers at an entry access checkpoint to the New Year's Eve celebration at Times Square.[137] Threats to law enforcement officers have been on the rise: The FBI found that more law enforcement officers were feloniously killed in the line of duty in 2021 than any year since 2001.[138] In addition to police officers and first responders, local government officials and poll workers are targets of physical attacks. A 2021 survey from the National League of Cities found that 81 percent of local officials reported experiencing harassment, threats, or violence.[139] A 2023 survey from the Brennan Center for Justice found that nearly one in three election officials have been abused, harassed, or threatened.[140]

Aging Infrastructure and Environmental Risks

Unlike cyber and physical threats, aging infrastructure and environmental risks are not caused by malicious actors. For example, materials used in the construction of critical infrastructures degrade over time. However, even though these forces are largely outside human control, policymakers can control how people adapt to these pressures. Aging infrastructure can be retrofitted or replaced to ensure safety. Infrastructure can be built to modern, climate-resilient standards based on local disaster risk.

The United States has struggled to modernize infrastructure to meet these age and environment demands. The 2021 Infrastructure Report Card from the American Society of Civil Engineers gave the nation's infrastructure a "C minus" grade, an improvement from the 2017 "D plus" grade.[141] Aging infrastructure contributed to this poor grade. The report notes that some sectors have "staggering maintenance deficits" and that older legacy assets, such as water and transportation networks, "suffer from chronic underinvestment and are in poor condition."[142] Aging infrastructure might fail on its own, or the process by which it degrades might make it increasingly vulnerable to cyber and physical threats and environmental risks.

Although infrastructure has always been vulnerable to damage from extreme weather, climate change has exacerbated these risks. CISA notes that, in the past 50 years, "Extreme weather events have become far more disruptive and destructive than ever recorded and are projected to steadily worsen as global warming progresses"[143]—this affects all critical infrastructure sectors. Extreme heat, droughts, wildfires, extreme cold, severe storms, flooding, cyclones, and sea level rise all pose threats to critical infrastructure.[144] A 2021 report from First Street Foundation found that 25 percent of all critical infrastructure across the nation is at risk of becoming inoperable from flooding.[145] Extreme weather and aging assets pose a risk to all critical infrastructure sectors.

Energy Infrastructure and Environment

Extreme weather events—such as cold snaps, high winds, and hurricanes—strain the resiliency of the electric grid.[146] In 2022, the average electricity customer experienced five hours and 30 minutes without power—a two-hour decline from the previous year driven by fewer interruptions from major weather events, such as hurricanes, wildfires, and snowstorms.[147] In 2021, Winter Storm Uri overwhelmed the Texas power grid,[148] resulting in 4.5 million homes without power and 246 deaths, largely resulting from hypothermia.[149] Hurricane Ian, a category-4 hurricane that struck Florida in 2022, left 2.7 million customers without power.[150] These extreme weather events pose a serious risk to energy infrastructure.

Aging infrastructure poses similar risks. Deteriorating energy infrastructure is susceptible to outages, inefficiencies, and costly repairs. These risks are particularly worrisome given the age of energy infrastructure: More than 70 percent of electricity transmission and distribution systems are in the second half of their 50-year lifespan, and more than "half of the natural gas transmission and distribution network was installed before 1960."[151] But upgrading these systems is costly, and a lack of shared understanding regarding vulnerabilities of ICS could result in legacy components being integrated into broader systems, even when doing so might constitute a cybersecurity vulnerability.

Some environmental threats that could interrupt power generation are not related to extreme weather events. For example, wildlife and vegetation can cause significant damage. In 1987, a squirrel "took out the power to a NASDAQ computer center for nearly an hour and a half, stopping an estimated 20 million shares from being traded."[152] A quick search reveals countless events in the past year alone linking squirrels (which chew through electrical wires) to power outages, often for thousands of customers at a time. Jellyfish have also impaired the processes of nuclear power plants: They have clogged the cooling pipes of nuclear reactors and caused plant shutdowns in the United States, Sweden, Scotland, Japan, and Australia, to name just a few of the countries affected.[153] There is no standard prevention mechanism for these intrusions (though scientists are exploring early warning system options), and plant closures—even if brief and temporary—are costly.[154]

Extreme weather and aging assets pose a risk to all critical infrastructure sectors.

Transportation Infrastructure and Environment

Extreme weather increases the stress on roadways; bridges; and rail, port, and aviation assets. These weather events might acutely damage assets or slowly reduce their lifespans. In the short term, the EPA notes that flooding can "affect roadways and tunnels, weaken roadway materials, and cause traffic congestion."[155] Heavy rains can cause mudslides, which have destroyed roads in California, Colorado, and New York. Hurricane Ian washed away portions of the Sanibel Causeway and Matlacha Pass Bridge, which link several barrier islands to mainland Florida.[156] The Federal Highway Administration reports that roughly 21 percent of all vehicle crashes, on average, are related to bad weather, and roughly 5,000 people are killed in weather-related crashes each year.[157] The increased stress on transportation systems from extreme weather might not be apparent for years but can unexpectedly shorten the lifespan of infrastructure, especially infrastructure built to different standards before extreme weather events became common. Aging transportation infrastructure poses a safety risk, impedes effective transportation, and affects supply chains. According to the *New York Times*, the U.S. Department of Transportation estimates that "obsolete road designs and poor road conditions are a factor in about 14,000 highway deaths each year."[158] In 2007, a bridge in Minneapolis along Interstate 35 collapsed, killing 13 people and injuring 145 more.[159] Although the collapse was attributed to a design error rather than aging infrastructure or environmental hazards, it demonstrates the human costs of infrastructure failure.[160] These risks are especially troubling given the advanced age of transportation infrastructure: 7.5 percent of all bridges in the United States are structurally deficient, and 178 million trips occur on these bridges per day.[161] The average age of all U.S. bridges is 44 years, which is of particular concern given that the lifespan for most bridges is 50 years.[162] Approximately 43 percent of public roadways are in poor or mediocre condition.[163]

Aging legacy banking systems are at increased risk of failure. These lagging systems pose a unique threat in a sector that has modernized in many areas.

In addition to posing safety risks, aging infrastructure reduces the efficiency of transportation and disrupts travel. For example, aging tunnel and bridge infrastructure is one factor that prevents Amtrak passenger trains from running at faster speeds between Washington and Boston;[164] the cost of safety equipment for faster trains and Amtrak sharing track with freight railroad also play a role in limiting the efficiency of trains.[165]

Financial Services Infrastructure and Environment

Extreme weather events present an immediate physical threat to financial assets. Banks, ATMs, and financial sector employees are vulnerable to floods, wildfires, hurricanes, and other extreme weather events. Superstorm Sandy in 2012 caused the closure of major equities exchanges for two days, including the New York Stock Exchange and Nasdaq Stock Market exchange.[166] Extreme weather has also affected financial services by altering the insurance industry. Insurance companies have withdrawn coverage in disaster-prone areas partly because of extreme weather, which contributes to higher premiums and fewer insurance choices. Farmers Insurance withdrew from Florida; State Farm, Allstate, and AIG have stopped taking new policies in California.[167] The places most at risk from extreme weather are also most vulnerable to these changing dynamics in the insurance market, amplifying the risk of dangerous weather.

Aging legacy banking systems are at increased risk of failure. These lagging systems pose a unique threat in a sector that has modernized in many areas. Legacy systems often run on a programming language called the Common Business-Oriented Language (COBOL), which was invented in 1959. A 2017 report from Reuters found that 43 percent of all banking systems were built on COBOL, despite the age of the system, and an estimated $3 trillion in daily commerce flowed through COBOL systems.[168] However, universities have prioritized newer programing languages (such as Python and Java) rather than focusing on COBOL, meaning that new programmers are less familiar with COBOL than previous generations and have less capacity to fix problems with the system.[169] As this gap grows, the continued use of legacy financial systems increases the danger that these financial systems will become inoperable and irreparable.

Communications Infrastructure and Environment

Communications assets—such as submarine cables, cell phone towers, and satellites—are vulnerable to extreme weather. Submarine cables carry more than 95 percent of all digital data traffic, making them critical for communication.[170] However, these cables are susceptible to the effects of climate change and severe weather. Sea level rise, storm tides, cyclones, coastal erosion, and river flooding all can damage underwater cables and land-based infrastructure—such as landing stations—necessary for communication.[171] Such assets as cell towers can be damaged by wildfires and other severe weather; for example, wildfires in Hawaii in August 2023 left parts of the island without access to cell service, phone connections, or 911 operators.[172] Other environmental effects from space, such as solar flares, can temporarily shut down or permanently degrade key communications components.[173]

Much of the country relies on older communications technology that is less reliable and suffers from slower communication. High-speed internet access, or broadband, remains unavailable in many parts of the country, often in more rural areas. Research from 2019 estimates that between 14.5 million and 42 million Americans lack access to broadband internet,[174] with the top 20 percent of household incomes being five times more likely to have broadband access than the bottom 20 percent.[175] In space, military satellite assets are often prone to technological obsolescence because of long development processes; sensors on the satellites can become outdated mere months after the satellite is placed in orbit.[176] A 2021 report from the Mitchell Institute asserts that legacy satellite systems have lower bandwidth, have more latency issues, and are not interoperable with some new technologies, all of which hampers communications.[177] Other age-related communications and satellite infrastructure vulnerabilities are poorly designed systems or user failure (often stemming from a lack of proper training), which can cause widespread disruptions to GPS and PNT systems. Additionally, there is a greater reliance on private-sector systems (such as Starlink) globally, which could create a new set of risks needing to be further evaluated.

Health Infrastructure and Environment

Extreme weather affects the buildings and equipment necessary to run health care facilities. Heat waves, hurricanes, blizzards, and cold snaps can harm the electric, water, and gas infrastructure that keeps hospitals functioning. In 2022, a major California city hospital, Santa Clara Valley Medical Center, experienced a power outage for several hours after a gas and power company substation failed on an unusually hot day. Some hospital backup generators failed, leaving patients, doctors, and staff in the dark. The emergency department was unable to admit patients who had suffered strokes, heart attacks, and trauma along with other patients who arrived by ambulance. Elective procedures were canceled, and surgery and trauma patients had to be evacuated to other parts of the hospital or different facilities.[178]

The large and complex system of physical assets that make up the health care network—including hospital facilities, medical equipment, and IT systems—requires continual funding for maintenance, infrastructure repairs, and essential upgrades. However, the COVID-19 pandemic stressed health care infrastructure and, according to the American Hospital Association, created revenue losses on the magnitude of $323.1 billion in 2020.[179] The association argues that this financial shortfall caused many hospitals to pause spending, thus delaying maintenance, infrastructure repairs, and upgrades. These age-related stressors are compounded by the cybersecurity risk posed by older and unpatched medical equipment and devices. According to the FBI, devices with outdated software and a lack of security features create vulnerability that can be exploited by cyber threat actors, affecting "healthcare facilities' operational functions, patient safety, data confidentiality, and data integrity."[180] Despite this risk, as of 2021, there was an average of 6.2 vulnerabilities per medical device, and more than 40 percent of devices at the end-of-life stage had inadequate security upgrades or patches. Issues related to aging infrastructure and environmental threats are crucial for the health care industry to consider as the sector prepares for an aging U.S. population that will increase the strain on health care facilities.

Water Infrastructure and Environment

Naturally occurring threats, such as contamination and natural disasters (for example, earthquakes and tornados), are a primary focus of the EPA. The agency conducts contaminant detection research and has application programming interfaces that can simulate disruptive incidents.[181] This helps utility companies better prevent and prepare for natural dangers. Other extreme weather conditions, such as drought, pose a risk to the amount of water in the system. The Colorado River system, which supplies drinking water to 40 million people and irrigates 5.5 million acres of farmland, has suffered substantial drought conditions that caused officials to worry that the river would dry up downstream, which occurs when reservoir water levels are too low to reach the intake valves and flow out of Lake Mead and Lake Powell.[182] In 2022, the reservoirs were at their lowest levels since their initial filling, storing roughly 25 percent of total capacity.[183] Persistent drought conditions threaten the entire water sector by removing the most essential component: the water itself.

In addition to unpredictable variables such as weather events, the sector is consistently behind in investment and maintenance on the millions of miles of pipelines that transport water through varying topographies.[184] On average, the drinking and wastewater pipes across the nation are 45 years old.[185] The age of these systems generates massive losses of clean water—water main breaks and other leaks result in more than 6 billion gallons of water lost per day.[186] As of 2021, an estimated 9.7 million to 12.8 million lead pipes still existed in the water network despite severe health risks from lead exposure, such as damage to the brain, nervous system, kidneys, blood cells, and cardiovascular system.[187] These aging and outdated systems pose a danger to human health and create inefficiencies in the water delivery system that would be problematic during a water shortage or crisis.

Municipal Services Infrastructure and Environment

Extreme weather events can affect municipal sector physical equipment, such as buildings and computers, and the people who work in this sector. This vulnerability to weather events is particularly notable given that municipal services, including police, fire, and emergency management services, are often critical during extreme weather situations. Potential cascading hazards might amplify these challenges: An effective emergency response from first responders requires power, running water, passable roads, and clear lines of communication, all of which are threatened by extreme weather events.

Municipal assets, such as school buildings and IT systems, are also aging. The threat related to these aging physical assets goes beyond simply leaving the people that work in them vulnerable; these buildings also often serve as emergency shelters, voting locations, and meeting forums, making their maintenance critical to keeping local municipalities functional. Despite this importance, 53 percent of public schools need repairs and modernization.[188] Outdated voting machines, or machines operated by poorly trained volunteer operators, are prone to failure and might be vulnerable to cyberattacks.[189] As described previously, aging municipal systems, limited budgets, and poor maintenance of these problems increase vulnerability to cyberattacks.[190]

Cascading Hazards

The impacts to infrastructure as described in response to each of the threat vectors and risks do not occur in vacuums. There are many interdependencies—“the behavior[s] and reliabilit[ies] of one system [that] can spread to another system”[191]—among sector assets that often result in outsize impacts and effects. To put the full interconnectivity of these sectors into perspective, we look to the health sector to demonstrate one succinct example of the impacts of cascading effects: Loss of power disrupts the functionality of hospitals and clinics, delays emergency procedures, harms the storage of lab samples, and makes equipment inoperable; without effective transportation, patients cannot visit medical facilities; clean water is crucial for patient hydration and the sterilization medical tools. These cascading effects, coupled with the large network of health care facilities across the country, create many points of vulnerability in health infrastructure.

As noted in our illustration of health interdependencies, damage to various sectors often creates ripple effects across other sectors and industries that rely on similar foundational scaffolding. For example, damage to the energy sector can hinder internet connections (in the communications sector) or the movement of people and goods (in the transportation sector). We cannot speak to all cascading hazards in this report because of the sheer volume of assets, interdependencies, and effects that might occur in response to various kinds of attacks. We do, however, we provide a few salient examples.

In 2001, a train carrying hazardous materials derailed in Baltimore's Howard Street Tunnel. This started a fire and ultimately caused significant disruption to the city.[192] The fire in the tunnel triggered a water main break, causing flooding and power loss. The fire also severed fiber-optic cables, resulting in disrupted internet services.[193] The incident lasted five days, caused five minor injuries, and cost an estimated $12 million in damages.[194] Later that same year, the September 11, 2001, terrorist attacks and sabotage of transportation infrastructure provided another clear example of downstream effects and cascading hazards. In the wake of September 11, some towns ran low on chemicals needed for water treatment after trains stopped moving because of safety concerns.[195] The attacks also led to the closure of the New York Stock Exchange as communications and other key services were knocked offline.[196] The digital infrastructures underpinning online banking and myriad other communications mechanisms rely on such physical inputs as energy infrastructure to operate, making the threat of power loss increasingly alarming.

The COVID-19 pandemic highlights another example of interlocking, infrastructure-related crises. This example is unique in that it focuses primarily on the soft infrastructure that maintains the economic, health, and educational elements of modern societies (versus hard infrastructure, such as roads and bridges). The inability for individuals to leave their homes forced greater reliance on energy and communications infrastructure and contributed to a sudden increase in demand for communications services.[197] This connectivity, in turn, increased the opportunity for cybercriminals to implement ransomware attacks on those working from home.[198] Strained health care systems and facilities, confinement measures, and sick individuals contributed to a disruption in the availability of workers in general; this included those working in public health and municipal functions, putting further stress on the ability of those sectors to respond to both related and unrelated crises. The American Society of Civil Engineers notes that "With the onset of the pandemic . . . municipal and state budgets are buckling under unprecedented demands, meaning less support is available for parks, schools, and other publicly-owned infrastructure precisely at the time we should be investing."[199]

The impacts to infrastructure as described in response to each of the threat vectors and risks do not occur in vacuums.

These examples are by no means exhaustive, and future research should involve an in-depth analysis of the inherent links in cascading attacks and the effects produced; this research would facilitate awareness and preparedness efforts.

Key Findings and Implications

In this report, we discuss threats and hazards to critical infrastructure and describe vectors by which the homeland is threatened. We provide an overview of seven key critical infrastructure sectors and detail cyber, physical, age, and environmental threats to each sector. This report provides a foundation for understanding threats against critical infrastructure and thus might be useful to policymakers and related audiences in surveying the threat landscape for critical infrastructure and understanding challenges related to sector- or threat-specific policy development and response efforts. We offer six key findings and implications that highlight potential challenges for a U.S. coordinated response to infrastructure-related crises:

1. Impacts resulting from critical infrastructure attacks or vulnerabilities are often intensified by interdependencies and cascading effects

across sectors and geographic boundaries; therefore, singular events are not really singular and will have outsize effects.

2. There is a high degree of interdependence in some sectors; the resulting difficulty in isolating the effects of an attack to a single actor or category makes attribution particularly challenging.
3. Hesitancy by private organizations to share details about specific threats or threat actors often stems from concerns regarding customer confidence, legal liabilities, or proprietary technology; this hinders information-sharing efforts, planning, response, recovery, and collaboration between affected entities and other stakeholders.
4. Infrastructure protection often requires a deep understanding of targeted infrastructure; highly trained individuals are needed to address these mitigations at the system level and work with other sector experts on cross-sector impacts.
5. Some sectors have underinvested in much-needed enhancements to infrastructure networks, assets, systems, and facilities; this increases the likelihood of disruption and interruption of services.
6. Sector authorities are often decentralized, and assets are largely privatized; resulting silos can create challenges in coordination and complicate efforts to maintain and enhance critical infrastructure.

The Biden administration is in the process of revising PPD-21,[200] which establishes national policy on critical infrastructure security and resilience and specifies the critical infrastructure security and resilience–related responsibilities of sector-specific agencies (now called Sector Risk Management Agencies).[201] PPD-21, issued in 2013, was written prior to CISA's establishment in 2018. The administration aims to rewrite PPD-21 with the intention of "clarify[ing] the roles, responsibilities, and services of the Sector Risk Management Agencies and the Cybersecurity and Infrastructure Security Agency (CISA) to coordinate a national effort to secure and protect against critical infrastructure risks."[202] Improvement to this directive and to the related National Infrastructure Protection Plan (including new, sector-specific plans), is a critical step toward addressing the vulnerabilities, threats, and potential challenges for a U.S. coordinated response to infrastructure-related crises. In addition to the federal government's efforts to support critical infrastructure security and resilience, SLTT and private-sector critical infrastructure stakeholders, such as owners and operators, must also prepare, mitigate, and ensure the resilience and security of critical infrastructure.

In this report, we describe the "wavetops" of sector interdependencies by citing examples of impacts caused by disruptive cascading effects to various systems and assets. However, we do not build out these links, which merit additional research. So do other topics, such as attacks combining multiple threat vectors (for example, coupling a sabotage with a cyberattack). Tangentially, the gray-zone tactics and hybrid warfare techniques that we mention briefly would benefit from further exploration. Future research should consider these tactics and use cases to provide a more robust view of the threat landscape.

Notes

[1] President's Commission on Critical Infrastructure Protection, *Critical Foundations*, p. 3.

[2] Pub. L. 107-56, Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism (USA PATRIOT ACT) Act of 2001.

[3] White House, Critical Infrastructure Security and Resilience. The 16 critical infrastructure sectors as recognized by PPD-21 are Chemical; Commercial Facilities; Communications; Critical Manufacturing; Dams; Defense Industrial Base; Emergency Services; Energy; Financial Services; Food and Agriculture; Government Facilities; Healthcare and Public Health; Information Technology; Nuclear Reactors, Materials, and Waste; Transportation; and Water and Wastewater.

[4] CISA, "Critical Infrastructure Systems."

[5] CISA, "Critical Infrastructure Sectors."

[6] CISA, "Critical Infrastructure Security and Resilience."

[7] Pub. L. 107-56, Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism (USA PATRIOT ACT) Act of 2001.

[8] CISA, "Energy Sector."

[9] CISA, "Critical Infrastructure Sectors."

[10] American Society of Civil Engineers, *2021 Infrastructure Report Card*.

[11] Coburn, "Oil and Gas Infrastructure."

[12] American Society of Civil Engineers, *2021 Infrastructure Report Card*.

[13] White House, Critical Infrastructure Security and Resilience.

[14] American Society of Civil Engineers, *2021 Infrastructure Report Card*.

[15] U.S. Maritime Administration, "Navigating a Stronger Future."

[16] Kramek, "The Critical Infrastructure Gap."

[17] Kramek, "The Critical Infrastructure Gap."

[18] CISA, "Transportation Systems Sector."

[19] FAA, "FAA Fact Book."

[20] CISA, "Transportation Systems Sector."

[21] Amtrak, "FY 2022 Company Profile."

[22] CISA, "Transportation Systems Sector."

[23] Financial Services Sector Coordinating Council, *Financial Services Sector-Specific Plan*.

[24] These designations include Systemically Important Financial Institutions; Global, Systemically Important Banks; and Systemically Important Financial Market Utilities.

[25] Financial Services Sector Coordinating Council, *Financial Services Sector-Specific Plan*; Tivnan, *Financial System Mapping*.

[26] The core network has several components, such as data operations centers, routing and switching equipment, domain name system servers, and fiber and copper transport nodes. See U.S. Department of Homeland Security, *Communications Sector-Specific Plan 2015*; and U.S. Government Accountability Office (GAO), *CISA Should Assess the Effectiveness of Its Actions to Support the Communications Sector*.

[27] Arghire, "Submarine Cables at Risk of Nation-State Sabotage, Spying: Report."

[28] CISA, "Understanding Vulnerabilities of Positioning, Navigation, and Timing."

[29] GAO, *GPS Alternatives*.

[30] Hampson, "This Alternative Could Stay on Target If GPS Fails" (caption).

[31] U.S. Department of Health and Human Services, *Healthcare and Public Health Sector-Specific Plan*.

[32] New York State Department of Environmental Conservation, "New York City Water Supply."

[33] Gamache, "Critical Infrastructure: Water and Wastewater Systems Sector."

[34] EPA, "Water and Wastewater Systems Sector-Specific Plan."

[35] Eytan, "Municipal Cyberattacks: A New Threat or Persistent Risk?"

[36] CISA, "Emergency Services Sector."

[37] CISA, "Government Facilities Sector."

[38] Eytan, "Municipal Cyberattacks: A New Threat or Persistent Risk?"

[39] EPA, "EPA's 6th Drinking Water Infrastructure Needs Survey and Assessment."

[40] White House, "Fact Sheet: The Bipartisan Infrastructure Deal."

[41] Eytan, "Municipal Cyberattacks: A New Threat or Persistent Risk?"

[42] Frye, "Pandemic Lessons: Improving Your Municipality's Continuity and Coordination of Services After COVID."

[43] Eling and Jung, "Heterogeneity in Cyber Loss Severity and Its Impact on Cyber Risk Measurement."

[44] Shea, "Smart City."

[45] DHS, "Secure Cyberspace and Critical Infrastructure."

[46] DHS, "Secure Cyberspace and Critical Infrastructure."

[47] Aratani, Duncan, and Laris, "As Southwest, FAA Probes Begin, Fallout Could Shape Flying for Years."

[48] FAA, "FAA NOTAM Statement."

[49] King, "How America's Power Grid Is Vulnerable to Undetected Cyberattack."

[50] GAO, *Offshore Oil and Gas*.

[51] Dragos, "Global Oil and Gas Cyber Threat Perspective."

[52] Miller, “Russian-Linked Malware Was Close to Putting the U.S. Electric, Gas Facilities ‘Offline’ Last Year.”

[53] “Galway Valley: China and India Clash on Freezing and Inhospitable Battlefield.”

[54] Sanger, “China Appears to Warn India: Push Too Hard and the Lights Could Go Out.”

[55] International Energy Agency, “Smart Grids.”

[56] Law, “Making Power Grids More Resilient.”

[57] Menn, “U.S. Warns Newly Discovered Malware Could Sabotage Energy Plants.”

[58] CISA, “Port Facility Cybersecurity Risks.”

[59] Transportation security SME, interview with the authors, November 15, 2022.

[60] Ileto, “Cyber at Sea: Protecting Strategic Sealift in the Age of Strategic Competition.”

[61] U.S. Senate Armed Services Committee, *Inquiry into Cyber Intrusions Affecting U.S. Transportation Command Contractors*.

[62] Transportation security SME, interview with the authors, November 15, 2022.

[63] Matza, “FAA Outage: US Airline Regulators Blame Contractor for Travel Chaos”; Roy and Sridhar, “Cyber-Threat Assessment for the Air Traffic Management System: A Network Controls Approach”; Thudimilla and McMillin, “Cyber-Physical Security of Air Traffic Surveillance Systems”; Tammimi, Hahn, and Roy, “Cyber Threat Impact Analysis to Air Traffic Flows Through Dynamic Queue Networks”; Tangel, “Why Planes Were Grounded for the First Time Since 9/11.”

[64] Romo, “Pro-Russian Hackers Claim Responsibility for Knocking U.S. Airport Websites Offline.”

[65] U.S. Senate Armed Services Committee, *Inquiry into Cyber Intrusions Affecting U.S. Transportation Command Contractors*.

[66] Figueroa Diaz, *An Analysis of Railway Industrial Control Systems Vulnerabilities*.

[67] Swain, “The Emerging Cyber Threat to the American Rail Industry.”

[68] Grohoski, *The Vulnerabilities of U.S. Strategic Ports to Acts of Sabotage*.

[69] Goldbaum and Rashbaum, “The MTA Is Breached by Hackers as Cyberattacks Surge.”

[70] Financial Services Sector Coordinating Council, *Financial Services Sector-Specific Plan*.

[71] Maurer and Nelson, “The Global Cyber Threat.”

[72] Ozarslan, “Key Threats and Cyber Risks Facing Financial Services and Banking Firms in 2022.”

[73] IBM Corporation, *X-Force Threat Intelligence Index 2022*.

[74] Henriquez, “Banking Industry Sees 1318% Increase in Ransomware Attacks in 2021.”

[75] Microsoft, “Ransomware as a Service: Understanding the Cybercrime Gig Economy and How to Protect Yourself.”

[76] Ozarslan, “Key Threats and Cyber Risks Facing Financial Services and Banking Firms in 2022.”

[77] FS-ISAC Global Intelligence Office, *Navigating Cyber 2022*; Kaffenberger and Kopp, *Cyber Risk Scenarios, the Financial System, and Systemic Risk Assessment*.

[78] “Ukraine: Disk-Wiping Attacks Precede Russian Invasion.”

[79] Mariano, “Cybersecurity Landscape in the Telecommunications Sector.”

[80] National Cyber Security Centre, “Russia Behind Cyber Attack with Europe-Wide Impact an Hour Before Ukraine Invasion.”

[81] Quach, “Belgian Parliament Halts China Uyghur ‘Genocide’ Debate After DDoS Smashes ISP Offline”; CISA, “China Cyber Threat Overview and Advisories.”

[82] CISA, “Understanding Vulnerabilities of Positioning, Navigation, and Timing.”

[83] Brunker, “GPS Under Attack as Crooks, Rogue Workers Wage Electronic War.”

[84] European Aviation Safety Agency, “Stand-Alone Airborne Navigation Equipment Using the Global Positioning System Augmented by the Satellite Based Augmentation System.”

[85] European Aviation Safety Agency, “Stand-Alone Airborne Navigation Equipment Using the Global Positioning System Augmented by the Satellite Based Augmentation System.”

[86] Balasubramanian, “With Increasing Reliance on Healthcare Technology, Cybersecurity Is a Growing Concern.”

[87] Neprash et al., “Trends in Ransomware Attacks on US Hospitals, Clinics, and Other Health Care Delivery Organizations, 2016–2021.”

[88] Fox, “Half of Ransomware Attacks Have Disrupted Healthcare Delivery, JAMA Report Finds.”

[89] Murez, “Patient Care Delayed at Large Hospital Chain After Ransomware Attack”; Page, “CommonSpirit Health Says Patient Data Was Stolen During Ransomware Attack.”

[90] CISA, “Healthcare and Public Health Sector.”

[91] McKeon, “CommonSpirit Health Faces Class Action Lawsuit in Wake of Healthcare Data Breach.”

[92] Montgomery and Logan, “Poor Cybersecurity Makes Water a Weak Link in Critical Infrastructure.”

[93] EPA, “Water Infrastructure Resilience.”

[94] Lyngaas, “Kansas Man Indicted in Connection with 2019 Hack at Water Utility.”

[95] Boubaker, “Twenty Years of Cyberattacks on the World of Water.”

[96] Coker, “Local Government Organizations Most Frequently Targeted by Ransomware.”

[97] Larson, “Municipal Cybersecurity.”

[98] Bischoff, "Ransomware Attacks on US Government Organizations Cost over $70bn from 2018 to October 2022."

[99] Bischoff, "Ransomware Attacks on US Government Organizations Cost over $70bn from 2018 to October 2022."

[100] Enzoic, "Cyberattacks on Municipalities & How to Defend Against Them."

[101] Benner and Perlroth, "Iranians Accused in Cyberattacks, Including One That Hobbled Atlanta."

[102] Kearney, "Atlanta Takes Down Water Department Website Two Weeks After Cyber Attack."

[103] National Association of State Chief Information Officers, "Ensure Dedicated Cybersecurity Funding for State and Local Governments with CIOs as Key Decisionmakers."

[104] KnowBe4, *The Economic Impact of Cyber Attacks on Municipalities*.

[105] Thompson, "Cybersecurity Best Practices for Municipalities."

[106] Preis and Susskind, "Municipal Cybersecurity."

[107] CISA, "Defining Insider Threats."

[108] Clarke et al., "The Targeting of Infrastructure by America's Violent Far Right."

[109] King, "How America's Power Grid Is Vulnerable to Undetected Cyberattack"; Brangham, "FBI Foils Extremist Plot to Bring Down Baltimore's Electrical Grid."

[110] National Conference of State Legislatures, *Human-Driven Physical Threats to Energy Infrastructure*.

[111] Englund, "Domestic Terrorism Is Evolving."

[112] Bergengruen, "'Is There Something More Sinister Going On?'"

[113] Levenson, "Attacks on Electrical Substations Raise Alarm."

[114] Nijhuis, "'I'm Just More Afraid of Climate Change Than I Am of Prison.'"

[115] DHS, *U.S. Department of Homeland Security Soft Targets and Crowded Places Security Plan Overview*, p. iii.

[116] Boucek, "Security Is the Watchword for U.S. Mass Transit Systems."

[117] Dillingham, "Vulnerabilities Still Exist in the Aviation System."

[118] Transportation security SME, interview with the authors, November 15, 2022.

[119] Savitz, "Beware the Explosive Vessels."

[120] Maruf, "Will the I-95 Collapse in Philadelphia Hurt the Economy?"

[121] Whitecomb and Gorman, "UPDATE 6—Settlement Reached to End 8-Day Los Angeles Port Strike."

[122] Osipovich, "After the 9/11 Attacks, Wall Street Bolstered Its Defenses."

[123] Pinkerton, "ATMs and Crime."

[124] Hassan and Bogel-Burroughs, "What We Know About the Louisville, Ky., Bank Shooting."

[125] Scott, "Will Russia Attack Undersea Internet Cables Next?"; Wall and Morcos, "Invisible and Vital: Undersea Cables and Transatlantic Security."

[126] Carrell, "Telephone and Internet Restored in Shetland After Cable Damage."

[127] Krill, "The Evolution of Critical Infrastructure Targeting by Violent Extremists"; FBI, "FBI Releases Report on Nashville Bombing."

[128] "Conspiracy Theorists Burn 5G Towers Claiming Link to Virus."

[129] Arkin, "Why Nashville Bomb Investigators Feared Copycat Attacks by 5G Conspiracists"; Flaherty, Sturm, and Farries, "The Conspiracy of Covid-19 and 5G."

[130] Hermsen, "Drug Tampering and Product Substitution in Healthcare Facilities."

[131] CISA, "Hospitals & Healthcare Facilities."

[132] Boone, "Attacks at US Medical Centers Show Why Health Care Is One of the Nation's Most Violent Fields."

[133] Copeland, *Terrorism and Security Issues Facing the Water Infrastructure Sector*.

[134] Shorman and Vockrodt, "Ex-Employee Remotely Hacks Kansas Water Treatment Plant."

[135] U.S. Attorney's Office, Northern District of California, "Tracy Resident Charged with Computer Attack on Discovery Bay Water Treatment Facility."

[136] Anthony et al., *On the Frontlines of Today's Cities*.

[137] U.S. Department of Justice Office of Public Affairs, "Federal Charges Announced Against Maine Man Who Carried Out Machete Attack in Times Square on New Year's Eve in Name of Jihad."

[138] Tucker and Krishnakumar, "Intentional Killings of Law Enforcement Officers Reach 20-Year High, FBI Says."

[139] Anthony et al., *On the Frontlines of Today's Cities*.

[140] Edlin and Norden, "Poll of Election Officials Shows High Turnover Amid Safety Threats and Political Interference."

[141] American Society of Civil Engineers, *2021 Infrastructure Report Card*.

[142] American Society of Civil Engineers, *2021 Infrastructure Report Card*, p. 2.

[143] CISA, "Extreme Weather and Climate Change."

[144] CISA, "Extreme Weather and Climate Change."

[145] First Street Foundation, *The 3rd National Risk Assessment*.

[146] Barone, "The U.S.'s Creaky Power Grid Is No Match for Worsening Weather Catastrophes."

[147] U.S. Energy Information Administration, "U.S. Electricity Customers Averaged Five and One-Half Hours of Power Interruptions in 2022."

[148] Ling, *The Timeline and Events of the February 2021 Texas Electric Grid Blackouts*.

[149] Texas Department of State Health Services, "February 2021 Winter Storm-Related Deaths—Texas."

[150] Ciampoli, "Outages Post-Hurricane Ian Down to Less Than 500,000 in Florida."

[151] American Society of Civil Engineers, *2021 Infrastructure Report Card*, p. 46.

[152] Peterson, "Are Squirrels a Bigger Threat to the Power Grid Than Hackers?"

[153] Laskow, "The Five Best Times Jellyfish Shut Down Power Plants."

[154] D'Agostino, "Jellyfish Attack Nuclear Power Plant. Again."

[155] EPA, "Climate Change Impacts on Transportation."

[156] Treisman, "Damage from Hurricane Ian Cuts Sanibel Island off from Florida's Mainland."

[157] Federal Highway Administration, U.S. Department of Transportation, "How Do Weather Events Impact Roads?"

[158] Nixon, "Human Cost Rises as Old Bridges, Dams and Roads Go Unrepaired."

[159] National Transportation Safety Board, *Collapse of I-35W Highway Bridge Minneapolis, Minnesota, August 1, 2007*.

[160] Minnesota Legislative Reference Library, "Minneapolis Interstate 35W Bridge Collapse."

[161] American Society of Civil Engineers, *2021 Infrastructure Report Card*.

[162] American Society of Civil Engineers, *2021 Infrastructure Report Card*.

[163] American Society of Civil Engineers, *2021 Infrastructure Report Card*, p. 107.

[164] Shepardson, "Amtrak Wants $8 Billion in US Funding for Infrastructure Projects."

[165] McFarland, "Amtrak Might Add More Than 50 New Routes. But They Still Won't Be Faster Than a Car."

[166] Fox, Riley, and Yousuf, "NYSE and Nasdaq Closed as Hurricane Sandy Hits."

[167] McDaniel, "Citing Climate Change Risks, Farmers Is Latest Insurer to Exit Florida."

[168] Irrera, "Banks Scramble to Fix Old Systems as IT 'Cowboys' Ride into Sunset."

[169] Shead, "Universities Won't Teach 'Uncool' COBOL Anymore—But Should They?"

[170] Clare et al., "Climate Change Hotspots and Implications for the Global Subsea Telecommunications Network."

[171] Lindoo, *Bringing COBOL Back into the College IT Curriculum*, p. 61.

[172] Kelly, "Why Cell Phone Service Is Down in Maui—and When It Could Be Restored."

[173] Space Weather Prediction Center, National Oceanic and Atmospheric Administration, "Solar Flares (Radio Blackouts)."

[174] Frost, "Pandemic Highlights Disparities in High-Speed Internet Service."

[175] American Society of Civil Engineers, *2021 Infrastructure Report Card*.

[176] Luinaud, "The Future of Military Satellites Lies in Modularity."

[177] Chilton, *The Backbone of JADC2*.

[178] del Castillo, "Backup Generators Fail at SJ Hospital During Blackouts, Leaving Workers Scrambling for Hours."

[179] American Hospital Association, "Federal Investment Needed to Keep Hospitals' Physical Infrastructure Ready to Meet Health Care Needs."

[180] FBI, "Unpatched and Outdated Medical Devices Provide Cyber Attack Opportunities."

[181] EPA, "Water Infrastructure Resilience."

[182] Flavelle, "A Breakthrough Deal to Keep the Colorado River from Going Dry, for Now."

[183] Bureau of Reclamation, "Drought Response Operations Agreement."

[184] Montgomery and Logan, "Poor Cybersecurity Makes Water a Weak Link in Critical Infrastructure."

[185] American Society of Civil Engineers, *2021 Infrastructure Report Card*, p. 152.

[186] American Society of Civil Engineers, *2021 Infrastructure Report Card*, p. 36.

[187] Olson and Stubblefield, "Survey: Lead Pipes Are Widespread and Used in Every State."

[188] American Society of Civil Engineers, *2021 Infrastructure Report Card*.

[189] Norden and McCadney, "Voting Machines at Risk: Where We Stand Today."

[190] Elwood, "Ransomware Poses Threat to Vulnerable Local Governments."

[191] Palleti et al., "Cascading Effects of Cyber-Attacks on Interconnected Critical Infrastructure."

[192] Capra, *Protecting Critical Rail Infrastructure*.

[193] Center for Infrastructure Protection & Homeland Security, George Mason University, *Derailed*.

[194] National Transportation Safety Board, "Railroad Accident Brief."

[195] Capra, *Protecting Critical Rail Infrastructure*.

[196] Osipovich, "After the 9/11 Attacks, Wall Street Bolstered Its Defenses."

[197] Ericsson, "Communication Needs in Times of Crisis."

[198] Duong, Bello, and Maurushat, "Working from Home Users at Risk of COVID-19 Ransomware Attacks."

[199] American Society of Civil Engineers, *Status Report: COVID-19's Impacts on America's Infrastructure*.

[200] White House, Critical Infrastructure Security and Resilience.

[201] Starks, "A Presidential Critical Infrastructure Protection Order Is Getting a Badly Needed Update, Officials Say."

[202] White House, "Letter from the President to Select Congressional Leadership on the Nation's Critical Infrastructure."

References

American Hospital Association, "Federal Investment Needed to Keep Hospitals' Physical Infrastructure Ready to Meet Health Care Needs," fact sheet, undated. As of August 17, 2023:
https://www.aha.org/fact-sheets/2021-05-26-fact-sheet-federal-investment-needed-keep-hospitals-physical-infrastructure

American Society of Civil Engineers, *Status Report: COVID-19's Impacts on America's Infrastructure*, June 2020.

American Society of Civil Engineers, *2021 Infrastructure Report Card: A Comprehensive Assessment of America's Infrastructure*, 2021.

Amtrak, "FY 2022 Company Profile: For the Period October 1, 2021–September 30, 2022," 2023.

Anthony, Clarence E., Tina Lee, Jacob Gottlieb, and Brooks Rainwater, *On the Frontlines of Today's Cities: Trauma, Challenges, and Solutions*, National League of Cities, 2021.

Aratani, Lori, Ian Duncan, and Michael Laris, "As Southwest, FAA Probes Begin, Fallout Could Shape Flying for Years," *Washington Post*, February 9, 2023.

Arghire, Ionut, "Submarine Cables at Risk of Nation-State Sabotage, Spying: Report," *Security Week*, June 28, 2023.

Arkin, William, "Why Nashville Bomb Investigators Feared Copycat Attacks by 5G Conspiracists," *Newsweek*, December 27, 2020.

Balasubramanian, Sai, "With Increasing Reliance on Healthcare Technology, Cybersecurity Is a Growing Concern," *Forbes*, April 29, 2023.

Barone, Emily, "The U.S.'s Creaky Power Grid Is No Match for Worsening Weather Catastrophes," *TIME*, November 18, 2022.

Benner, Katie, and Nicole Perlroth, "Iranians Accused in Cyberattacks, Including One That Hobbled Atlanta," *New York Times*, November 28, 2018.

Bergengruen, Vera, "'Is There Something More Sinister Going On?' Authorities Fear Extremists Are Targeting U.S. Power Grid," *TIME*, January 9, 2023.

Bischoff, Paul, "Ransomware Attacks on US Government Organizations Cost over $70bn from 2018 to October 2022," *Comparitech*, November 9, 2022.

Boone, Rebecca, "Attacks at US Medical Centers Show Why Health Care Is One of the Nation's Most Violent Fields," *ABC News*, August 7, 2023.

Boubaker, Khobeib Ben, "Twenty Years of Cyberattacks on the World of Water," Stormshield, August 30, 2021.

Boucek, Christopher, "Security Is the Watchword for U.S. Mass Transit Systems," Royal United Services Institute, November 19, 2007.

Brangham, William, "FBI Foils Extremist Plot to Bring Down Baltimore's Electrical Grid," PBS, February 7, 2023.

Brunker, Mike, "GPS Under Attack as Crooks, Rogue Workers Wage Electronic War," NBC, August 8, 2017.

Bureau of Reclamation, "Drought Response Operations Agreement," webpage, updated July 5, 2023. As of August 17, 2023:
https://www.usbr.gov/dcp/droa.html

Capra, Gregory S., *Protecting Critical Rail Infrastructure*, Air University, December 2006.

Carrell, Severin, "Telephone and Internet Restored in Shetland After Cable Damage," *The Guardian*, October 2022.

Center for Infrastructure Protection & Homeland Security, George Mason University, *Derailed: A Cast Study of the 2001 Baltimore Howard Street Tunnel Fire with Exercises*, undated.

Chilton, Kevin P., *The Backbone of JADC2: Satellite Communications for Information Age Warfare*, Mitchell Institute, December 2021.

Ciampoli, Paul, "Outages Post-Hurricane Ian Down to Less Than 500,000 in Florida," American Public Power Association, October 5, 2022.

CISA—*See* Cybersecurity and Infrastructure Security Agency.

Clare, M. A., I. A. Yeo, L. Bricheno, Y. Aksenov, J. Brown, I. D. Haigh, T. Wahl, J. Hunt, C. Sams, J. Chaytor, B. J. Bett, and L. Carter, "Climate Change Hotspots and Implications for the Global Subsea Telecommunications Network," *Earth-Science Reviews*, Vol. 237, February 2023.

Clarke, Colin, Mollie Saltskog, Michaele Millender, and Naureen C. Fink, "The Targeting of Infrastructure by America's Violent Far Right," *CTC Sentinel*, Vol. 16, No. 5, May 2023.

Coburn, Timothy C., "Oil and Gas Infrastructure: A Technical Overview," *Oxford Handbook of Energy Politics*, June 8, 2020.

Coker, James, "Local Government Organizations Most Frequently Targeted by Ransomware," *Infosecurity*, August 27, 2020.

"Conspiracy Theorists Burn 5G Towers Claiming Link to Virus," Associated Press, April 21, 2020.

Copeland, Claudia, *Terrorism and Security Issues Facing the Water Infrastructure Sector*, Congressional Research Service, RL32189, December 15, 2010.

Cybersecurity and Infrastructure Security Agency, "China Cyber Threat Overview and Advisories," webpage, undated. As of February 7, 2023:
https://www.cisa.gov/uscert/china

Cybersecurity and Infrastructure Security Agency, "Critical Infrastructure Sectors," webpage, undated. As of August 17, 2023:
https://www.cisa.gov/topics/critical-infrastructure-security-and-resilience/critical-infrastructure-sectors

Cybersecurity and Infrastructure Security Agency, "Critical Infrastructure Security and Resilience," webpage, undated. As of July 22, 2023:
https://www.cisa.gov/topics/critical-infrastructure-security-and-resilience

Cybersecurity and Infrastructure Security Agency, "Critical Infrastructure Systems," webpage, undated. As of August 17, 2023:
https://www.cisa.gov/topics/critical-infrastructure-security-and-resilience/resilience-services/infrastructure-dependency-primer/learn/critical-infrastructure-systems

Cybersecurity and Infrastructure Security Agency, "Defining Insider Threats," webpage, undated. As of August 17, 2023:
https://www.cisa.gov/topics/physical-security/insider-threat-mitigation/defining-insider-threats

Cybersecurity and Infrastructure Security Agency, "Emergency Services Sector," webpage, undated. As of February 27, 2023:
https://www.cisa.gov/topics/critical-infrastructure-security-and-resilience/critical-infrastructure-sectors/emergency-services-sector

Cybersecurity and Infrastructure Security Agency, "Energy Sector," webpage, undated. As of August 29, 2023: https://www.cisa.gov/topics/critical-infrastructure-security-and-resilience/critical-infrastructure-sectors/energy-sector

Cybersecurity and Infrastructure Security Agency, "Extreme Weather and Climate Change," webpage, undated. As of August 17, 2023: https://www.cisa.gov/topics/critical-infrastructure-security-and-resilience/extreme-weather-and-climate-change

Cybersecurity and Infrastructure Security Agency, "Government Facilities Sector," webpage, undated. As of June 26, 2023: https://www.cisa.gov/topics/critical-infrastructure-security-and-resilience/critical-infrastructure-sectors/government-facilities-sector

Cybersecurity and Infrastructure Security Agency, "Healthcare and Public Health Sector," webpage, undated. As of August 6, 2023: https://www.cisa.gov/stopransomware/healthcare-and-public-health-sector

Cybersecurity and Infrastructure Security Agency, "Hospitals & Healthcare Facilities," action guide, undated.

Cybersecurity and Infrastructure Security Agency, "Transportation Systems Sector," webpage, undated. As of August 29, 2023: https://www.cisa.gov/topics/critical-infrastructure-security-and-resilience/critical-infrastructure-sectors/transportation-systems-sector

Cybersecurity and Infrastructure Security Agency, "Understanding Vulnerabilities of Positioning, Navigation, and Timing," fact sheet, undated.

Cybersecurity and Infrastructure Security Agency, "Port Facility Cybersecurity Risks," infographic, December 2020. As of August 29, 2023: https://www.cisa.gov/sites/default/files/publications/port-facility-cybersecurity-risks-infographic_508.pdf

D'Agostino, Susan, "Jellyfish Attack Nuclear Power Plant. Again," Bulletin of the Atomic Scientists, October 28, 2021.

del Castillo, Amanda, "Backup Generators Fail at SJ Hospital During Blackouts, Leaving Workers Scrambling for Hours," ABC 7 News, September 7, 2022.

DHS—*See* U.S. Department of Homeland Security.

Dillingham, Gerald, "Vulnerabilities Still Exist in the Aviation System," testimony before the Subcommittee on Aviation, Committee on Commerce, Science, and Transportation, U.S. Senate, April 6, 2000.

Dragos, "Global Oil and Gas Cyber Threat Perspective," July 29, 2019.

Duong, Anthony An, Abubakar Bello, and Alana Maurushat, "Working from Home Users at Risk of COVID-19 Ransomware Attacks," *Cybersecurity and Cognitive Science*, 2022.

Edlin, Ruby, and Lawrence Norden, "Poll of Election Officials Shows High Turnover amid Safety Threats and Political Interference," Brennan Center for Justice, April 25, 2023.

Eling, Martin, and Kwangmin Jung, "Heterogeneity in Cyber Loss Severity and Its Impact on Cyber Risk Measurement," *Risk Management*, Vol. 24, No. 3, 2022.

Elwood, Karina, "Ransomware Poses Threat to Vulnerable Local Governments," *Washington Post*, August 22, 2021.

Englund, Scott, "Domestic Terrorism Is Evolving. It Needs Imaginative Counterterrorism," Brookings Institution, January 18, 2023.

Enzoic, "Cyberattacks on Municipalities & How to Defend Against Them," Security Boulevard, March 29, 2021.

EPA—*See* U.S. Environmental Protection Agency.

Ericsson, "Communication Needs in Times of Crisis," extract from the Ericsson Mobility Report, June 2020.

European Aviation Safety Agency, "Stand-Alone Airborne Navigation Equipment Using the Global Positioning System Augmented by the Satellite Based Augmentation System," European Technical Standard Order C146e, February 21, 2018.

Eytan, Oren, "Municipal Cyberattacks: A New Threat or Persistent Risk?" *Forbes*, June 22, 2021.

FAA—*See* Federal Aviation Administration.

FBI—*See* Federal Bureau of Investigation.

Federal Aviation Administration, "FAA NOTAM Statement," January 19, 2023.

Federal Aviation Administration, "FAA Fact Book," webpage, February 8, 2023. As of August 29, 2023: https://www.faa.gov/newsroom/facts-about-faa-and-air-traffic-control

Federal Bureau of Investigation, "FBI Releases Report on Nashville Bombing," March 15, 2021.

Federal Bureau of Investigation, "Unpatched and Outdated Medical Devices Provide Cyber Attack Opportunities," Private Industry Notification 20220912-001, September 12, 2022.

Federal Highway Administration, U.S. Department of Transportation, "How Do Weather Events Impact Roads?" webpage, February 1, 2023. As of August 17, 2023: https://ops.fhwa.dot.gov/weather/q1_roadimpact.htm

Figueroa Diaz, Victor M., *An Analysis of Railway Industrial Control Systems Vulnerabilities*, Capstone Project, Utica College ProQuest Dissertations Publishing, 2018.

Financial Services Sector Coordinating Council, *Financial Services Sector-Specific Plan*, U.S. Department of Homeland Security and U.S. Department of the Treasury, 2015.

First Street Foundation, *The 3rd National Risk Assessment: Infrastructure on the Brink*, October 2021.

Flaherty, Eoin, Tristan Sturm, and Elizabeth Farries, "The Conspiracy of Covid-19 and 5G: Spatial Analysis Fallacies in the Age of Data Democratization," *Social Science & Medicine*, Vol. 293, January 2022.

Flavelle, Christopher, "A Breakthrough Deal to Keep the Colorado River from Going Dry, for Now," *New York Times*, May 25, 2023.

Fox, Andrea, "Half of Ransomware Attacks Have Disrupted Healthcare Delivery, JAMA Report Finds," *Healthcare IT News*, January 10, 2023.

Fox, Emily Jane, Charles Riley, and Hibah Yousuf, "NYSE and Nasdaq Closed as Hurricane Sandy Hits," CNN Business, October 29, 2012.

Frost, Riordan, "Pandemic Highlights Disparities in High-Speed Internet Service," Joint Center for Housing Studies of Harvard University, blog post, September 8, 2021. As of August 17, 2023: https://www.jchs.harvard.edu/blog/pandemic-highlights-disparities-high-speed-internet-service

Frye, Celeste, "Pandemic Lessons: Improving Your Municipality's Continuity and Coordination of Services After COVID," American City & County, June 30, 2021.

FS-ISAC Global Intelligence Office, *Navigating Cyber 2022: Annual Cyber Threat Review and Predictions*, Financial Services Information Sharing and Analysis Center, March 2022.

"Galway Valley: China and India Clash on Freezing and Inhospitable Battlefield," BBC, June 17, 2020.

Gamache, Kevin R., "Critical Infrastructure: Water and Wastewater Systems Sector," *Encyclopedia of Security and Emergency Management*, January 1, 2021.

GAO—*See* U.S. Government Accountability Office.

Goldbaum, Christina, and William K. Rashbaum, "The MTA Is Breached by Hackers as Cyberattacks Surge," *New York Times*, July 20, 2021.

Grohoski, David, *The Vulnerabilities of U.S. Strategic Ports to Acts of Sabotage*, thesis, Naval War College, February 12, 1996.

Hampson, Michelle, "This Alternative Could Stay on Target If GPS Fails," *IEEE Spectrum*, May 22, 2023.

Hassan, Adeel, and Nicholas Bogel-Burroughs, "What We Know About the Louisville, Ky., Bank Shooting," *New York Times*, April 12, 2023.

Henriquez, Maria, "Banking Industry Sees 1318% Increase in Ransomware Attacks in 2021," *Security Magazine*, September 20, 2021.

Hermsen, Catherine, "Drug Tampering and Product Substitution in Healthcare Facilities," *Journal of Healthcare and Protection Management*, Vol. 38, No. 1, 2022.

IBM Corporation, *X-Force Threat Intelligence Index 2022*, February 2022.

Ileto, Jason, "Cyber at Sea: Protecting Strategic Sealift in the Age of Strategic Competition," Modern War Institute, May 10, 2022.

International Energy Agency, "Smart Grids," webpage, undated. As of September 11, 2023: https://www.iea.org/energy-system/electricity/smart-grids

Irrera, Anna, "Banks Scramble to Fix Old Systems as IT 'Cowboys' Ride into Sunset," Reuters, April 11, 2017.

Kaffenberger, Lincoln, and Emanuel Kopp, *Cyber Risk Scenarios, the Financial System, and Systemic Risk Assessment*, Carnegie Endowment for International Peace, September 30, 2019.

Kearney, Laila, "Atlanta Takes Down Water Department Website Two Weeks After Cyber Attack," Reuters, April 15, 2018.

Kelly, Samantha Murphy, "Why Cell Phone Service Is Down in Maui—and When It Could Be Restored," CNN Business, August 10, 2023.

King, Llewellyn, "How America's Power Grid Is Vulnerable to Undetected Cyberattack," *Forbes*, January 28, 2021.

KnowBe4, *The Economic Impact of Cyber Attacks on Municipalities*, 2022.

Kramek, Joseph, "The Critical Infrastructure Gap: U.S. Port Facilities and Cyber Vulnerabilities," Brookings Institution, July 2013.

Krill, Ilana, "The Evolution of Critical Infrastructure Targeting by Violent Extremists," *Lawfare*, October 2022.

Larson, Kevin, "Municipal Cybersecurity: How to Prepare as Cybercriminals Go Hyperlocal," Citizens Bank, undated.

Laskow, Sarah, "The Five Best Times Jellyfish Shut Down Power Plants," *Grist*, October 2, 2013.

Law, Selene, "Making Power Grids More Resilient," Cleantech Group, blog post, February 14, 2023. As of September 11, 2023: https://www.cleantech.com/making-power-grids-more-resilient/

Levenson, Michael, "Attacks on Electrical Substations Raise Alarm," *New York Times*, February 4, 2023.

Lindoo, Ed, *Bringing COBOL Back into the College IT Curriculum*, Consortium for Computing Sciences in Colleges, 2014.

Ling, Nin, *The Timeline and Events of the February 2021 Texas Electric Grid Blackouts*, University of Texas at Austin Energy Institute, July 2021.

Luinaud, Mathiew, "The Future of Military Satellites Lies in Modularity," Via Satellite, June 27, 2022.

Lyngaas, Sean, "Kansas Man Indicted in Connection with 2019 Hack at Water Utility," *Cyberscoop*, April 21, 2021.

Mariano, Mike, "Cybersecurity Landscape in the Telecommunications Sector," IS Partners, October 31, 2022.

Maruf, Ramishah, "Will the I-95 Collapse in Philadelphia Hurt the Economy? Look at Other Cities for Answers," CNN Business, June 12, 2023.

Matza, Max, "FAA Outage: US Airline Regulators Blame Contractor for Travel Chaos," BBC, January 19, 2023.

Maurer, Tim, and Arthur Nelson, "The Global Cyber Threat," International Monetary Fund, 2021.

McDaniel, Justine, "Citing Climate Change Risks, Farmers Is Latest Insurer to Exit Florida," *Washington Post*, July 12, 2023.

McFarland, Matt, "Amtrak Might Add More Than 50 New Routes. But They Still Won't Be Faster Than a Car," CNN, September 1, 2021.

McKeon, Jill, "CommonSpirit Health Faces Class Action Lawsuit in Wake of Healthcare Data Breach," Health IT Security, January 23, 2023.

Menn, Joseph, "U.S. Warns Newly Discovered Malware Could Sabotage Energy Plants," *Washington Post*, April 13, 2022.

Microsoft, "Ransomware as a Service: Understanding the Cybercrime Gig Economy and How to Protect Yourself," May 9, 2023.

Miller, Maggie, "Russian-Linked Malware Was Close to Putting the U.S. Electric, Gas Facilities 'Offline' Last Year," *Politico*, February 14, 2023.

Minnesota Legislative Reference Library, "Minneapolis Interstate 35W Bridge Collapse," webpage, October 2022. As of September 17, 2023: https://www.lrl.mn.gov/guides/guides?issue=bridges

Montgomery, Mark, and Trevor Logan, "Poor Cybersecurity Makes Water a Weak Link in Critical Infrastructure," Foundation for Defense of Democracies, November 18, 2021.

Murez, Cara, "Patient Care Delayed at Large Hospital Chain After Ransomware Attack," *US News & World Report*, October 10, 2022.

National Association of State Chief Information Officers, "Ensure Dedicated Cybersecurity Funding for State and Local Governments with CIOs as Key Decisionmakers," press release, January 22, 2020.

National Conference of State Legislatures, *Human-Driven Physical Threats to Energy Infrastructure*, May 22, 2023.

National Cyber Security Centre, "Russia Behind Cyber Attack with Europe-Wide Impact an Hour Before Ukraine Invasion," May 10, 2022.

National Transportation Safety Board, "Railroad Accident Brief," 2004.

National Transportation Safety Board, *Collapse of I-35W Highway Bridge Minneapolis, Minnesota, August 1, 2007*, Highway Accident Report NTSB/HAR-08/03, 2008.

Neprash, Hannah T., Claire C. McGlave, Dori A. Cross, Beth A. Virnig, Michael A. Puskarich, Jared D. Huling, Alan Z. Rozenshtein, and Sayeh S. Nikpay, "Trends in Ransomware Attacks on US Hospitals, Clinics, and Other Health Care Delivery Organizations, 2016–2021," *JAMA Health Forum*, Vol. 3, No. 12, 2022.

New York State Department of Environmental Conservation, "New York City Water Supply," webpage, undated. As of July 17, 2023:
https://www.dec.ny.gov/lands/25599.html

Nijhuis, Michelle, "'I'm Just More Afraid of Climate Change Than I Am of Prison,'" *New York Times*, February 13, 2018.

Nixon, Ron, "Human Cost Rises as Old Bridges, Dams and Roads Go Unrepaired," *New York Times*, November 5, 2015.

Norden, Lawrence, and Andrea Cordova McCadney, "Voting Machines at Risk: Where We Stand Today," Brennan Center for Justice, March 5, 2019.

Olson, Erik D., and Alexandra Stubblefield, "Survey: Lead Pipes Are Widespread and Used in Every State," Natural Resources Defense Council, July 8, 2021.

Osipovich, Alexander, "After the 9/11 Attacks, Wall Street Bolstered Its Defenses," *Wall Street Journal*, September 7, 2021.

Ozarslan, Suleyman, "Key Threats and Cyber Risks Facing Financial Services and Banking Firms in 2022," Picus Labs, March 24, 2022.

Page, Carly, "CommonSpirit Health Says Patient Data Was Stolen During Ransomware Attack," *TechCrunch*, December 9, 2022.

Palleti, Venkata Reddy, Sridhar Adepu, Vishrut Kumar Mishra, and Aditya Mathur, "Cascading Effects of Cyber-Attacks on Interconnected Critical Infrastructure," *Cybersecurity*, Vol. 4, 2021.

Peterson, Andrea, "Are Squirrels a Bigger Threat to the Power Grid Than Hackers?" *Washington Post*, January 12, 2016.

Pinkerton, "ATMs and Crime," blog post, undated. As of August 17, 2023:
https://pinkerton.com/our-insights/blog/atms-and-crime

Preis, Benjamin, and Lawrence Susskind, "Municipal Cybersecurity: More Work Needs to Be Done," *Urban Affairs Review*, Vol. 58, No. 2, 2022.

President's Commission on Critical Infrastructure Protection, *Critical Foundations: Protecting America's Infrastructures*, October 1997.

Public Law 107-56, Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism (USA PATRIOT ACT) Act of 2001, 2001.

Quach, Katyanna, "Belgian Parliament Halts China Uyghur 'Genocide' Debate After DDoS Smashes ISP Offline," *The Register*, May 2021.

Romo, Vanessa, "Pro-Russian Hackers Claim Responsibility for Knocking U.S. Airport Websites Offline," NPR, October 10, 2022.

Roy, Sandip, and Banavar Sridhar, "Cyber-Threat Assessment for the Air Traffic Management System: A Network Controls Approach," *Proceedings of the 16th AIAA Aviation Technology, Integration, and Operations Conference,* June 2016.

Sanger, David E., "China Appears to Warn India: Push Too Hard and the Lights Could Go Out," *New York Times*, February 28, 2021.

Savitz, Scott, "Beware the Explosive Vessels," *Real Clear Defense*, October 20, 2022.

Scott, Mark, "Will Russia Attack Undersea Internet Cables Next?" *Politico*, September 2022.

Shea, Sharon, "Smart City," Tech Target, July 2020.

Shead, Sam, "Universities Won't Teach 'Uncool' COBOL Anymore—But Should They?" ZDNet, March 7, 2013.

Shepardson, David, "Amtrak Wants $8 Billion in US Funding for Infrastructure Projects," Reuters, June 5, 2023.

Shorman, Jonathan, and Steve Vockrodt, "Ex-Employee Remotely Hacks Kansas Water Treatment Plant," *Kansas City Star*, April 13, 2021.

Space Weather Prediction Center, National Oceanic and Atmospheric Administration, "Solar Flares (Radio Blackouts)," webpage, undated. As of August 17, 2023:
https://www.swpc.noaa.gov/phenomena/solar-flares-radio-blackouts

Starks, Tim, "A Presidential Critical Infrastructure Protection Order Is Getting a Badly Needed Update, Officials Say," *Washington Post*, May 11, 2023.

Swain, Claudia, "The Emerging Cyber Threat to the American Rail Industry," *Lawfare*, October 20, 2022.

Tammimi, Ali, Adam Hahn, and Sandip Roy, "Cyber Threat Impact Analysis to Air Traffic Flows Through Dynamic Queue Networks," *ACM Transactions on Cyber-Physical Systems*, Vol. 4. No. 3, March 2020.

Tangel, Andrew, "Why Planes Were Grounded for the First Time Since 9/11," *Wall Street Journal*, February 14, 2023.

Texas Department of State Health Services, "February 2021 Winter Storm-Related Deaths—Texas," December 31, 2021.

Thompson, Lisa N., "Cybersecurity Best Practices for Municipalities," New Hampshire Municipal Association, 2019.

Thudimilla, Anusha, and Bruce McMillin, “Cyber-Physical Security of Air Traffic Surveillance Systems,” *Critical Infrastructure Protection XIV*, 2020.

Tivnan, Brian, *Financial System Mapping*, Homeland Security Systems Engineering and Development Institute, MITRE Corporation, case number 18-1703, DHS reference number 16-J-00184-09, 2018.

Treisman, Rachel, “Damage from Hurricane Ian Cuts Sanibel Island off from Florida’s Mainland,” NPR, September 30, 2022.

Tucker, Emma, and Priya Krishnakumar, “Intentional Killings of Law Enforcement Officers Reach 20-Year High, FBI Says,” CNN, January 13, 2022.

“Ukraine: Disk-Wiping Attacks Precede Russian Invasion,” Symantec, blog post, February 24, 2022. As of July 17, 2023: https://symantec-enterprise-blogs.security.com/blogs/threat-intelligence/ukraine-wiper-malware-russia

U.S. Attorney’s Office, Northern District of California, “Tracy Resident Charged with Computer Attack on Discovery Bay Water Treatment Facility,” press release, July 7, 2023.

U.S. Department of Health and Human Services, *Healthcare and Public Health Sector-Specific Plan*, May 2016.

U.S. Department of Homeland Security, *Communications Sector-Specific Plan 2015: An Annex to the NIPP 2013*, 2015.

U.S. Department of Homeland Security, *U.S. Department of Homeland Security Soft Targets and Crowded Places Security Plan Overview*, May 2018.

U.S. Department of Homeland Security, “Secure Cyberspace and Critical Infrastructure,” webpage, updated December 1, 2023. As of August 6, 2023: https://www.dhs.gov/secure-cyberspace-and-critical-infrastructure

U.S. Department of Justice Office of Public Affairs, “Federal Charges Announced Against Maine Man Who Carried Out Machete Attack in Times Square on New Year’s Eve in Name of Jihad,” press release, January 10, 2023.

U.S. Energy Information Administration, “U.S. Electricity Customers Averaged Five and One-Half Hours of Power Interruptions in 2022,” webpage, January 25, 2024. As of March 4, 2024: https://www.eia.gov/todayinenergy/detail.php?id=61303

U.S. Environmental Protection Agency, “Water and Wastewater Systems Sector-Specific Plan,” 2015.

U.S. Environmental Protection Agency, “EPA’s 6th Drinking Water Infrastructure Needs Survey and Assessment,” webpage, August 27, 2018. As of September 7, 2023: https://www.epa.gov/dwsrf/epas-6th-drinking-water-infrastructure-needs-survey-and-assessment

U.S. Environmental Protection Agency, “Climate Change Impacts on Transportation,” webpage, December 13, 2022. As of August 17, 2023: https://www.epa.gov/climateimpacts/climate-change-impacts-transportation

U.S. Environmental Protection Agency, “Water Infrastructure Resilience,” webpage, May 29, 2023. As of June 19, 2023: https://www.epa.gov/emergency-response-research/water-infrastructure-resilience

U.S. Government Accountability Office, *CISA Should Assess the Effectiveness of Its Actions to Support the Communications Sector*, GAO-22-104462, November 2021.

U.S. Government Accountability Office, *Offshore Oil and Gas: Strategy Urgently Needed to Address Cybersecurity Risks to Infrastructure*, GAO-23-105789, October 2022.

U.S. Government Accountability Office, *GPS Alternatives: DOD Is Developing Navigation Systems but Is Not Measuring Overall Progress*, GAO-22-106010, August 5, 2023.

U.S. Maritime Administration, “Navigating a Stronger Future,” website, undated. As of August 29, 2023: https://www.maritime.dot.gov/

U.S. Senate Armed Services Committee, *Inquiry into Cyber Intrusions Affecting U.S. Transportation Command Contractors*, 2014.

Wall, Colin, and Pierre Morcos, “Invisible and Vital: Undersea Cables and Transatlantic Security,” Center for Strategic and International Studies, June 2021.

White House, Critical Infrastructure Security and Resilience, Presidential Policy Directive 21, February 12, 2013.

White House, “Fact Sheet: The Bipartisan Infrastructure Deal,” November 6, 2021.

White House, “Letter from the President to Select Congressional Leadership on the Nation’s Critical Infrastructure,” November 7, 2022.

Whitecomb, Dan, and Steve Gorman, “UPDATE 6—Settlement Reached to End 8-Day Los Angeles Port Strike,” Reuters, December 4, 2012.

Acknowledgments

The authors wish to recognize the contributions of the reviewers, support staff, publishing staff, and especially the participants in the INVERTED ROOK game, who provided thoughtful, timely, and operationally relevant input at each stage of the game.

About This Report

In this report, we analyze threats and hazards to critical infrastructure and examine the vectors by which an adversary might conduct attacks against the homeland. We also look at the cascading effects of an attack and other impacts related to infrastructure age and maintenance and to weather challenges. These threats are demonstrated across critical infrastructures on a daily basis, but it is easy to become desensitized to such risks and vulnerabilities—particularly when not presented as part of a holistic picture of threats in aggregate. Here, we offer characterizations of various types of threat actors and vectors to raise awareness of systemic vulnerabilities and threat environments that can affect our critical infrastructure.

This report is based on unclassified insights gained before, during, and after RAND's tabletop exercise, INVERTED ROOK, in May 2023. The exercise involved numerous interagency sponsors and participants, and all players provided invaluable input; however, the research, analysis, and final product are solely the responsibility of the authors and do not reflect the policy or positions of any U.S. government department or agency.

The research reported here was completed in February 2024 and underwent security review with the sponsor and the Defense Office of Prepublication and Security Review before public release.

RAND National Security Research Division

This research was sponsored by the Office of the Director of National Intelligence (ODNI), the Department of the Army, and the Under Secretary of Defense for Intelligence and Security and conducted within the International Security and Defense Policy Program of the RAND National Security Research Division (NSRD), which operates the National Defense Research Institute (NDRI), a federally funded research and development center sponsored by the Office of the Secretary of Defense, the Joint Staff, the Unified Combatant Commands, the Navy, the Marine Corps, the defense agencies, and the defense intelligence enterprise.

For more information on the RAND International Security and Defense Policy Program, see www.rand.org/nsrd/isdp or contact the director (contact information is provided on the webpage).

For more information on this publication, visit www.rand.org/t/RRA2397-2.

Cover photos: Andreas Gruhl/Adobe Stock; Anoo/Adobe Stock; WS Films/Adobe Stock; peshkov/Getty Images

www.rand.org

RR-A2397-2