

ONE STEP AHEAD:

A CRITICAL INFRASTRUCTURE PROTECTION RESEARCH AND STRATEGY PUBLICATION

Spring 2024



Insights of the



**INSTITUTE FOR
HOMELAND SECURITY**
SAM HOUSTON STATE UNIVERSITY®

ONE STEP AHEAD

A CRITICAL INFRASTRUCTURE PROTECTION RESEARCH AND STRATEGY PUBLICATION

Editorial Office:
Institute for Homeland Security
Criminal Justice Center
Sam Houston State University
PO Box 2296
Huntsville, TX 77340
Email: IHS@ihsonline.org
www.ihsonline.org



EDITOR

Dr. Ryan Randa, Research Director
Institute for Homeland Security

MANAGING EDITOR

Dr. Shannon M. Lane, Program Manager, Research
Institute for Homeland Security

INSTITUTE FOR HOMELAND SECURITY

Michael Aspland, Executive Director
Cindy Martinez, Executive Coordinator

SAM HOUSTON STATE UNIVERSITY

Dr. Alisa White, President
Dr. Phillip Lyons, Dean, College of Criminal Justice

TEXAS STATE UNIVERSITY SYSTEM BOARD OF REGENTS

Alan L. Tinsley, Chairman, Madisonville
Dionicio (Don) Flores, Vice Chairman, El Paso
Charlie Amato, Regent, San Antonio
Duke Austin, Regent, Houston
Sheila Faske, Regent, Rose City
Russell Gordy, Regent, Houston
Stephen Lee, Regent, Beaumont
Tom Long, Regent, Frisco
William F. Scott, Regent, Nederland
Kelvin Elgar, Student Regent, Beaumont
Brian McCall, Chancellor

Message from the Editor/Director



INSTITUTE FOR HOMELAND SECURITY

SAM HOUSTON STATE UNIVERSITY®

Partners,

On behalf of the team here at the Institute for Homeland Security, I am pleased to present the 2nd edition of our publication *One Step Ahead: A Critical Infrastructure Protection Research and Strategy Journal*.

In staying *One Step Ahead* in research, our academic and professional partners from the critical infrastructure protection (CIP) world create innovative, value-added knowledge that meets the needs of our constituents. The following papers stand out as our “best in show” because of their exploration of unseen threats and emerging technological challenges. These papers are representative of our Core Purpose: *We Stay One Step Ahead*, transforming knowledge to protect critical infrastructure. It is our hope that the information herein stands to fill research gaps in the CI protection space. As it is through the dissemination of our research that we seek to sustain existing relationships and build new connections with the homeland security professional.

For a complete searchable listing of our sponsored research projects, please go to our website at www.ihsonline.org and select Sponsored Research tab. Finally, if you are interested in submitting a research proposal, select the Research Proposal tab and tell us about your topic. Our team will review your submission and work with you to develop your submission. Thank you for being part of our goal to stay *One Step Ahead*!

Michael J. Aspland
Executive Director



Mission

The SHSU Institute for Homeland Security provides innovative, value-added knowledge tailored to the needs of industry and public institutions, to protect critical infrastructure supporting Texas and the nation's economy.

Our Four Pillars

Texas Nexus

We believe in a secure and unified Texas, connecting our private industry partners with public institutions through productive conversation.

One Step Ahead

Our focus is to stay ahead in an ever-changing security environment by providing innovative solutions that support business continuity and critical infrastructure protection.

Complement to Complete

We aim to fill the gaps and meet the needs of critical infrastructure sectors alongside our institutional partners.

Disruptive but Helpful

We believe in serving our private industry partners and public institutions in ways not done before.

ELEVATING HOMELAND SECURITY RESEARCH: NAVIGATING CRITICAL CONCEPTS AT IHS

Greetings,

As you've likely discovered, the Institute for Homeland Security (IHS) at Sam Houston State University stands as a cornerstone for research on critical infrastructure protection. Allow me to offer a panoramic overview of our approach in uncovering pressing industry inquiries and aligning them with research partners to furnish actionable solutions for our audience.

At present, our research trajectory orbits around seven pivotal themes, forged through our enduring collaborations with governmental and industrial stakeholders. These themes, encapsulated within the inaugural iteration of IHS Critical Concepts, represent our guiding compass. Yet, as the security landscape evolves, so too shall our vista of critical concepts.

- Artificial Intelligence: The burgeoning practical applications of AI in critical infrastructure protection for both government and industry partners underscore the imperative of prioritizing this domain to maintain a proactive stance. With new potentials emerging daily, AI finds utility in diverse areas such as threat detection and risk management/analysis, facilitated by its increasing accessibility and sophistication.
- Cascading Effects: Cascading effects encapsulate the intricate dynamics witnessed in disasters, where the repercussions of a physical event or an initial technological or human failure trigger a chain reaction of events across human subsystems, culminating in varying degrees of physical, social, or economic disruption.
- Critical Infrastructure Workforce Development: The feedback from industry and government stakeholders underscores the pressing need to address the underdevelopment within the critical infrastructure (CI) workforce pool. Understanding the gap between traditional educational pathways and the evolving needs of CI employers, alongside identifying existing strengths and opportunities for enhancement in workforce development, serves as a linchpin for bolstering critical infrastructure operations and protection.
- Cyber-Security Threat: Benchmarking best practices for responding to cyber-security threats in Texas-based hospitals and medical centers is paramount. This encompasses combatting attacks such as ransomware and accidental breaches leading to the loss of protected data or the disruption of critical operating systems, which can significantly impair operational capabilities.
- Emerging Threats: Emerging threats denote novel and evolving risks that are yet to be comprehensively understood or addressed, presenting a complex interplay of opportunities and risks that necessitate agile responses and adaptive strategies.
- Security Drone and Robot Deployment: Evaluating the cost-effectiveness of integrating security drones and robots into government-approved security management protocols spans a spectrum of functionalities, including access control, visitor management, cargo inspection, perimeter patrol, and emergency response scenarios. These technologies offer multifaceted solutions ranging from firefighting to toxic release containment, heralding a paradigm shift in security management.
- Security Risk Assessment: Security risk assessment serves as a pivotal process in identifying, analyzing, and implementing security controls within organizational settings. It aims to proactively mitigate vulnerabilities and threats, safeguarding physical and informational assets against unauthorized access and misuse.
- Social Network Analysis (SNA): Utilizing a social network analysis (SNA) approach enables the identification of organizational personnel and staffing dynamics, facilitating insights into optimizing team structures, processes, and staffing frameworks across public and private sectors. This strategic alignment ensures workforce and production compliance while fostering operational efficacy.
- Supply Chain Risks: Efficiently and meaningfully assessing critical infrastructure corporations' supply chain interdependencies is vital for quantifying crisis management readiness among key suppliers. This holistic understanding empowers critical infrastructure corporations to make strategic decisions informed by identified risks, thereby fortifying resilience in decision-making processes.
- Water/Wastewater: The intricate processing and management of water and wastewater underscore a critical nexus between industry and public health, warranting comprehensive exploration of threats, vulnerabilities, systemic issues, regulatory compliance, and process safety concerns. In-depth studies and articulation of these aspects promise improvements across all facets of this vital infrastructure vertical.

As we continue to chart our course forward, our ambition is to organically cultivate and refine our Critical Concepts in resonance with the evolving needs of our industry and governmental allies. Your voices remain our compass in navigating the realm of critical infrastructure protection and strategy.

For those inclined to contribute to our research endeavors, we've streamlined the process through our website's research tab (IHSOnline.org). There, you'll find our proposal submission form, designed for seamless completion and direct transmission to our dedicated email address (IHS@shsu.edu).

Rest assured, we actively solicit and support projects aligned with our critical concepts. Our research ensemble convenes weekly to assess submissions, engage potential authors, and enrich our knowledge repository.

With gratitude for your ongoing collaboration, we eagerly anticipate advancing together.

Warm regards,



Ryan Randa, PhD

Research Director, Institute for Homeland Security

Contents

| | |
|---|----|
| ENSURING THE CYBERSECURITY OF TEXAS’ CRITICAL INFRASTRUCTURES | 1 |
| Brooke Nodeland | |
| CONVERGENCE OF MISSION AND MOMENT: IMAGINING THE EMERGING TECHNOLOGY ANALYST | 11 |
| Nick Reese | |
| UNSEEN THREATS TO TEXAS CRITICAL INFRASTRUCTURE: THE RISK TO BURIED UTILITIES AND TARGETED POLICY SOLUTIONS TO PROTECT THEM | 25 |
| Benjamin Dierker | |
| SUPPLY CHAIN MAPPING FOR EMERGENCY MANAGEMENT DECISION-MAKING | 37 |
| Mark Scott | |
| RESILIENCE TO HIGH CONSEQUENCE CASCADING FAILURES OF CRITICAL INFRASTRUCTURE NETWORKS | 50 |
| Arthur Mouco, Benjamin L. Ruddell, Susan Ginsburg, and Criticality Sciences | |

ENSURING THE CYBERSECURITY OF TEXAS' CRITICAL INFRASTRUCTURES

Brooke Nodeland
Prepared for Sam Houston State University

Abstract

The daily threat of cyber-attacks on Texas' critical infrastructure present significant challenges for public and private critical infrastructure providers. COVID-19 related supply chain issues provided insight into the catastrophic effects that could be caused by a cyber-attack on the transportation sector. These disruptions effect our ability to distribute products and medical necessities as well as essential personnel in times of crisis. Protecting the state's transportation, energy, and chemical cyber networks is imperative in ensuring the sustainability of daily life and business continuity in the event of a cyber-attack. Of additional concern is a growing reliance on cyber-based control, navigation, tracking, positioning, and communications systems creating ample opportunities for exploitation of the transportation cyber systems on which industry have become dependent (Transportation Systems Sector-Specific Plan, 2015). The cyber security of the energy sector ensures the health and welfare of Texans by ensuring steady energy is supplied via electricity, oil and other natural gas resources. The energy infrastructure is primarily owned in the private sector, supplies fuel to the transportation industry, and electricity to businesses and households. Recent ransomware attacks aimed at Western targets, including the energy sector, continue to pose challenges in cybersecurity (Montague, 2023). The recent accidental chemical spill in Ohio also provides insight into the possible outcomes of an intentional cyber-attack against this infrastructure. The regular operations of the chemical sector are imperative to the economic and manufacturing health of state and often involves transporting dangerous chemicals on which other critical infrastructures are dependent (Introduction to the Chemical Sector Risk Management Agency, n.d.).

Cyber threats are of particular concern in Texas, where large corporations continue to relocate, and the population continues to climb. It is imperative industry leaders are able to recognize and identify their cyber risks to develop prevention strategies and respond to cyber-attacks more quickly and effectively. Disruptions to critical infrastructures could lead to theft of intellectual property; supply chain disruption; electricity disruption; loss of operations capacity; or chemical theft, diversion, or release (Introduction to the Chemical Sector Risk Management Agency, n.d.). Texas' industrial vulnerability to cyber-attacks through phishing, ransomware, and malware pose significant threats to the security of critical infrastructures. Securing networks against internal and external cyber-attacks requires industry leaders to be proactive and reactive in their approach.

The proposed paper seeks to present a translational synthesis of the existing literature regarding best cybersecurity practices for securing critical infrastructure in Texas. In doing so, agencies will be able to better align and prioritize cybersecurity initiatives with industry missions, risk tolerance, and resources (Cybersecurity, C.I., 2018). This review will also include recommendations for improving risk readiness for the transportation, energy, and chemical industry in the state moving forward.

Keywords: cybersecurity, transportation, energy, chemical, critical infrastructure

INTRODUCTION AND OVERVIEW

Nearly 25 years ago, the attention of the nation was on the terrorist attacks on September 11, 2001, and in the days that followed, society seemed to virtually shut down. The physical attacks on the World Trade Center were unprecedented in American history and fueled national discussion of the security of the nation's critical infrastructures. The following month, President Bush convened the President's National Infrastructure Advisory Council (NIAC) by executive order whose responsibility since has been to advise the President on practical strategies for industry and government to reduce complex risks to critical infrastructures. The following year, the Department of Homeland Security (DHS) became a formal stand-alone federal department to coordinate and unify national homeland security efforts (Creation of the Department of Homeland Security, n.d.). In the years since, the council's, DHS, and national conversation has extended beyond simply the prevention of physical attacks on critical infrastructure, to ensuring protection and response plans for cyber-attacks on these important assets.

The national Cybersecurity and Infrastructure Security Agency (CISA), part of the DHS, was created by President Trump in 2018. The mission of the cybersecurity division is to defend and secure cyberspace by leading national efforts to drive and enable effective national cyber defense, resilience of national critical functions, and a robust technology ecosystem (Cybersecurity Division, n.d.). To accomplish this, CISA works to fortify the nation's cyber defenses against immediate threats and vulnerabilities, building the nation's long-term capacity to withstand and operate through cyber incidents, to achieve a defensible cyberspace ecosystem by ensuring that changes in the ecosystem shift the advantage to network defenders (Cybersecurity Division, n.d.). They are responsible for strengthening cybersecurity and infrastructure protection across all levels of government, coordinating cybersecurity programs with U.S. states, and improving the governments cybersecurity against both private and nation-state hackers (Cimpanu, 2018). CISA makes critical infrastructure designations because their assets, systems, and networks, both physical and virtual, are considered to be so vital to the United States that their incapacitation or destruction would debilitate the security, national economic security, national public health or safety or some combination, of the entire country (Gregory, 2022). Further, when a cyber-attack occurs against one of these assets, the impact typically goes beyond the direct industrial fall-out by way of a ripple effect with many often-unexpected consequences (Gregory, 2022). The transportation systems sector, chemical sector, and energy sector are among the 16 critical infrastructures in the U.S.

Recent events, such as the novel coronavirus COVID-19 pandemic, provide some insight into what the real-world impact could be if a cyber-attack against critical infrastructure occurred. By mid-2020, the COVID-19 pandemic had significantly impacted the daily lives of people and businesses around the world as the result of mandatory shutdowns and stay at home orders for millions of Texans and Americans (Ivanov & Dolgui, 2020). These orders forced workers out of offices and into work from home situations, for those who were able to keep their jobs, with essential workers comprising those who were leaving the house. These shutdowns had a profound impact on almost every aspect of daily life, including the creation of significant new opportunities for cyber criminals

(Kumar, Sharma, Vachhani, & Yadav, 2022). Cyber security threats were rampant, and employees were now using their home networks to conduct business operations leaving ample opportunity for cyber breaches (Lallie, Shepherd, Nurse, Erola, Epiphaniou, Maple, & Bellekens, 2021). Further, the security of many software products were revealed to be underprepared for the drastic change in the working situations (Georgiadou, Mouzakitis, & Askounis, 2021).

According to a recent report on data breaches, cyber-attacks on critical infrastructure industries cost an average of \$4.8 million, not including the cost to consumers and other businesses, such as the cost associated with supply chain disruption (Gregory, 2022). The development and deployment of the Internet of Things (IoT) has made the cyber-systems of critical assets even more susceptible attack. The primary methods of cyber-attacks to critical assets include IT failure, human error, their-party business partners, destructive attacks, ransomware, and other malicious attacks (Cost of a Data Breach Report 2023, n.d.), and typically cost more than \$1 million more than other types of data breaches (Gregory, 2022). To prepare for and effectively respond to a cyber-attack, it is imperative that critical infrastructure providers understand the most prominent threats facing their cyber-networks so that they can identify their risks (Johnson, 2015). Risk assessment will allow them to work with their cyber-security team and industrial and governmental partners to develop and implement readiness and response plans to future cyber threats. Then, if, or when, a cyber-attack occurs, they are prepared with solutions that make resolution of the immediate issues and any fallout more efficient. Critical infrastructure providers are on the frontline of defense in protecting the transportation, chemical, and energy sectors in the United States and in Texas. The following discussion presents a risk assessment for these critical infrastructures, followed by a discussion of the most prominent cyber-security threats today, and finally, an overview of strategies and recommendations for ensuring that industry leaders and government agencies are risk ready when a cyber-threat is identified.

Problem Statement

Public and private sector critical infrastructure providers face a constantly evolving landscape of increasingly destructive, and rapidly growing number of cyber-threats. Opportunities for cyber attackers have become more prevalent and more attractive as the number of devices with internet capabilities expands (Lee, 2020). The IoT technologies are comprised of computational devices that extend the connectivity of systems and users to improve and optimize real-time operations in every aspect of daily life, including power grids and industrial systems (Stellios et al., 2018). And as more information is stored and shared online, individuals, businesses, and government agencies have more to lose today than ever before (Johnson, 2015). Cyber-attackers can be anyone, including insiders like government employees or industrial employees, as well as external actors (Cormier & Ng, 2020). For example, industry insiders (e.g. poorly trained or disgruntled employees) or incompetent contractors may create opportunities for outsiders to penetrate poorly protected cyber networks and systems (Tal, 2018). Criminal organizations may target industrial cyber systems using spam, phishing, or spyware and malware, for identity theft, online fraud, or computer extortion (Tal, 2018). Cyber-attacks can be designed and targeted to damage or disrupt critical infrastructure necessary to deliver vital services by infiltrating the digital systems that control physical processes, damaging specialized equipment, and disrupting vital services without a physical attack (Johnson, 2015). If used by terrorists, nation states, or cyber-criminal organizations, these attacks could destroy, incapacitate, degrade, or exploit critical infrastructures to threaten national security, weaken the economy, or cause mass casualties.

Critical infrastructure providers are typically industrial partners responsible for the management of cyber networks containing both information technology (IT) and operational technology (OT) increasing their vulnerability to cyber-threats (Ellis, Locasto, & Balenson, 2020). IT systems comprise the network of computers, servers, and mobile devices as well as the information that flows

between them, by being connected to the internet; while OT includes the physical devices and software that control operations in the real world, such as meters or robotics (5 ways to prevent cyber-attacks on critical infrastructure, n.d.). Once an OT system is compromised, the potential for threats is endless as hackers then can disrupt vital services, physically endanger employees and customers, damage or destroy equipment, and harm the environment (5 ways to prevent cyber-attacks on critical infrastructure, n.d.).

Topic Discussion

The daily threat of cyber-attacks on Texas' critical infrastructure present significant challenges for providers in the state. Protecting the state's transportation, energy, and chemical networks is imperative to ensuring the sustainability of daily life and business continuity in the event of a physical- or cyber-attack. The states dependence on these sectors cannot be understated. Texas' transportation sector is massive, consisting of all aviation, highway and motor carriers, maritime transportation systems, mass transit and passenger rails, pipeline systems, freight rails, and postal and shipping operations, each of which have become increasingly reliant on cyber-based control, navigation, tracking, positioning, and communications systems creating ample opportunities for exploitation (Transportation Systems Sector, n.d.). Together, these subsectors are responsible for the quick, safe, and secure movement of people and goods throughout the state, and even the smallest cyber disruption can have catastrophic effects (Transportation Systems Sector, n.d.). Increasingly threats to this critical infrastructure are becoming cyber-physical, and as vehicles, aircrafts, vessels, and control systems are more often connected online, securing both the physical safety and cyber security of these assets will become synonymous (Lehto, 2020). For Texans, protecting more than 300,000 miles of highway, 10,400 miles of freight rail, nearly 400 airports, and 21 seaports, makes ensuring the cyber-security of the transportation sector an enormous operation (McPherson, Donald, & Wright, 2018).

The potential for damage inflicted by a cyber-attack can be seen in all areas of transports. For example, radio frequency technologies, such as automotive radar, are used to increase driving safety and more automated (Yeh, Choi, Prelcic, Bhat, & Heath, 2018). Autonomous vehicles are being tested and deployed (Lim & Taeihagh, 2018). Millions of passengers fly in and out of Texas each year, making aviation both vulnerable and attractive to cyber threats. Smart airports, for example, have emerged in recent years as IoT has enabled enhanced robustness, efficiency and control, and real-time monitoring and analytics of operations and cyber-security (Koroniotiset et al., 2020). While these technologies control the environmental conditions inside the airport, automate passenger-related actions, and support airport security, they also create opportunities for security intrusions into network systems (Koroniotiset et al., 2020). While convenient, this expansion requires connectivity and data sharing across a variety of users (including customers, airline employees, external contractors, etc.) which then creates new opportunities for bad actors to infiltrate secure networks. The complexity of cyber-attacks has also increased, making smart airports more susceptible to network disruption, cancelled travel, or stealing of sensitive information (Koroniotiset et al., 2020). Consider that several times a year, one of the major airlines report significant cyber-disruption to their flight schedules causing delays and cancellations leaving thousands of passengers stranded, making them frustrated, unable to reach their destination, and resulting in significant monetary loss for customers and the airlines themselves. While the cause of these disruptions is often left out of reports, an intentional cyber-attack could cause even more damage by grounding flights, stranding passengers, making it impossible for essential personnel and cargo to be transported in the event of an emergency. Disruptions in the supply chain resulting from the novel coronavirus, COVID-19, provide just a glimpse of the potential impact of an intentional disruption to operations in the transportation sector. The pandemic led to misalignment between supply and demand, resulting from planes, trains, and maritime vessels from transporting goods in a timely or

efficient manner. Delays and congestion both on land and sea lasted months, resulting in shortages in household necessities, cleaning supplies, food, as well as medical supplies, equipment, and medicines themselves. The disruption resulting from the COVID-19 fallout could be much greater if the result of an intentional, organized cyber-attack.

Relatedly, rail cars and maritime vessels often carry large amounts of hazardous materials and chemicals, and sometimes travel in very close proximity to large concentrations of people and industry, drawing attention to another critical infrastructure facing significant cyber threats (5 ways to prevent a cyber-attack on critical infrastructure, n.d.). The regular operations of the chemical sector are imperative to the economic and manufacturing health of the state and often involve transporting dangerous chemicals on which other critical infrastructures are dependent. Comprised of basic, specialty, and agricultural chemicals as well as consumer products, the chemical sector converts raw materials into diverse products that are essential to modern life (Chemical sector, n.d.). Texas is home to nearly 2,000 chemical manufacturing plants, and with Louisiana, produces roughly 80 percent of the nation's main petrochemical supply (Texas Comptroller, n.d.). The amount of data used and produced by the industry makes it difficult to both manage and secure, placing this sector at considerable risk to cyber-threats (Texas Comptroller, n.d.). Increasingly, operational and information technologies converge to allow for remote, real-time access to the operation of chemical facilities (Cormier & Ng, 2020). The uninterrupted operation of these facilities ensures chemicals are used, manufactured, stored, transported and delivered to critical infrastructure and industrial sectors in an efficient and safe manner (Chemical sector, n.d.). The risk posed by disruption to this process was previewed in the West Fertilizer Company explosion in West, Texas in 2013, resulting in chemical fires that killed 15 and injured more than 160 people. The Colonial Pipeline ransomware attack in May 2021, provides additional insight into the potential impact of cyber-attack on this sector. The pipeline spans 5,500 miles stretching from Texas to New York and carries up to 3 million barrels of fuel per day (Gregory, 2022). In this case, hackers utilized ransomware to shut down their operations for nearly a week affecting roughly 12,000 gas stations. The shutdown reduced the amount of fuel available to the East Coast by nearly half leading to gas shortages and higher prices at the pump (Gregory, 2022). Colonial Pipeline paid \$4.5 million in ransom to regain access to comprised systems and was also responsible for paying additional fines for operational lapses and management failures (Gregory, 2022). The Transportation Security Administration for U.S. pipelines also issued a series of new directives to prevent similar attacks and reduce their impact (Gregory, 2022). Finally, the chemical spill following a train derailment in East Palestine, Ohio in February 2023, made the potential devastation posed by an intentional cyber-attack on the transportation and/or chemical sector even more visible. According to the National Transportation Safety Board, a 38-train car derailment was followed by a fire which caused damage to an additional 12 cars (Hauser, 2023). The train was carrying chemicals and combustible materials containing a toxic flammable gas (Hauser, 2023). The derailment, led to evacuation orders in both Pennsylvania and Ohio on either side of the fires, placing thousands of residents at risk (Hauser, 2023). While the toxic chemicals were released from tankers and burned off, the risk faced by local residents included pollution to the air, soil, and water supply (Hauser, 2023). As the second largest chemical manufacturer in the world, unauthorized access to chemical facilities or distribution methods have the potential to devastate the physical and economic well-being of Texas.

Consistent operation of the energy sector ensures the health and welfare of Texans by ensuring steady energy is supplied via electricity, oil, and other natural gas resources, with 43 percent of America's oil refineries located along the Texas and Louisiana coasts. Primarily owned and run in the private sector, Texas' energy infrastructure supplies fuel to the transportation industry, and ensures power distribution to over 26 million customers via natural gas, wind, coal, nuclear, and solar resources (Wind Energy in Texas, n.d.). Ninety percent of the electric load in Texas is managed by the Electric Reliability Council of Texas (ERCOT) who ensures power distribution to over 26 million

customers, connects more than 52,700 miles of transmission lines, and 1,100 generation units (About ERCOT, n.d.). Texas' independent and separate electrical grid is well-known and comprises one of three primary power grids in the United States. Texas' power grid relies on smart technologies that are mostly capable of identifying and preventing known threats (Cheri, Fofana, & Yang, 2021). While most commonly motivated to take advantage of electricity market interactions and electricity price fluctuations (Ahmadian, Malki, & Han, 2018), recent ransomware attacks aimed at Western targets, highlight just some of the challenges in securing the sectors cyber networks. In recent years, extreme weather events, such as the winter storm in February 2021, led to the widespread failure of electric generation facilities across the state. Extreme conditions led to blackouts affecting millions of residents, causing extensive property damage upwards of 80-130 billion dollars, and contributing to at least 210 deaths. These outages combined freezing weather conditions forced businesses to close, icy roads made driving impossible, people were unable to stay warm, they could not prepare food, and operate life-saving medical devices were in cases inoperable. And these were just the effects of a weather event. Consider the potential for harm in the event of a targeted cyber-attack.

As the demand on the state's power grid continues to grow, the threat posed by intentional cyber-actors becomes more significant as the energy sector is an increasingly popular target for hackers experiencing more than 40 industry attacks between 2017-2018 alone (Krauss, 2018). Energy companies are even more vulnerable due to the types of data they possess including consumer and business data as well as proprietary information about their holdings, trading strategies and exploration and production technologies (Krauss, 2018). One of the most infamous cyber-attacks against industrial control systems that threatened energy production critical infrastructure in the United States was a cyber campaign carried out by the cyber espionage group Dragonfly in 2014 and from 2015-2017 (Chowdury & Gkioulos 2021). These hackers were interested in learning both how each energy facility operated as well as how to gain access to operational systems, the Dragonfly potentially obtained the ability to sabotage or gain control of electricity grids and nuclear facilities around the country (Threat Hunter Team, 2017). Their second campaign, Dragonfly 2.0 campaign, further utilized multiple techniques, including malware, to gain access to numerous computer systems and mount sabotage operations that could have disrupted energy supplies (Chowdury & Gkioulos, 2021). This type of intentional disruption to the energy critical infrastructure in Texas could have devastating consequences particularly as the state's population and demand for power continue to grow.

In the coming years, cyber threats to Texas' critical infrastructure will continue to increase. Industry leaders in critical infrastructure must work with government agencies to prepare for, defend against, and respond to cyber intrusions. Cyber-security, at a minimum, ensures that critical infrastructure providers are protected against the criminal or unauthorized use of electronic data. Cyber-security firms are commonly used by both public and private sector providers to ensure the safety and upkeep of their client's cyber networks, systems, connected devices, clouds, and databases through the provision of technology support, managed services, software tools, penetration testing, systems auditing, and vulnerability analysis. While this type of protection is imperative for the protection of critical infrastructure, consider the fallout from a cyber-attack on one of these firms. In 2020, the Texas-based cyber-security firm SolarWinds, was breached by the Russian Foreign Intelligence Service (RSV). The firm provides secure public sector IT management and monitoring services, including regular software updates. During a regular software update providing bug fixes and performance enhancements, hackers simultaneously exploited this vulnerability by taking the opportunity to gain access to, and install malicious software on, SolarWinds widely used network management system, Orion (Temple-Raston, 2021). This intrusion represents a massive cyber-attack against the United States that gave hackers access to thousands of client networks, comprised the cyber-security of roughly 100 companies, including Microsoft, Intel, and Cisco, and

also gave them access to roughly a dozen government agencies, including the Treasury, Justice and Energy departments, the Pentagon, and the Cybersecurity and Infrastructure Security Agency (CISA) (Temple-Raston, 2021). The breadth and type of access they obtained was concerning on multiple fronts, including the possibility of hackers ability to steal, alter, or destroy data, which could have had devastating consequences if targeted at critical infrastructures (Temple-Raston, 2021). While the impact of this attack was not nearly as bad as it could have been, this type of intrusion has the possibility of causing significant cyber-, and even physical-, damage to the Texas' critical infrastructure.

WAY FORWARD

Moving forward, it is vital that government agencies, critical infrastructure providers, and cyber-security experts work together to identify cyber-threats, ensure the readiness of cyber systems to respond to these attacks, and develop solutions for implementation in the event of a cyber-attack. Cyber-attacks are often successful because of user lack of awareness or formal staff training (Chowdury & Gkioulos, 2021). Therefore, in order to respond to a cyber-attack, providers should understand the most prominent types of cyber-threats they are facing. The most common form of cyber-threat facing critical infrastructure are phishing attacks. Phishing occurs when a cyber-actor sends communication mimicking a trusted source to gain access to a cyber-network or system (Johnson, 2015). For critical infrastructure, these attacks may take the form of an email sent to a large group of employees attempting to gain access to a company's cyber network via one of their accounts. For example, hackers would send an email to every employee of a large airline asking them to authenticate their credentials to be able to download a software update with enhanced cybersecurity features. The email might appear to come from a corporate office but would actually contain malicious software in the download link that would allow hackers access to the airline's cyber networks. Related is spear phishing, a more targeted version of phishing, wherein cyber-attackers will research email recipients ahead of time to make their emails appear to be even more legitimate. For example, they might craft an email to a team of utility customer service representatives asking them to click a link to download a software update. The email would appear as though it came directly from their team lead or supervisor, as the from email address would contain this person's name, but it would actually be from a fake email account that is like an actual company email address, but with small differences that would make it difficult to notice if the email was not read carefully. Zero-day attacks are additional threats that occur when hackers identify and exploit weaknesses in a network, software, or hardware before a company has discovered and resolved the issue (Johnson, 2015). Denial-of-Service (DoS) attacks are also prevalent occurring when a network, or device, is bombarded with traffic, overwhelming a system, and preventing it from functioning normally. They can cause systems to crash and prevent them from responding to legitimate requests from customers or employees. Malware/ransomware are among the biggest threats to critical infrastructure. Malware is malicious software that can spy on communications, steal information, damage, or destroy data, or encrypt files once in a cyber network. Ransomware is a type of malware that encrypts files on a corrupted network making it impossible for legitimate users to access these systems and bringing industrial operations to a halt. Once in a system, hackers will ask for a "ransom" to be paid in order to restore access, or decrypt files, so that legitimate use and business can resume. Malware and ransomware can enter a system in multiple ways, including external phishing attacks or internal intentional network intrusion, such as via a corrupted flash drive.

Since 2010, the federal Government Accountability Office (GAO) has called for improvements to cybersecurity around critical infrastructure. In 2017, the President's National Infrastructure Advisory Council likened the nation's cyber positioning to be equivalent to a pre-9/11-level cyber moment, with a narrow and fleeting window of opportunity to coordinate resources effectively. And in early 2023, President Biden issued an executive order prioritizing the expansion of minimum-security

requirements for critical infrastructures as well as improvements in collaboration between public and private sector entities to develop a more expedient and effective cyber incident response. The National Infrastructure Protection Plan (NIPP) further outlines the national vision for protecting critical infrastructure (Cybersecurity and Infrastructure Security Agency, 2019):

A Nation in which physical and cyber critical infrastructure remain secure and resilient, with vulnerabilities reduced, consequences minimized, threats identified and disrupted, and response and recovery hastened. This vision drives the basic approach to critical infrastructure security and resilience in the United States, to: Strengthen the security and resilience of the Nation's critical infrastructure, by managing physical and cyber risks through the collaborative and integrated efforts of the critical infrastructure community.

Identifying and responding to emerging and ongoing cyber threats requires that stakeholders across critical sectors communicate and collaborate to develop cyber response plans. Information sharing within each sector is among the most important activities of an effective and efficient cyber response plan (Johnson, Badger, Waltermire, Snyder, & Skorupka, 2016). The ability to provide actionable threat information to owners and operators of these networks allows them to implement plans and take appropriate action in response to cyber-attacks. Housed in North Texas, Region 6 of the federal governments' CISA delivers services to support the security and resilience of critical infrastructure to owners and providers in conjunction with state, local, tribal, and territorial partners (Cybersecurity and Infrastructure Security Agency, 2019). Together, with well-trained cyber-security professionals, critical infrastructure providers should ensure they have an up to date cyber security response plan in place before an incident occurs. The plan should be among the first steps in generating a culture of cyber-security where every person knows their role and takes action. The plan should be approved by senior leadership and should clarify the roles and responsibilities for critical personnel and their tasks before, during, and after a confirmed or suspected cyber incident (Incident Response Plan (IRP) Basics, n.d.). The incident response plan, should, at a minimum, incorporate the following procedures (Incident Response Plan (IRP) Basics, n.d.):

1. Before a cybersecurity incident

- Train all staff. Since many attacks are possible due to lack of training, missing protocols, or human error, equipping employees with the knowledge, tools, and awareness to be vigilant and responsive can go a long way toward ensuring network security. Ensuring all staff understands their role in ensuring the security of the organization, as well as how to report suspicious events are imperative to an effective plan.
- Review cyber response plan with an attorney, CISA regional team 6, and local law enforcement. Collaboration among each of these ensures the most up to date and comprehensive plan is put into place.
- Print the document and associated contact list and distribute to all personnel. This ensures everyone has access to the information in the event of an attack when digital communication will be shut down.
- Develop a plan and make sure everyone is aware of the role that they play, including who will need to be notified in the event of an attack. This could include board of directors, key investors, and critical partners.
- Review the plan quarterly and adjust in accordance with current threats.
- Prepare press responses in advance.
- Select an outside technical resource or firm that will investigate any breaches.

- Conduct attack simulation exercises to ensure that everyone knows their role and carries it out appropriately.
2. During a cybersecurity incident
 - Assign an Incident Manager who will be responsible for leading the response managing how communication flows, updating stakeholders, and delegating tasks. This person should not be responsible for performing any technical duties.
 - Assign a Tech Manager who will serve as the subject matter expert that brings together internal and external experts.
 - Assign a Communications Manager to interact with reporters, post updates on social media, and interact, as needed, with external stakeholders.
 3. After a cybersecurity incident
 - Hold a formal retrospective meeting to report out the known incident timeline and ask for additions and edits. Security breaches are often the result of multiple person's actions, so make sure these reports are blameless to ensure that all participants feel comfortable speaking freely about the incident.
 - Update policies and procedures based on the meeting.
 - Communicate findings to staff. This contributes to a culture of security and builds trust among staff showing that cyber-security threats are taken seriously.

Critical infrastructure providers should further ensure the following practices (5 ways to prevent cyber-attacks against critical infrastructure, n.d.):

1. Be vigilant and read all emails with a critical eye looking for inconsistencies, grammatical errors, looking for known senders etc. to avoid exposing cyber-systems to cyber-threats.
2. Ensure all networks, systems, and software are up to date and that security patches are applied regularly to avoid vulnerabilities that might leave an opening for a hacker to enter the system.
3. Require strong passwords before access to any critical systems.
4. Utilize multi-factor authentication to ensure only legitimate access to critical cyber networks and systems.
5. Audit devices, assets, and other network components regularly.

Finally, utilities and industrial partners should share best practices for network security and encourage transparency by reporting known cyber-attacks to the appropriate government agency, software providers, other critical infrastructure providers, and the network cybersecurity team for the most timely and efficient response possible. The development and adoption of Artificial Intelligence (AI)-enabled cyber-defense techniques are also needed to protect smart enabled infrastructure to respond to the constantly evolving nature of contemporary cyber-attacks (Koroniotiset et al., 2020).

Texas remains particularly vulnerable to cyber threats as a desirable location to live, work, and conduct business. We have the 9th largest economy in the world, are home to headquarters of more than 50 fortune 500 companies and are the leading destination for companies relocating from other states. For 20 years in a row, Texas has been the number 1 U.S. exporter, with exports totaling approximately \$375 billion in 2021. We are the largest energy-producing state in the nation, and are home to 26 commercial airports, 19 seaports, 22 interstate highways, and 58 freight railroads. Our cyber vulnerabilities are plentiful with many attractive targets for cyber criminals and organizations around the world. It is imperative industry leaders are able to recognize and identify

their cyber risks to develop prevention strategies and respond to cyber-attacks more quickly and effectively. Disruptions to critical infrastructures could lead to theft of intellectual property; supply chain disruption; electricity disruption; loss of operations capacity; or chemical theft, diversion, or release. Texas' industrial vulnerability to cyber-attacks through phishing, ransomware, and malware pose significant threats to the security of our critical infrastructures and daily life. Both public and private sector cybersecurity professionals must remain cognizant of their responsibility to secure the states most important cyber networks.

REFERENCES

For a complete listed of article reference, please see the link below to our online publication forum.

Suggested citation: Nodeland, B. (2023) Ensuring the Cybersecurity of Texas' Critical Infrastructures. (Report No. IHS/CR-2023-1023). The Sam Houston State University Institute for Homeland Security. <https://doi.org/10.17605/OSF.IO/4ZVRU>
One Step Ahead, April 2024, 1-10.

CONVERGENCE OF MISSION AND MOMENT: IMAGINING THE EMERGING TECHNOLOGY ANALYST

Nick Reese

Prepared for Sam Houston State University

Abstract

The Department of Homeland Security (DHS) was built to prevent terror attacks in the homeland and its culture and structure reflect its birth in 2002. Unlike the world changing event that created DHS, the gradual fading of the terror threat has left it misaligned to respond to new nation-state sponsored threats. The homeland security mission is at a true inflection point as it looks for new ways to use its capabilities and authorities while the central force driving global competition is being established. Just as the field of cyber was being established in the late 1990s and early 2000s in response to new threats, so too must the field of emerging technology be developed today. Examining the realities of the world today, we see the need for professionals who specialize in how emerging technologies create risks and opportunities in a way that is distinct from how cyber professionals do the same for the cyber domain. This work examines the geopolitical reality and how it reflects on the homeland. It goes a step further by conducting a comparative analysis between current cyber analyst requirements and skills and what would be required for an equivalent emerging technology analyst. This analysis informs governments, academia, and industry by creating a baseline from which emerging technology professionals can be created and evaluated with direct application on practitioners in critical infrastructure.

INTRODUCTION

The Department of Homeland Security (DHS) was born at a different time. One year, two months, and twenty-four days after the attack on the World Trade Center, Pentagon, and United Flight 93, DHS was born. The Homeland Security Act was signed on November 25, 2002, and carried with it fresh and open wounds from the horrifying attack just over a year past. The authorities granted to the new Department, its Components, and its eager workforce were all shaped by the new geopolitical era that would come to be defined by non-state actors. First responders, critical infrastructure, and industry all followed the lead of the founding of DHS and focused intensely on the prevention of attacks. Another wave of terrorist attacks on U.S. soil was assumed and lawmakers and policy makers marshalled funds and resources to provide the tools homeland security organizations needed for the fight. For the next twenty years, the homeland security mission would be defined by the manner of its birth; secure the homeland against the terrorist threat.

That was then. Still a threat but not nearly with the power and reach to dominate geopolitics, the era of non-state actors such as al-Qaeda, Daesh, and al-Shabab has faded into the shadow of the new era. Unlike the world changing event that created DHS, the gradual fading of the terror threat has left it misaligned to respond to new nation-state sponsored threats. A series of five-year plans

and clockwork eight percent per year economic growth placed China in a position with a new term in geopolitics; near-peer adversary. Bringing small-economied but like-minded allies along, China created the beginning of a geopolitical orbit not seen since Cold War-era capitalism versus communism. National powers around the world are all arriving at the same conclusion at the same time, emerging technology is the source of power of the future.

Technology has been a primary feature of statecraft since the Greeks built defensive walls around Athens in 465 B.C. E. catalyzing the Peloponnesian War. However, today's race centers around technological advancements that dwarf others in the history of statecraft. Artificial intelligence (AI), quantum information science (QIS), new infrastructure for soft power, biotechnology, advanced materials, space capabilities, and other technologies are central to the Chinese plan for usurpation of the U.S. position as the dominant economy and dominant power in the world. A new era of great power competition has begun, and the quantity being competed over is emerging technology and all that supports it.

This paper studies the convergence of two inflection points, the shift of the homeland security mission and the maturation of emerging technology as a defined professional field. This moment in the history of homeland security in the U.S. is one that will be looked back upon and studied as two extraordinary factors are colliding to create the conditions for a new way to define the practice of homeland security. Just as cybersecurity was a new field 30 years ago, so too is emerging technology today. Emerging technology's maturation parallels the trajectory of the homeland security mission provided organizations can identify the global dynamics that will affect them soon. Cyber is the domain where this competition is taking place, but it is not the goal. Global dynamics show us that the goals of our adversaries surround emerging technology and that technology is primarily being developed in the private sector. That means the private sector is the target of cyber actors with nation-state resources behind them who are in pursuit of their most valuable intellectual property. Intellectual property that will be applied to adversarial actions against the homeland. To meet this moment, this study will build the first vision of an emerging technology analyst to help governments, academia, and industry define this new role and the skills required to make impact in this new reality.

STRUCTURE AND CONTEXT

A brief examination of world power dynamics over the last seventy years reveals three significant shifts in the dominant threats to U.S. interests. Post-World War II (WWII), the Cold War era was characterized by a bipolar world with two dominant global powers competing for hegemony.¹ Globally, smaller, less powerful states were pulled into either the capitalism or communism orbit. This competition over economic systems and systems of government created a global arms race that developed into an existential threat to life on earth. The fall of the Soviet Union in 1991 left the U.S. as the unrivaled global hegemon in an era that would soon be defined by the rise of non-state actors.² September 11, 2001, brought a world changing event that pivoted the world's attention to the terrorist threat and defined the practice of homeland security for twenty years. Twenty years of war against terrorism diminished the role of non-state actors in global power dynamics. The era of non-state actors was characterized by ideologically motivated irregular warfare that included a broad sense of good versus evil, making it a compatible issue internationally. Traditional non-allies were happy to collaborate on counterterrorism issues because it was a zero-sum game with little

1 Thies, Cameron; *The Roles of Bipolarity: A Role Theoretic Understanding of the Effects of Ideas and Material Factors on the Cold War*; August 2013; *International Studies Perspectives*, 14 (3), pp 269-288; Oxford University Press

2 Krauthammer, Charles; *The Unipolar Moment*; January 1, 1990; *Foreign Affairs*; <https://www.foreignaffairs.com/articles/1990-01-01/unipolar-moment>

sympathy for terrorist causes and considerable international consequences for lending support. In each of these constructs, the issues of the day drove the application of state power, which in turn drove priorities, budgets, missions, and more. Terms like “national security” or “homeland security” or “economic power” meant measurably different things in different eras because of the geopolitical context. With the benefit of hindsight, we can look at our current era and place a theoretical framework around it to give decision makers the advantage of having the structure and context to make the right decisions.

State power is an elusive term in international relations and is generally understood as the ability of one state to bend the will of another state to take an action it would not otherwise take. Instruments of power in traditional statecraft levers may include military, diplomatic, economic, financial, law enforcement, and others. States also practice soft power such as influence, international institutions, culture, etc. In the context of GPC, power refers to a state’s ability to develop its own statecraft-level technological capabilities and its ability to effectively employ them. Even with significantly larger economies, 2nd and 11th, respectively, China and Russia are in no hurry to engage in a force-on-force hot war with the U.S. and the North Atlantic Treaty Organization (NATO) but are constantly exerting power through cyber-attacks and pouring treasure into the development of emerging technologies such as AI and QIS.³ As these countries continue to sponsor technological development at a state level and continue to refine their craft, they present a real threat to critical infrastructure, democratic institutions, data privacy, military secrets, intelligence methods, border security, and more. Holding one’s water supply system hostage by infiltrating its operational technology systems is certainly a way to bend the will of an adversary to take an action it otherwise would not.

The current GPC era competition is over emerging technologies and the standards and norms of their development and use. Exercising state power is now a function of a state’s ability to develop and employ technology to attain hard power goals, such as cyber-attacks, or to increase its economic footprint in support of soft power goals. Emerging technology is the commodity over which states will compete and around which state power will be defined. Within emerging technology are essential elements that a state must control to be considered a great power. Being a great power in the GPC era means having a strong and attractive innovation ecosystem. Defining this ecosystem gives homeland security professionals both a list of strategic assets that must be protected and a list of targets an adversary might strike. The innovation ecosystem and its strategic importance definitively shift more burden onto the homeland security mission space than in previous eras. Global competition surrounds emerging technology and emerging technology is developed inside a nation’s innovation ecosystem. That innovation ecosystem is the target of disruption and intellectual property theft by adversary nation-states and those actions are taking place inside the homeland. It impacts our critical infrastructure, economic progress, and our top talent. However, if homeland security professionals are to understand what they are protecting, we must define the essential elements of a strong innovation ecosystem; digital creative industries (DCI), advanced materials, strategic investments, and standards and norms.

DCI

A space currently dominated by the U.S., DCI is the industry that creates social media, multimedia platforms, gaming, popular applications, hardware, and other online entertainment. DCI is a critical element because it is the engine that generates the economic value that is then pumped back into the R&D cycle creating new innovations and more economic value. The products of DCI such as social media platforms, mobile devices, and online streaming services provide the infrastruc-

3 Silver, Caleb; *The Top 25 Economies in the World*; September 1, 2022; Investopedia; <https://www.investopedia.com/insights/worlds-top-economies/>

ture on which American soft power is delivered to the world. Those same products represent the platforms on which American offensive cyber capabilities occur and where intelligence collection activities reside. The loss of American dominance in DCI means the loss of a soft power dissemination, control over the cyber battlespace, and the loss of intelligence collection capabilities.

Materials

Continued innovation depends on the availability and production of advanced materials such as new alloys, semiconductors, and lighter carbon materials. The production of advanced materials in turn depends on a complex supply chain that includes the mining of rare earth minerals and possible mining efforts in outer space. Semiconductors are the most ubiquitous and best-known example of the need for advanced materials and the importance of their supply chain. China has already taken significant leaps forward in their domestic semiconductor production, threatening the market share of American companies such as Intel.

Strategic Investment

DCI companies such as Google are involved in the development of new and groundbreaking technologies that have nothing to do with their core business of search engines, social media platforms, or gaming. Google invests significant resources and treasure into biomedical research that may result in extending human life. Google and others are investing strategically to make breakthroughs that will become their core business in the next decade and beyond. They are looking beyond their current economic value and planning for the next innovation that can create and dominate a new market first. Strategic investment should find ways to support emerging technology research with mutual benefit to private companies and the government without crossing the line of state-controlled enterprises like Russia or China.

Standards and Norms

Much like air power in World War I, cyber power in the first decades of the 2000s, and space in 2020, emerging technology is an area where standard and norms are being defined with implications to state power. How standards and norms develop could result in the migration of technology companies and talent to one market over another. In May 2023, the U.S. government published its first ever National Standards Strategy prioritizing U.S. participation in international standards making processes for critical and emerging technology.⁴ This document is a strategic move to position the U.S., and its innovation ecosystem, in a leadership position in standards making.

Putting emerging technology into the right context and defining its critical elements are important first steps. The largest players in the elements of the innovation ecosystem above are in the private sector but their actions have direct impacts on homeland security. The nexus between private sector technology development is a significant feature of a future emerging technology analyst and of the emerging technology field. To build on this understanding, we will move to a comparative analysis of the homeland security mission and emerging technology as a driver of global action.

CONVERGENCE

We reviewed the manner of the birth of DHS, the September 11, 2001, terror attacks. We see how a world changing event created a new U.S. federal government department and how the broader field of homeland security followed the cultural and organizational lead of its establishment. The

4 The White House; *National Standards Strategy for Critical and Emerging Technology*; May 2023; <https://www.whitehouse.gov/wp-content/uploads/2023/05/US-Gov-National-Standards-Strategy-2023.pdf>

homeland security mission space was dominated for over 20 years by the fight against terrorism as the major elements of U.S. national power were focused on the terrorism issue at home and abroad. During that same time, the cyberspace emerged as a contested domain for terrorists, nation-states, and criminals alike. Social media, online gaming, and other online communications also proliferated during the same period. While homeland security organizations focused on detecting explosives on aircraft and stopping plots against domestic targets, the nation-state threat was beginning to emerge in the cyber domain. New capabilities were being developed to attack adversaries in new ways. Ways that allowed for direct attacks on home soil that have not been possible without an invading army in previous generations. Homeland security organizations were certainly not blind to the threat but the context around it would not become clear until much later.

As cyberspace became a contested domain internationally, the world's powers devolved into a constant state of cyber warfare where attacks, disruptions, and persistent presences have become a daily occurrence. Cyber-attacks are not merely launched as an augment to a traditional conflict but used constantly in what USCYBERCOM calls "defend forward."⁵ This constant state of cyberwar developed slowly over time into a defining characteristic of this geopolitical era. Rather than being able to point to one or two defining events such as the fall of the Berlin Wall or the September 11th attacks, two slow burn factors came together to create the dynamics that are changing the homeland security mission. First, twenty years of sustained global pressure eroded the power and reach of the international terrorist groups that carried out complex and multinational attacks. Second, the cyber domain was maturing and with it the professionals that would specialize in cyber. Cyberspace is a contested domain, but it is how other goals are achieved in the same way that control of the air domain helps militaries achieve their goals. Cyber is an attractive method to launch action against an adversary because it is cheap and offers some degree of anonymity. The question that should be asked is not about why or how the cyber domain is being used but what the goals of its use are.

The decrescendo of international terrorist organizations and the crescendo of cyber warfare slowly but definitively changed what is meant by national security and homeland security from the era prior. By the early 2020s it was clear that cyber threats to both information technology (IT) and operational technology (OT) were significant threat vectors and attacks against critical infrastructure by these means could have catastrophic effects on the homeland and the economy. At the same time, scientific and technological breakthroughs were growing new capabilities in emerging technologies like AI, quantum, telecommunications, data, and outer space. Nation-states around the world, including the United States, recognized the strategic advantages conferred upon the state that can bring these capabilities both to the economic market and into their state power arsenals. The nexus with the constant state of cyber warfare was immediately apparent in that states could both augment their cyber capabilities and use the cyber domain to augment their emerging technology capabilities. States could steal intellectual property from an adversary's innovation ecosystem at home to shortcut their own research and development projects. They could likewise outsmart cyber defenses or engage in increasingly effective information operations by bringing technologies like AI to bear. As of 2023, this dynamic is now the one that dominates interactions between adversaries in the cyber domain.

Cyber is a domain but is not itself a goal. Cyber is the "how" but the "what" is equally important. Nation-state conflict and competition increasingly takes place online, but those operations are being done with goals in mind. A review of national priorities around the world over the past three years nets thousands of pages of policy documentation prioritizing emerging technology strategic

5 Goldsmith, Jack; *The United States' Defend Forward Strategy: A Comprehensive Legal Assessment*; March 2022, The Hoover Institute; <https://www.hoover.org/research/united-states-defend-forward-cyber-strategy-comprehensive-legal-assessment>

advantage. As one example, the U.S. signed the Initiative for Critical and Emerging Technologies with a strategically important partner in India using emerging technology as an internationally compatible issue in the same way that counterterrorism was once used.⁶ China's Made in China 2025 plan prioritizes an intelligent Industry 4.0 vision, which would require dominance in areas like Internet of Things (IoT), telecommunications, AI, cloud computing, and more.⁷ In 2017, Russian president Vladimir Putin said that the country that leads in AI will be the leader of the world.⁸ Many more laws, Executive Orders, policies, and priority documents can be found that say the same thing; major powers around the world are prioritizing emerging technologies. With well-developed cyber capabilities and professionals, the cyber domain was the logical place for competition to start and it has been playing out this way since.

This convergence of events creates an entirely new mission dynamic of homeland security organizations across the country and for the professionals that support them. If the development and ultimate leadership in emerging technologies is the stated goal of the world's powers and they are using the cyber domain to execute on their priorities, that means that nation-state actions will by nature take place against targets inside the homeland security mission space. Homeland security professionals must contend with threats that have nation-state level resources and a recognition that targets like critical infrastructure services are legitimate. Success in a newly defined homeland security mission space means first recognizing the shift then bringing existing capabilities and authorities into alignment with contextual realities. The contextual reality that created DHS and rapidly expanded the homeland security mission continues to define its culture today. However, we are in a moment where two slow burning changes have reached inflection points and attention is required. A new professional that can cut across domain expertise and technical expertise and can view risk based on the correct geopolitical context.

BUILDING THE EMERGING TECHNOLOGY ANALYST

This study thus far has focused on the change in geopolitical era and its impact on the security of the homeland, however, this perspective is not the primary focus of the paper. Whether felt directly or as a second or third order effect, the characteristics of any geopolitical era impact governments, private companies, and academic institutions alike. Universities respond to global conditions by offering new programs of study that reflect the needs of public and private employers. Governments respond through budget prioritization, creation of new offices, and adjustments to missions sets. Private companies respond by protecting their interests and offering products and services that reflect the needs of others. Central to all these responses is the people that each organization brings in to lead their response efforts. This dynamic has been on full display over the past twenty years as organizations, public and private, have brought in cyber professionals and universities have increased their cyber-based offerings. While this response has absolutely been warranted, it has only addressed part of the problem.

Cybersecurity will continue to be an extremely important aspect for public, private, and academic organizations and the demand for cyber professionals will remain. What has been missed is that cyber is not a goal. Cyber is a means that nation-states and cyber criminals use to achieve

6 White House; *United States and India Elevate Strategic Partnership with the initiative on Critical and Emerging Technology*; January 31, 2023; <https://www.whitehouse.gov/briefing-room/statements-releases/2023/01/31/fact-sheet-united-states-and-india-elevate-strategic-partnership-with-the-initiative-on-critical-and-emerging-technology-icet/>

7 Kennedy, Scott; *Made in China 2025*; June 1, 2015, CSIS; <https://www.csis.org/analysis/made-china-2025>

8 Maggio, Edoardo; *Putin Believes that Whatever Country has the Best AI will be "the Ruler of the World"*; September 4, 2017; Business Insider; <https://www.businessinsider.com/putin-believes-country-with-best-ai-ruler-of-the-world-2017-9?op=1>

their goal. Cyber's value proposition is that it allows one to infiltrate otherwise sovereign territory and escape with something valuable with a reasonable chance of not being caught or attributed. That's tremendously appealing but only insofar as it yields something of value. Per multiple strategic documents from multiple world power, that something valuable is emerging technology in the form of intellectual property, data, and source code. In the U.S., and in fact in most of the Western world, the value being created in the emerging technology domain is being created by the private sector making it the target for cyber operations with nation-state resources behind them. Many private companies are not equipped to withstand attacks that are funded and resourced by a nation-state government, but they find themselves in the crosshairs. This problem has no singular solution but a part of it is the development of emerging technology as a professional field in the same way that cyber developed over the last thirty years. Augmenting the technical cybersecurity expertise with emerging technology expertise will create a strong team that is trained in both the technical defenses and recognizing the targets before the attack.

Before we think about an emerging technology analyst, we will define the emerging technology professional field. Much like any professional field, there will be areas of specialization and focus but the following characteristics will be critical based on the analysis above.

- **STEM/National Security Blend:** An emerging technology analyst should have a deep STEM background enabling them to be conversant with technologists developing the technologies. Likewise, the analyst should be able to recognize geopolitical factors that may impact emerging technology development or implementation. This crossover will require an equal blend in terms of depth and complexity in both fields.
- **Public/Private Sector:** An emerging technology professional should as a matter of professional development spend time in both the private and public sectors. This will help bridge the gap that characterizes public-private cooperation on technology.
- **Tactical and Strategic:** Emerging technology analysts should be able to recognize how the strategic situation impacts day-to-day missions on the ground. Having direct impact that can be felt by practitioners should be the goal.

The government needs professionals like this to make effective technology and national security policy decisions on critical technology topics. The private sector needs these professionals to identify the targets of significant cyber-attacks to give defenders a real chance to withstand attacks. The question is if an organization will be attacked but its ability to recover. Recovery is important but the emerging technology professional can have impact to the left of the event and help reduce the damage and lessen recovery time. This provides immediate value to private companies who are targets every day. The bridge between the public and private sectors also provides instant value to sides.

Importantly, most strategic national assets in recent decades have been about power projection. Think aircraft carriers, intercontinental ballistic missiles, and long-range bombers. Today, we are adding another strategic asset that by its definition is in the homeland and directly includes private technology firms. The innovation ecosystem is the most valuable strategic asset for the U.S., and it resides inside the homeland. Unlike the traditional view of strategic assets as power projection, the innovation ecosystem is the base from which the U.S. will derive its power for decades to come. In another shift, this strategic asset focuses on the private sector and academic institutions. The crossing of national security and private innovation is the defining characteristic of this geopolitical era and organizations, public and private, need professionals trained to meet this challenge.

CYBER ANALYST EVOLUTION

The cyber analyst position has been around long enough to have gone through a few evolutionary cycles. Appendix A contains two sample job descriptions from major federal government contractors for a cyber analyst and a threat hunting analyst, respectively. In each, education requirements can be offset by years of experience. Both descriptions show the willingness to hire a candidate with only a high school diploma if that person meets the requisite number of years of experience. Certifications of skills like coding, network security, and others are also listed as primary qualifications along with the ability to obtain and maintain a security clearance. Cyber is evolving this way because the skills required to be a cyber analyst can be learned through a variety of means including, but not limited to, formal degree programs. A cyber analyst is becoming a very skills-based profession requiring constant upskilling and updating of current approaches that can be done as a part of a formal study program or within online communities. While traditional degrees in the subject are offered and undertaken by prospective cyber analysts, there are other approaches, and some may decide not to invest in the degree program given the requirements. Cyber analysts are highly technical and specific often with deep expertise in certain types of systems, coding languages, or aspects of cybersecurity.

The field has had time to mature into these highly specific sub-topic areas allowing for greater specialization. An academic institution seeking to serve the needs of cyber analyst professionals must contend with the reality that employers are not necessarily requiring traditional degrees to obtain a well-paying cyber analyst position. The market for cyber skills certification is saturated with companies and certifications that are accepted as the industry standard. Some will choose the traditional route, but others will choose not to incur the costs and spend the same years working to increase years of experience. The skills and experience required to be an effective cyber analyst are well known and accepted across the industry preferencing highly specific skills development and experience at least on par with formal degrees.

BUILDING THE EMERGING TECHNOLOGY ANALYST

The nature of emerging technology as a geopolitical reality demands a different approach for developing professionals. Being a highly specific professional in a single emerging technology area such as AI or quantum is not sufficient. It is also not sufficient for a prospective professional to have the “mile wide, inch deep” approach because understanding the impacts of emerging technologies in various critical infrastructure and homeland security mission areas requires technical knowledge.

As emerging technology matures as a professional and academic field, its definition may change but can at this moment be generally characterized as the study of the impacts of emerging technology research, development, deployment, and implementation on a given mission area.

To affect this outcome, an analyst would have to undertake a significantly different training and continuing education program than a cyber analyst; one that is more conducive to the offerings of academia.

The emerging technology analyst possess a broad base of knowledge but also have enough depth in each to be able to both explain technical topics to non-technical audiences and to evaluate technical details of technology development for their impacts to given mission areas. In this way, the emerging technology analyst requires a knowledge of international relations, advanced mathematics, computer science, physics, sociology, crisis communications, and public policy. The analyst would be required to interface with technical experts and developers, non-technical decision makers, cyber professionals, and academics among others. It is not possible to achieve

this with a pure generalist approach but to overlap more heavily with STEM courses and learning. Much like cyber, emerging technologies evolve and change rapidly making the need for continuing education critical. As such, the following is proposed as a framework for emerging technology education in upper division undergraduate requirements and post-graduate work augmented by professional development training courses:

- A. Courses in Domain Specialty
 - a. Energy
 - b. Law Enforcement
 - c. Healthcare
 - d. Others
- B. Courses in Technical Skills
 - a. Mathematics (linear algebra, calculus, etc.)
 - b. Computer Science
 - c. Data Science
 - d. Physics
 - e. Biology

This course work should be followed up with a for-credit practicum that provides students with scenario-based practical application of the skills they learned.

Professional development courses should be curated over the life of the student's career and provide updates in specific technology areas of strategic importance paired with leadership and organizational management courses:

- A. Quantum
- B. Blockchain
- C. AI
- D. Outer Space
- E. Telecommunications
- F. Organizational Change Management
- G. First Line Leadership
- H. Budget Management
- I. Others

Together, these courses create a consistently relevant path for student success and the continued security of the homeland.

Whereas the skill and education requirements for cyber professionals is trending away from the formal academic institution models, the emerging technology field is by its nature suited for direct and long-lasting engagement between academic institutions and learners. Creating a new model whereby the graduation of a student is not the end of their engagement with the university, but the beginning creates a constant resource for students and a constant source of revenue for academic institutions. Creating both undergraduate and graduate programs that combine domain expertise with technical knowledge will serve students and the homeland by focusing deep skills and understanding. After graduation, academic institutions should create a talent pipeline that offers a variety of professional development and upskilling programs tailored to the working professional and

aligned with specific career phases. In this way, academia can maintain relevance in a new technical field rather than seeing its phasing out as is taking place in the cyber profession. Engagement with the community through events and unique research will augment this approach and create a sustained leadership position attracting students and life-long learners alike. This presents an opportunity for first movers in academia to establish themselves destinations of choice for domain experts to continue their education and create the critical mass of enrollments required to sustain an emerging technology program.

RECOMMENDATIONS

The creation of a new academic and professional discipline is not a simple undertaking and often lags the real-world need. Cyber had to grow and develop into the field it is today but that process has been slow. We are already in a world that demands emerging technology professionals, but defined career paths and training programs are lacking. To affect a more expeditious path to value for private and public organizations, the following recommendations are provided. These recommendations target private companies and academic institutions and serve as actions that can be taken immediately to have direct impact on security across multiple domains.

ACADEMIA

1. *Partnerships and Joint Course Offerings Between Science/Engineering Departments and Policy/National Security Programs:* Building this kind of cross-department learning into program requirements will begin to develop the skills needed to create the type of professional being sought by public and private sectors.
2. *Consulting Practicums:* In-class learning should be paired with experience-based learning that mirrors the real world. Partnerships between academic institutions and private companies will give students experience operating in a private sector environment and responding to challenges that impact their mission. This experience can be carried forward into any future job as added value.
3. *Professional Upskilling Offerings:* Starting with degree-seeking programs will not be sufficient as the current workforce needs to be trained today. A robust offering of professional development courses will give established professionals the ability to bring new skills to their already deep experience providing immediate impact and value to their organizations.

PRIVATE INDUSTRY

1. *Fellowship Programs with Governments:* Industry and government need to speak the same language and opportunities to bring government professionals into private firms and private professionals into government offices on a temporary basis would create immediate value.
2. *Integration of Emerging Technology Talent with Cybersecurity Teams:* Focusing only on cybersecurity is only fighting half the battle. Emerging technology professionals can focus on the goals of the cyber intrusion to help vector defenses and speed up recovery.
3. *Funding for STEM Professional Development:* Private companies should increase professional development funding for STEM fields to give all employees a better view into the critical context all firms operate inside.

PRACTICAL APPLICATION

Cyber programs in academia abound because they've had 30 years to mature. Emerging technology programs are just beginning as top universities respond to the demands from industry and

governments. Creating unique student experiences that prepare them for practical realities must reflect the environment in which they will operate. Homeland security professionals are securing a homeland that includes the most valuable strategic assets our country possesses, our innovation ecosystem and its products. Those assets are also targets meaning that analysts, officers, and agents throughout the homeland security enterprise will need to be able to recognize the reasons behind cyber intrusions, not simply that one has occurred. Mitigating cyber events remains important but why the event occurred at all is key for practitioners so they can prevent the next one. Critical infrastructure will continue to be both enhanced and threatened by emerging technologies as new capabilities and use cases emerge. The security of the homeland does not hinge on the development of any specific technology but of the people who are managing risk and evaluating opportunities. Those people must be prepared and have an academic partner who will continue to provide them with updated content throughout their professional journeys.

Remaining geopolitically competitive and maintaining our national security means having and securing a robust innovation ecosystem. That ecosystem is inside the homeland and contains private companies. Those companies are targets of well-resourced cyber actors who seek their valuable intellectual property, and this dynamic will define this era. Emerging technology as a profession is in its earliest stages of life, but the requirements are present today. Academic institutions could create a strong program to meet student needs throughout their career lifecycle keeping them relevant and valuable to organizations. Further, academic institutions can avoid a situation mirroring the cyber field where degrees and certificates are no longer strictly necessary for employment. The inflection point is now.

APPENDIX A: SAMPLE CYBER JOB DESCRIPTIONS

Key Role:

Perform advanced analysis of adversary tradecraft, malicious code, and capabilities. Provide intelligence analysis of cyber threats and develop briefings and reports to distribute and aid in information sharing and protection efforts among senior government members and Combatant Commands. Develop and maintain subject matter expertise of Advanced Persistent Threats and assist with Incident Response efforts. Perform advanced research into threat actor and adversary capabilities and develop custom threat intelligence reports to assist ongoing mission efforts.

Basic Qualifications:

- Experience with extensive military and cyber threat operations.
- Ability to work in a high paced and dynamic work environment.
- TS/SCI clearance.
- HS diploma or GED and 8 years of experience in IT and cyber threat information, or Associate's degree and 6 years of experience in IT and cyber threat information.

Additional Qualifications:

- Experience in the Joint Staff or other U.S. Military Staff.
- Experience with Microsoft Office products.
- Knowledge of JCIDS.
- CISSP, GREM, GCIH, or GCIA Certification.
- Completion of DAU training.

Clearance:

Applicants selected will be subject to a security investigation and may need to meet eligibility requirements for access to classified information; TS/SCI clearance is required.

Compensation

At Booz Allen, we celebrate your contributions, provide you with opportunities and choices, and support your total well-being. Our offerings include health, life, disability, financial, and retirement benefits, as well as paid leave, professional development, tuition assistance, work-life programs, and dependent care. Our recognition awards program acknowledges employees for exceptional performance and superior demonstration of our values. Full-time and part-time employees working at least 20 hours a week on a regular basis is eligible to participate in Booz Allen's benefit programs. Individuals that do not meet the threshold are only eligible for select offerings, not inclusive of health benefits. We encourage you to learn more about our total benefits by visiting the Resource page on our Careers site and reviewing Our Employee Benefits page.

Salary at Booz Allen is determined by various factors, including but not limited to location, the individual's particular combination of education, knowledge, skills, competencies, and experience, as well as contract-specific affordability and organizational requirements. The projected compensation range for this position is \$81,800.00 to \$186,000.00 (annualized USD). The estimate displayed represents the typical salary range for this position and is just one component of Booz Allen's total compensation package for employees.

Work Model

Our people-first culture prioritizes the benefits of flexibility and collaboration, whether that happens in person or remotely.

If this position is listed as remote or hybrid, you'll periodically work from a Booz Allen or client site facility.

If this position is listed as onsite, you'll work with colleagues and clients in person, as needed for the specific role.

EEO Commitment

We're an equal employment opportunity/affirmative action employer that empowers our people to fearlessly drive change – no matter their race, color, ethnicity, religion, sex (including pregnancy, childbirth, lactation, or related medical conditions), national origin, ancestry, age, marital status, sexual orientation, gender identity and expression, disability, veteran status, military or uniformed service member status, genetic information, or any other status protected by applicable federal, state, local, or international law.

Responsibilities:

Peraton is seeking a Threat Hunting Analyst to join our team of qualified and diverse individuals. The qualified applicant will become part of Department of State (DOS) Consular Affairs Enterprise Infrastructure Operations (CAEIO) Program, for the Bureau of Consular Affairs (CA). This initiative is to provide IT Operations and Maintenance to modernize the legacy networks, applications, and databases supporting CA services globally.

Day to Day Work Responsibilities:

- Conducts research and data correlation using a variety of enterprise data sources with specific emphasis on network operations and cyber warfare tactics, techniques, and procedures.
- Analyzes network events to determine the impact on current operations and conduct research to determine adversary capability and intent.
- Analyzes identified malicious network and system log activity to determine weaknesses exploited, exploitation methods, effects on systems and information.
- Collects and analyzes network device integrity data for signs of tampering or compromise.
- Prepares assessments and cyber threat profiles of current events based on the sophisticated collection, research, and analysis of information.
- Conducts data analysis in support of directed assessments, anomaly investigations, long term trending and system check out.
- Develops and maintains analytical procedures to meet changing requirements and customer inquiries.
- Serves as the cyber technical liaison to stakeholders, explaining investigation details.
- Tracks and documents incident response activities and provides updates to leadership through executive summaries and in-depth technical reports.
- Create, discuss, and explain Cyber investigative documentation.
- Resolve highly complex malware and intrusion issues using computer host analysis, forensics, and reverse engineering.
- Characterize and analyze network traffic, identify anomalous activity / potential threats, and analyze anomalies in network traffic using metadata.

Qualifications:**Basic Qualifications:**

- US Citizenship required and an active **TOP SECRET** clearance.
- BS degree and 12 to 15 years', experience or MS degree with 10 to 13 years', experience or a high school diploma/equivalent with minimum 16 years', experience.
- Possess CISSP or similar cybersecurity certification.
- 8+ years of directly relevant experience in cyber forensic and network investigations using leading edge technologies and industry standard forensic tools.
- Experience with reconstructing a malicious attack or activity.
- In depth knowledge and experience of identifying different classes and characterization of attacks and attack stages.

Preferred Qualifications:

- Knowledge of cybersecurity frameworks and standards.
- Ability to track incidents using MITRE ATT&CK and Cyber Kill Chain methodology.
- Knowledge of cloud security.
- Knowledge of current IT security best practices.

- Knowledge of system administration, networking, and operating system hardening techniques.
- Mixed operating systems experience: (Linux, Windows).
- Scripting/coding experience.

Shift/Hours: 1st Shift - Monday through Friday.

Peraton Overview:

Peraton drives missions of consequence spanning the globe and extending to the farthest reaches of the galaxy. As the world's leading mission capability integrator and transformative enterprise IT provider, we deliver trusted and highly differentiated national security solutions and technologies that keep people safe and secure. Peraton serves as a valued partner to essential government agencies across the intelligence, space, cyber, defense, civilian, health, and state and local markets. Every day, our employees do the can't be done, solving the most daunting challenges facing our customers.

Target Salary Range: \$146,000 - \$234,000. This represents the typical salary range for this position based on experience and other factors. EEO Tagline (Text Only): An Equal Opportunity Employer including Disability/Veteran.

REFERENCES

For a complete listed of article reference, please see the link below to our online publication forum.

Suggested citation: Reese, N. (2023) Convergence of Mission and Moment: Imagining the Emerging Technology Analyst. (Report No. IHS/CR-2023-1025). The Sam Houston State University Institute for Homeland Security. <https://doi.org/10.17605/OSF.IO/JXWRF>
One Step Ahead, April 2024, 11-24.

UNSEEN THREATS TO TEXAS CRITICAL INFRASTRUCTURE: THE RISK TO BURIED UTILITIES AND TARGETED POLICY SOLUTIONS TO PROTECT THEM

Benjamin Dierker
Prepared for Sam Houston State University

Abstract

Excavation damage to underground infrastructure is a nationwide challenge. Ranging from a local nuisance to both lethal and regional crises, the damage and costs from buried facility strikes are almost entirely preventable. Texas is at unique risk because of its concentrated energy infrastructure, its considerable and growing population, and its competitive economy that ensures constant development activity. Each of these factors correlate to excavation damage and help explain why Texas routinely leads the nation in excavation damage incidents that disrupt critical energy and services. Billions of dollars in economic harm, waste, and inefficiency emanate from this issue and ripple throughout the Lone Star State every year. Solutions include systemic implementation of validated technology, adherence to best practices, and public policy reforms proven to reduce this damage to virtually zero – sparing lives, saving dollars, and protecting critical infrastructure.

Key Words: Damage Prevention, Excavation, Pipelines, Utilities, Infrastructure, Natural Gas, One-Call, 811

INTRODUCTION

Texas is the energy capital of the world and facilitates the exploration and production, transportation, refining, and consumption of oil and gas as well as wind energy at higher levels than anywhere else in the United States. Texas uniquely features its own energy grid, distinct from the Eastern and Western Interconnections that unite the rest of the states with one another. These

Benjamin is the Executive Director of the Alliance for Innovation and Infrastructure, specializing in economic, administrative, and legal aspects of American energy, transportation, infrastructure, and innovation. His goal is to analyze and explain the economic and legal realities underpinning public policy at the state and federal level. He strives to bring a balanced, accurate, and accessible perspective to enable students, specialists, the public, and elected representatives to make the best informed decisions on these critical issues.

Benjamin is a graduate of Texas A&M University, where he earned a Bachelor of Arts in Economics and a Master of Public Administration at the Bush School of Government and Public Service. He then earned his Juris Doctor from the Antonin Scalia Law School at George Mason University. He is admitted to practice law in Washington, D.C. and South Carolina.

bdierker@aii.org
<https://www.linkedin.com/in/benjamin-r-dierker>

energy infrastructure components result in millions of linear miles of pipelines, cables, and wires spanning the state. While many of these assets are overhead, such as powerlines and telecommunications towers, a significant proportion is buried – a process known as *undergrounding*.

Among the buried facilities in the Lone Star State are 488,564 miles¹ of pipelines, more than any other state.² As the top class of critical infrastructure – and also the most dangerous if damaged – the over 230,000 miles of natural gas pipelines receive heightened focus. Together with these pipelines, there are a total of over 7 million miles of pipes, cables, and wires comprising the Texas network of underground infrastructure.³ The true mileage is likely even higher, and Texas hosts over one-quarter of all buried infrastructure in the United States.⁴

Every construction project that involves breaking ground, including thousands of landscaping tasks, home projects, and other digging activities, puts buried infrastructure at risk. This not only threatens to damage the infrastructure itself but can result in serious injury or death to the excavator or homeowner. Moreover, it results in extensive economic consequences that ripple throughout the community.

This makes every digging project a potential safety risk, economic risk, and environmental concern due to the potential to strike buried service lines that are powering the community. The more digging that takes place, the more these risks arise.

Since 2020, Texas received the highest number of new residents of any state.⁵ All factors indicate that the Texas population will continue to grow,⁶ which will result in both greater construction spending and development activity. The growing population will require more utilities to serve their needs – increasing demand for undergrounding of new pipelines, buried cables and wires, and related infrastructure. This will in turn require new trenches and digging to place these lines underground, which threatens existing buried facilities and increases the total amount of buried infrastructure, thus increasing the probability of future damage.

These factors raise questions about the current state of critical buried infrastructure in Texas, what solutions and processes are currently in place to address it, and what private sector and public responses may be warranted.

STATE OF BURIED INFRASTRUCTURE IN TEXAS

While visible infrastructure gets the most attention, out-of-sight components are very often out-of-mind. In Texas, surface-level infrastructure is often well-maintained and safe. For instance, the state ranks 51 out of 52 for percentage of structurally deficient bridges – in other words, Texas is second only to Arizona in having the lowest percentage of the state's bridges in need of critical repair. Below ground is another story.

- 1 Texas Railroad Commission. (2023). *Texas Pipeline System Mileage*. Texas Pipeline System mileage. <https://www.rrc.texas.gov/pipeline-safety/reports/texas-pipeline-system-mileage/>.
- 2 Texas Railroad Commission. (2023). *Texans need to call 811 before digging projects*. Texas Railroad Commission. <https://www.rrc.texas.gov/news/040821-safe-digging-month/>.
- 3 The number is likely much higher, as this figure is older than two years old. See, <https://texas811.org/pdf/Texas811-Digital-Ads.pdf>.
- 4 See, Dierker, B., (2020). *The Longest Running Statistic*. Alliance for Innovation and Infrastructure. Aii.org.
- 5 U.S. Census Bureau. (2023, April 3). *Growth in U.S. population shows early indication of recovery amid covid-19 pandemic*. Census.gov. <https://www.census.gov/newsroom/press-releases/2022/2022-population-estimates.html>.
- 6 From Texas's fifth highest birth rate in the nation, from high domestic migration, and its unique position on the border receiving international migration. See, *Fastest Growing States 2023*. Fastest growing states 2023. (2023). <https://worldpopulationreview.com/state-rankings/fastest-growing-states>.

Texas reports the highest number of excavation damage events in the country every year at nearly twice the level of the next highest state.⁷

Nationally, the most-damaged facility is telecommunications lines followed by natural gas pipelines.⁸ In Texas, this same trend is observed – although in 2021 damage to natural gas pipeline from excavation were reported at a higher level than any other facility type.

These facilities are each critical, and disruptions have far-reaching consequences. Damage to telecommunications lines may not strike the average person as highly consequential, but it should be a cause of concern. When these lines are cut, individuals, homes, businesses, and even entire communities may lose access to the Internet or related communications services. This shuts economic activity, interferes with modern appliances, creates cyber and building security concerns, and threatens the interconnectedness of modern technology and society. Repair may take hours or days, and the costs climb the longer Texans are without Internet, phone, and other related services.

The risks associated with natural gas pipeline damage need less explanation. From silent gas leaks to fiery explosions, there are fatal consequences to striking these lines, which also come with serious price tags. Alarming, in Texas natural gas pipelines are experiencing more damage from excavation each year. Even in 2020, when national excavation damage rate fell due to construction slowdowns and COVID-19 policy disruptions, the number of excavation damage events to natural gas pipelines in Texas increased. Similarly, in 2021, when the state’s primary damage reporter sent no records to the industry tracker, there was still an increase in reported digging-related damage to natural gas pipelines. This likely means the true excavation damage numbers are even higher, and natural gas distribution lines in Texas are particularly at risk.

Reported Unique Damages by Facility Operation

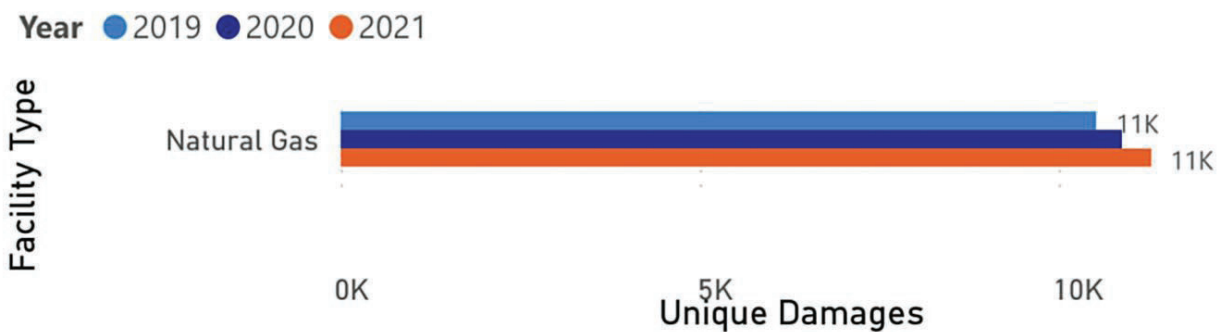


Figure 1: Three-year trend in excavation damage to Texas natural gas infrastructure (Source: Common Ground Alliance)

According to data from the Pipeline and Hazardous Materials Safety Administration (PHMSA), Texas has a disproportion pipeline excavation damage problem compared with other states. In 2022, for all reported pipeline excavation damage incidents across the country, 18.9 percent oc-

7 Reporting in 2021 was irregular and despite this, expert analysis maintains that Texas had the highest level of damage in that year, consistent with prior years. The discrepancy is explained by a primary reporter in the state failing to report damage for that year. See, Common Ground Alliance. (2022). *Damage Information Reporting Tool Interactive Dashboard*. <https://commongroundalliance.com/DIRT-Dashboard>. and Dierker, B. (January, 2023). *Improving Upon Our Dig Laws: Why Data Must Take Center Stage to Reform Damage Prevention*. Alliance for Innovation and Infrastructure. <https://www.aii.org/wp-content/uploads/2023/01/Improving-Upon-Our-Dig-Laws-2021-Data.pdf>.

8 Supra note 8, DIRT Explorer.

curred in Texas.⁹ Even though it is a single state, we know Texas has more mileage of pipelines than most states, so that is not cause for concern on its own. The disproportionate impact is seen more clearly in the reported costs and product lost associated with these pipeline strikes.

Last year, the share of reported costs for all national pipeline damage that occurred in Texas was 82 percent, while Texas represented 100 percent of the reported barrels spilled from excavation damage nationally.¹⁰ At over \$8 million and nearly 6,000 barrels spilled, Texas residents, environment, and infrastructure experienced real negative impacts; but even this is only a partial picture.

While those incidents had to be reported to the federal government, they only involve a handful of facility types, namely certain gas distribution, hazardous liquids, and gravity and reporting-regulated gathering hazardous liquids lines. This small set of pipelines under federal jurisdiction pale in comparison to the linear mileage of other gas and liquid transmission and distribution lines, telecommunications cable and wire, electrical lines, and other public utilities.

To understand the overall impact, we can look to the Common Ground Alliance (CGA), the trade organization comprising stakeholders from across industries in excavation, utility locating, utility owners and operators, and others. CGA compiles voluntary damage reports across all infrastructure types and also presents a framework for understanding direct and indirect costs from excavation damage. The ripple associated with a single pipeline incident, for instance will go on to impact the community at large and even the entire state economy.

By a factor of 30:1, indirect costs are borne by individuals and communities entirely uninvolved in the excavation and construction process.¹¹ These include road closures, emergency vehicles, construction delays, traffic, lost services (e.g., water, internet, power), lost productivity, and over a dozen other impacts.¹² This means that just the relative handful of pipeline incidents from Texas in 2022 – that were reportable to the federal government and overseen by PHMSA (reportedly \$8 million) – likely cost Texas residents a total of around \$250 million in both direct and indirect costs.

When the other thousands of digging-related damage incidents to non-federally-governed pipes, cables, and wires are added in, Texas faces upwards of \$4 billion annually in avoidable economic harm.¹³ These expenses manifest in out-of-pocket dollars, lights not turning on when the switch is flipped, Internet outages, traffic delays, and many other impacts statewide.

In Texas, a typical year results in over 70,000 reports of excavation damage.¹⁴ These reports are made voluntarily by industry stakeholders, which means that many buried facility strikes go unreported. The reports may come from the excavator, locators, 811 call centers, utility companies,

9 Pipeline and Hazardous Materials Safety Administration. (2023). *PHMSA Pipeline Incidents: (2003-2022)*. US DOT Pipeline and Hazardous Materials Safety Administration. <https://www.phmsa.dot.gov/data-and-statistics/pipeline/pipeline-incident-20-year-trends>.

10 *Id.*

11 Common Ground Alliance. (October, 2020). *Damage Information Reporting Tool, Volume 16*. <https://commongroundalliance.com/Portals/0/Library/2020/DIRT%20Reports/2019%20DIRT%20Report%20FINAL.pdf?ver=2020-10-14-185343-180>.

12 Zeiss, G. (2020, April 14). *Cost of underground utility damage represents a major drag on national economies*. Between the Poles. <https://geospatial.blogs.com/geospatial/2020/04/cost-of-underground-utility-damage-represents-a-major-drag-on-national-economies.html>.

13 Infrastructure Protection Coalition. (2021). *Texas Report, 811 Emergency, \$61 Billion Lost to Waste, Inefficiency in System to Protect Underground Utilities*. <https://www.ipcweb.org/images/reports/TX-RPT.pdf>.

14 The reported figure for 2019 is 70,011. The data for 2020 was atypical due to COVID-19, while in 2021 the largest stakeholder group in Texas failed to provide voluntary reporting thus negating the data quality considerably.

bystanders, or other stakeholders. After telecommunications and natural gas infrastructure, these excavation incidents result in damage to Texans' cable, electric, water, sewer, other liquid pipe, steam, and more buried utilities.

Another interesting feature of excavation damage in Texas is its seasonal damage numbers. While nationally, the summer is the peak for excavation damage, Texas appears to peak in September and into the fall. This may be due to weather and climate in Texas, making summer construction less desirable or efficient.

It also presents a unique opportunity for Texas to lead on this issue, learning from national trends occurring in the months before and implementing systemic reforms ahead of its own construction peak.

Damage Timeline

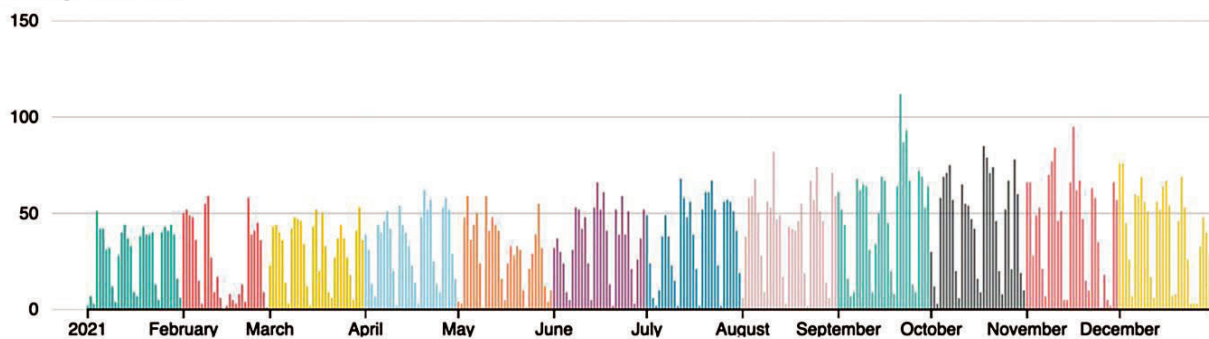


Figure 2: Timeline of reported excavation damage events in Texas in 2021 (Source: Common Ground Alliance)

CURRENT SOLUTIONS AND PROCESSES

There is a process for preventing excavation damage that is longstanding and well-established. With proper use of the 811 “call before you dig” process, virtually every excavation project can avoid striking buried utilities irrespective of how many lines may be underfoot.

The process is simple: anyone doing any digging with shovels, rakes, augers, backhoes, excavators, or other ground-breaking tools notifies 811 – either by phone or on the state’s call center website – to present advanced notice of a dig and to request utility locating. The one-call center enters the information to see whether the proposed excavation site overlaps with known facilities in their database, which is created by utilities submitting their records. Any overlap results in out-bound notifications to the implicated facility owners/operators. Those utility operators then send in-house or third-party contract locators to the site to identify and mark the presence and location of any buried facilities with color-coded spray paint markings to designate the tolerance zones for the buried infrastructure. This spray paint displayed across city streets, sidewalks, and green spaces are the guidelines excavators use to avoid striking buried utilities.

The Texas 811 system is one of the best in the nation, despite the record of high damage numbers. The call center offers homeowners and excavators a log-in portal, where they can provide notice of their intent to dig and request a location. From there, they can also check the status of their ticket and see which utilities will have to respond and whether each has it in real time.

There is a mapping tool integrated with GoogleMaps that allows excavators to designate their dig site from an overhead perspective. This allows the excavator or homeowner to set a GPS pin over their dig site or draw a rectangle that covers the area of the dig. However, many virtual fields are

not required, and an excavator can provide poor information to the call center and by extension to the utility companies and their locators.

Overall, the process offers great potential but does not extract the highest value from it. Despite considerable advancements in technology and best practices, the overall process of notifying a call center and receiving spray paint markings at a proposed dig site looks virtually identical to the how it looked a decade ago, if not last century. While industry stakeholders boast that when 811 is called, damage is avoided 99 percent of the time, there are many incidents that still happen after a call has been made and there are considerable costs associated with the current process.

Astonishingly, experts assess that there is an *additional* \$4 billion in annual costs dragging on the Texas economy that actually comes from the process of preventing excavation damage in the first place. These are *not* damage costs nor do they represent investments; rather this sum represents waste and inefficiency within the system. That means that joined with the direct and indirect costs rippling through the community from damage, there is a combined total of \$8 billion in economic harm and drag on the Texas economy every year. Fortunately, virtually all of this multibillion-dollar harm can be streamlined and eliminated while preventing more damage than before and ensuring safer construction and infrastructure reliability for every Texan.

NEEDED SOLUTIONS AND PROCESSES

Texas has more buried infrastructure than any state and has the second largest economy within the United States. It is only reasonable, then, to expect a higher level of excavation damage, given the strong correlation between construction spending and damage to buried utilities. But the damage prevention process promises to prevent damage regardless of how much infrastructure is beneath the ground and how much ground-breaking occurs.

Texas stands to be the uncontested leader in reducing its damage numbers by implementing reforms that would make good on the promise of damage prevention. Given the state's high mileage of buried utilities and active construction industry, it could achieve a disproportionately *low* level of excavation damage.

Many of the processes needed are ready to be implemented systemically within the existing process. Not only are they available, but they are also consensus best practices, not only by unanimous industry approval, but by validation and recommendations from key safety agencies in the federal government. Texas is already halfway to fully integrating these, and through close collaboration between industry and policymakers, the Lone Star state can lead the nation as the lone state with all key reforms in place.

The four key steps include continue promoting use of web-entry locate requests, allowing ticket scheduling and prioritization, integrating electronic white-lining, and ensuring systemic use of enhanced positive response.

Contacting Texas811

In 2005, the Federal Communications Commission designated 8-1-1 as the "Nationwide Number to Protect Pipelines, Utilities from Excavation Damage." This enormous leap forward consolidated the thousands of 10-digit phone numbers from state call centers and individual utilities spread across the country into a unified program that operates like 9-1-1. Homeowners or excavators simply dial 811 from anywhere and reach their state or regional call center.

"Call 811 Before You Dig" and similar variants became the nationwide slogan that has been reinforced in marketing campaigns for nearly two decades. Recently, however, there has been a

national shift toward excavators using their state’s call center website to directly enter their dig information. Web-entry (or online portal) tickets have been shown in some places to reduce damage in half relative to call-in notice. With this finding, alongside the revealed preference and industry trend, a more intentional move to web-entry should be cultivated with less reliance on “calling” before you dig as a central message.

Texas already uses “contact 811” rather than “call” or “dial” like other states. This helps express neutrality between “clicks and calls,” but there is room for improvement.

In Canada, “click before you dig” is the preferred slogan, because 811 was already designated for another purpose in that country. This preferential marketing helped lead to over 75 percent of incoming locate requests to be made online rather than by phone. When notification center leaders in Canada assessed the impact of web-entry and call-ins, they found that among known damages for which notice was given, calls were responsible for twice the damage of web-entry. Simply stated, “Analysis has proven that the online locate request process significantly reduces damage to underground infrastructure. The more we shift Calls to Clicks, the less damage there will be.”¹⁵ It also allowed a streamlined process, eliminating redundant or unnecessary overhead and personnel to operate phones even while increasing hour of operations and expanding service areas.

In Texas, the “*contact*” or “*connect*” with 811 has flexibility, but still fails to encourage the more efficient and damage-preventing online portal. Because the website URL includes the phone number (Texas811.com), many excavators will likely utilize the online function even if directed to “811” generally. Still, a more intentional approach to direct excavators to the website would help reduce damage and streamline costs, directly affecting both sides of the \$8 billion annual economic drag in the state.

TICKET SCHEDULING AND PRIORITIZATION

Part of what makes web-entered tickets desirable is that excavators can enter information at their own pace, submit multiple locate requests at once, and use the website at any time of day or night. Once on that platform, however, homeowners and excavators have a rigid option: request a locate to be performed in the next two business days.

Excavator interests are not always aligned with the interests of locators or utility companies. It is not uncommon for excavators to request a locate for a large scale project only to complete a small portion of the work within the ticket window. This necessitates additional locate requests and site visits by locators to refresh or update the marks – or leads excavators to dig outside of the ticket window in violation of law and best practices because old marks are present. Offering a scheduling option would likely ensure more efficient locating, which would both streamline costs and reduce locator burdens and error, again tackling both sides of the \$8 billion coin.

There is currently no option for scheduling in standard online portal requests. Further, while all tickets are free, offering a paid alternative could incentivize marginal excavators to provide notice rather than risk digging. That is because some excavators on tight deadlines choose not to provide notice and wait two days – in fact, according to research from North Carolina, as much as 85 percent of “no call” damage likely comes from excavators who know about 811, but who choose not to provide notice. Offering optional, low cost, paid priority tickets may be worth it to capture this significant proportion of stakeholders.

15 British Columbia Common Ground Alliance. (2017). *QR Code To Click Before You Dig!* <https://commongroundbc.ca/april-is-safe-dig-month/qr-code-to-click-before-you-dig/>

Improving Electronic White-Lining

All 16 stakeholder groups within the Common Ground Alliance have unanimously agreed that electronic white-lining is a best practice and that it should be the first step in the ideal dig of the future. Texas811 offers a resource that reaches toward this goal but requires improvements to unlock its full potential.

When submitting a locate request, Texas811 does ask if the excavator has used white spray paint, stakes, or flags to designate the project area, stating “These markings show the locators exactly where you intend to dig.” Nevertheless, it is not required either by the call center or state law. This simple step could be required by law, although a simpler option is to incorporate virtual processes alongside a web-entry locate request.

Texas811 offers a map interface that enables excavators to draw their dig site onto a GoogleMap. More impressively, the platform allows users to switch between a road map view, a terrain (satellite) view, and a hybrid view, and even gives the option to view Bing versions of these aerial maps. This map is used to generate a polygon to overlap with known utility lines on the call center’s side of the system.

The benefit of electronic white-lining is that it offers excavators the ability to pre-mark their dig site from a remote location, which eliminates waste like multiple unnecessary site visits. It also allows a unique aerial perspective for the excavator to clearly and precisely delineate the actual dig they intend to undertake. By doing so virtually, they unlock the benefits of physical pre-marking with white spray paint while giving locators and utility companies the clearest view of where digging will occur. By sharing this virtually, it may help screen out unnecessary locates, and can spare locator resources by narrowing the area in need of marking.

In Texas811’s online portal, the pre-marking tool specifically explains to “Use this tool to draw a rectangle **around your property**” (emphasis added). It does not say “around your dig site.” This partially undermines the purpose of pre-marking with a virtual tool. All this does is ensure the locators go to the right address, without narrowing down the location of the dig.¹⁶

The reform would be to allow the excavator to drop multiple points to form or draw their own pre-dig polygon and send it in addition to the buffered notification polygon. This way, all relevant utility companies are still notified because of the larger buffer zone but they and their locators can also see where the excavator intends to dig precisely. For a given home landscaping project, with an input rectangle of approximately 315 feet in perimeter and 6,500 square feet in area, the polygon Texas811 generates to notify utilities is as much as 895 feet in perimeter and 44,800 square feet, an increase of around 185 percent in perimeter and 500 percent in area.

¹⁶ For a homeowner locate, this is likely not a problem, but on larger property or for professional contractors working at commercial or larger developments, having a more precise tool is important.

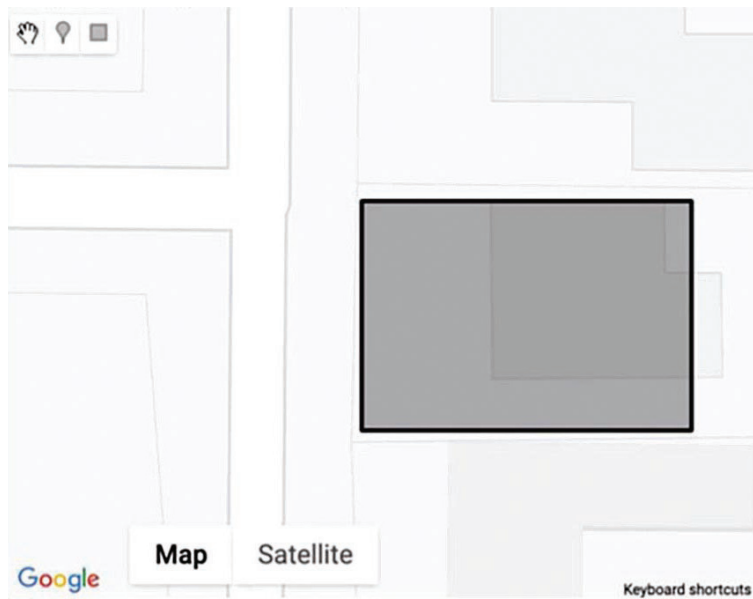


Figure 3: Excavator-entered dig site identification

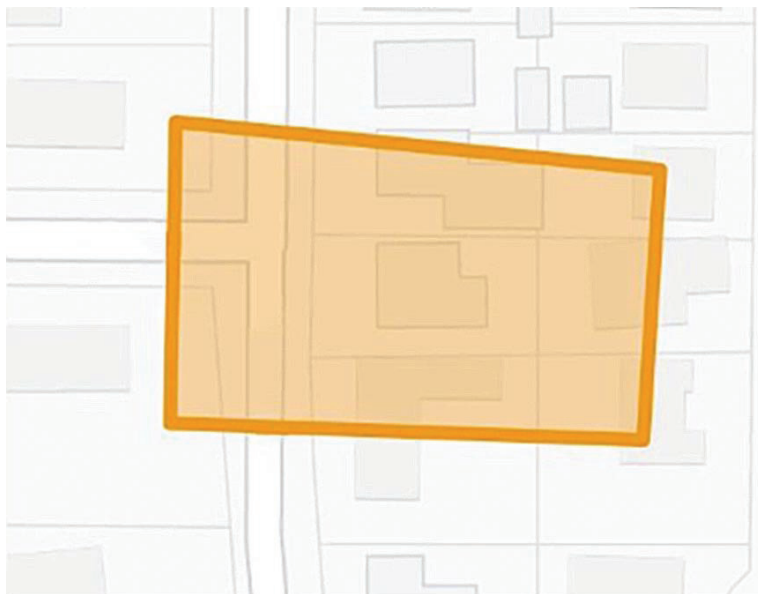


Figure 4: Texas811-generated buffer that utility/locator sees.

The size of the buffer may contribute to over-notification – that is, more utility companies being notified by the call center of a proposed dig, who then are responsible for paying the call center for the notice.

While Texas buffer size is not unreasonable,¹⁷ it does demonstrate that there is room for improvement, particularly by allowing excavators to draw their own polygons (not limited to fixed rectangular shapes) and providing the actual excavator-drawn polygon in addition to the buffer zone to

¹⁷ In fact, in other states, the buffer zone is inflated to as much as 6,700 percent in area, covering as many as 25 times the number of homes in a residential neighborhood.

utility owners and locators, which might look like a smaller grey box inside of the orange notification polygon.

The orange buffer is important for ensuring all potential facility owners in the area are notified, but the gray box is important because it shows where the digging will take place. With a more precise tool than a rectangle, this could offer excavators the ability to draw out trenches, circles for trees and shrubs, irregular shapes for pools, and many other scenarios. On larger properties, this could help narrow down the specific location of the dig rather than locators only knowing excavation work will happen at that address. The locators would then be able to pay special attention to this area and ensure they are in the correct spot by cross-referencing with material on their mobile devices.

These commonsense benefits are why the Common Ground Alliance lists electronic white-lining as its number one step in the idealized dig by 2030 and why the group believes it has among the highest return on investment for any technological best practice. PHMSA also explains that by narrowing the dig site more precisely, it helps reduce damage and “every stakeholder benefits.”¹⁸ These combined factors improve stakeholder communication from afar, reduce unnecessary site visits, save time, save money, and reduce potential for damage – single handedly tackling numerous aspects of the systemic waste and inefficiency while reducing excavation damage and their associated costs.

Systemic Adoption of Enhanced Positive Response

Following the Common Ground Alliance’s best practice recommendations, the second step of the ideal dig of the future is the use of enhanced positive response.

Every locate request submitted to Texas811 will result in a “positive response” back to the excavator. This may be a markings or documentation left at the job site, callback, fax, or an automated response system to notify the excavator that the utility company has no facilities present (clear) or that the locator has completed the marking (marked).

In Texas, not only is this basic positive response guaranteed, but the call center offers an online portal to track the status of a ticket. This *electronic positive response* gives excavators more insight during the waiting period while underground infrastructure is being marked. It displays each utility company that was notified based on the buffered polygon and gives real-time status updates once the utility company has cleared the ticket or the locators have completed their work. The needed step is to allow commonly collected enhanced information to be made available to the excavator – a more complete way to close the communication loop opened by the excavator first notifying Texas811 and known as an *enhanced positive response*.

First piloted in 2014, enhanced positive response packages the ticket, virtual manifest, digital photographs, and in some cases, facility maps together for the excavator to access in their email or through the electronic portal hosted through the call center’s website. This was demonstrated to reduce damage by as much as 67 percent.¹⁹

18 VA, PHMSA. (2007). *Virginia Pilot Project Incorporating GPS Technology to Enhance One-Call Damage Prevention Phase I – Electronic White Lining Project Report*. U. S. Department of Transportation’s Pipeline and Hazardous Materials Safety Administration and the Virginia State Corporation Commission. https://primis.phmsa.dot.gov/comm/publications/Virginia_Pilot_Project_Report_Phase_I.pdf.

19 (2014). *Enhanced Positive Response Pilot*. MISS Utility, Washington Gas, Pepco, Verizon, CertusView, UtiliQuest, Lamberts, Hinkle Construction. https://commongroundalliance.com/sites/default/files/EnhancedPositiveResponsePilot_June2014.pdf.

The benefits apply to virtually every aspect of the excavation process and resulted in findings of improved jobsite safety, damage prevention, and job efficiency. Stakeholders found it to provide valuable improvements to communication; then less than three years later, enhanced positive response emerged as the number one recommendation of the leading damage prevention safety agency, the Pipeline and Hazardous Materials Safety Administration in a report to Congress.²⁰

Texas811 is geared towards enhanced positive response with a ticket check system that displays the full ticket and even offers a tab to “add/view attachments,” but the state and its call center can lead the charge by ensuring every locator shares photographs and related enhanced information to the portal or to the excavator directly.

PHMSA summarizes not only the benefit but where to build out the systemic use of this technological best practice: “Enhanced positive response coordinated through one-call centers needs wider implementation; it can vastly improve communication among all involved in the digging process and has been shown to reduce damage rates.”²¹

NO STAND-ALONE SOLUTIONS

The solutions to this industry must be systemic because the damage prevention process is collaborative. It requires a system that all stakeholders can utilize to communicate and share information to best protect critical infrastructure and worker safety. When these are done, economic and environmental protections follow.

In Texas, the four key solutions outlined above go hand-in-hand. Most of these are already in the works in Texas but are not yet the standard. Web-entered tickets already account for around 80 percent of incoming tickets each year, but the user portal can be improved with scheduling, prioritizing, and mapping features. The excavator notice generates a buffer area that is used to notify utilities in the area, but a virtual pre-marking is not available, and the utility companies and locators do not receive the more precise rectangle drawn by excavators online. The ticket check system offers great information with the potential to maximize communication and collaboration by facilitating the sharing of enhanced information.

Together, these reforms would drive damages to unprecedented lows, potentially leading Texas to best the damage levels of much smaller states even despite its unparalleled infrastructure network and booming construction sector. These reforms build on and complement one another, each strengthening the others. This is illustrated well in Canada, where the various features fit together,

In Canada, **on-line / web locate** requests have emerged as a preferred method of requesting a locate. Any person **requesting a locate** can do so **24/7/365** and is typically **able to plot or draw** their dig site on a sketch or map reducing the risk of misinterpretation to an Agent thereby **improving the damage prevention process**.²²

Excavators placing their own requests rather than having a phone Agent interpreting the request can **reduce potential utility strikes by nearly one half**, particularly in regions that have **virtual white-lining**.²³ (all emphases added)

20 (2017). *A Study on Improving Damage Prevention Technology*. U.S. Department of Transportation Pipeline and Hazardous Materials Safety Administration. <https://www.phmsa.dot.gov/news/report-congress-improving-damage-prevention-technology>.

21 *Id.*

22 (2020). *DIRT Report 2019*. Canadian Common Ground Alliance. <https://www.canadiancga.com/resources/Documents/DIRT-Reports/DIRT%20-%202019-Eng-Final.pdf>.

23 (2022). *DIRT Report 2021*. Canadian Common Ground Alliance. <https://www.canadiancga.com/resources/Documents/DIRT-Reports/DIRT%202021-04B%20ENGLISH.pdf>.

The ability for excavators to access an online portal at any time of day or night, where they can draw a virtual pre-marking to pass along to the utility company and locators in addition to the buffer for notification that the call center generates is important. Ensuring the platform can host the enhanced information provided from excavator to locators and as an enhanced positive response from locators to excavator is the major step in reducing damage by 67 percent – and far more with the other reforms combined.

Together, these also offer unique post-damage benefits. The nature of excavation makes determining fault, liability, and root causes difficult. When the ground is disturbed, any spray paint or site markings will be disrupted, and records can be lost. The one-call center's online platform serving as a central location for communication helps safeguard against this by generating and preserving electronic records of things like pre-marking/white-lining, digital photographs of the site, and other enhanced information. If a damage does still result, even with these tools in place, the root cause can be determined more easily, and accident investigators can gain key insights. Moreover, it can help shift stakeholder incentives to provide better records, so they do not get falsely assigned liability or partake in costly litigation.

With all of these reforms in place, stakeholder behavior is likely to change for the better. Streamlining the process will help eliminate waste and inefficiency on the front end. This will likely also encourage more use of the Texas811 system by “no-call” excavators and greater use of the tools within the online portal by those providing notice. The systemic use of these technological best practices also stands to eliminate the majority of excavation damages, sparing communities from devastating harms.

The use of industry-consensus and safety agency-recommended technological best practices will protect Texas's critical infrastructure and its people. This will reduce billions of dollars in economic waste, inefficiency, and harm that drags on the state every year while boosting public safety and environmental protections.

Without these reforms, Texas may be on a path toward greater risk to its infrastructure. Its rising population and development activity alongside its uniquely high mileage of buried assets demand that damage prevention receive heightened attention and targeted reforms. These are ready to deploy today to protect the state tomorrow.

REFERENCES

For a complete listed of article reference, please see the link below to our online publication forum.

Suggested citation: Dierker, B. R. (2023) Unseen Threats to Texas Critical Infrastructure. (Report No. IHS/CR-2023-1007). The Sam Houston State University Institute for Homeland Security. <https://doi.org/10.17605/OSF.IO/UFQWZ>
One Step Ahead, April 2024, 25-36.

SUPPLY CHAIN MAPPING FOR EMERGENCY MANAGEMENT DECISION-MAKING

Mark Scott
Critical Infrastructure Consultant

Abstract

Supply chain issues are a growing concern for public sector emergency managers because communities rely on these privately-owned and operated systems to deliver goods needed for daily life and survival. Recent events have highlighted the many ways supply chains can be disrupted. Knowing how these systems are configured and how they operate is essential to making more effective operational decisions during emergencies and to support supply chain owners/operators restore flow following a disruption. Mapping the supply chain is a proven private sector practice for gaining visibility into these systems that may have application in the public sector. This paper describes why mapping helps improve emergency preparedness, how mapping has been done, and two case studies of its application for lifeline commodity supply chains in the National Capital Region. The paper concludes with a path forward for emergency managers seeking to use mapping to strengthen supply chain resilience in their communities, regardless of scale.

Keywords: supply chain; mapping; emergency managers; resilience

INTRODUCTION

Supply chains are critical to community security and resilience.

Supply chains are systems or networks that encompass the entire process of making and delivering commercial goods. They include every stage from the supply of materials and the manufacture and packaging of the goods through to their distribution and sale. Supply chains are comprised

Mark Scott's career spans over 40 years in risk management in the public, private, and nonprofit sectors. His experience includes professional engagement in critical infrastructure security and resilience, environmental and health & safety regulation, and hazardous materials risk management.

Most recently Mark managed critical infrastructure programs and initiatives for the District of Columbia's Homeland Security and Emergency Management Agency. In that role he designed and managed projects to assess the resilience of the food, water, fuel and healthcare supply chains serving the National Capital Region. Mark has also advised FEMA on supply chain resilience issues and training programs for local emergency managers, and has presented on supply chain resilience at multiple national forums.

Mark has lived and worked in the Washington D.C. area since 2008, having previously resided in Charleston, West Virginia and Pittsburgh, Pennsylvania. He holds a master's degree in urban and regional planning from the University of Pittsburgh. Mark also has served as member and past Vice-Chair of the Department of Homeland Security's State, Local, Tribal, and Territorial Government Coordinating Council.

Disclosure: The author reports there are no competing interests to declare.

of geographically dispersed and distinct private sector entities. No one business owns a supply chain, although dominant players are usually present.¹

Supply chains include systems that provide lifeline commodities – such as food, water, fuel, and healthcare supplies – that communities need for everyday life and survival. While private sector entities own and operate supply chains, the public depends on their continued operation and their ability to recover quickly if disrupted.

Supply chain disruptions are increasing

Supply chains need to be flexible enough to absorb any shocks that may disrupt system operations. Yet events in recent years have shown that supply chains can and do get disrupted, sometimes violently, and these disruptions will likely increase due to climate change impacts, geopolitical conflicts, cyberattacks, future public health emergencies, and the likelihood of compounding and cascading events.

McKinsey² has classified supply chain shocks into four different types, based on their impact, lead time, and frequency of occurrence. For public sector officials and emergency managers, these shocks can be seen as the following events:

- *Unanticipated catastrophes.* These are historically remarkable events that can't be anticipated and lead to trillions of dollars in losses. Examples include extreme terrorism, large scale pandemics, and a systemic cyberattack.
- *Foreseeable catastrophes.* Similar magnitude to an unanticipated catastrophe but differs in that larger patterns and probabilities can guide general preparedness. Examples include large scale natural hazards and geopolitical conflicts.
- *Unanticipated disruptions.* These are serious and costly events but are on a smaller scale than catastrophes. Examples include localized natural disasters, civil unrest, and industrial accidents.
- *Foreseeable disruptions.* Some disruptions can be spotted in advance of their arrival. Examples include transportation labor disputes and global shortages of essential commodities.

There is a growing awareness of the need for supply chain visibility

Before a community can identify risks to these critical systems, it needs to understand what the supply chain looks like and how it works. Since the Covid-19 pandemic, there has been increasing attention by policy makers, regulators, industry bodies and governments to how contemporary supply chains are configured, operated, and controlled. Along with this has come heightened interest in active surveillance of supply chains as they operate in real time. These interests require accurate information-based maps to facilitate risk analysis, monitoring, surveillance, and early detection of supply problems. Supply chain mapping is the key to gaining this visibility into the system.

Who the paper is directed to, and why it matters

This paper is written from a public sector perspective for officials and emergency managers working at the state, regional tribal, and local levels. These leaders share a common mission of protect-

1 MacCarthy, Bat L., Wafaa A.H. Ahmed, and Guven Demirel. "Mapping the supply chain: Why, what, and how?", *International Journal of Production Economics*, Volume 250, August 2022, 108688. <https://doi.org/10.1016/j.ijpe.2022.108688>

2 McKinsey. "What is supply chain?" <https://www.mckinsey.com/featured-insights/mckinsey-explainers/what-is-supply-chain?cid=other-eml-onp-mip-mck&hlkid=7e01943f8c914cbd829fcac2d4f31d28&hctky=12203888&hdpid=8f9d71d3-7318-471b-93b2-7e073406d67a>

ing public health and safety, and one key to mission success is ensuring availability of commodities essential for daily life and survival. Recognizing and mitigating vulnerabilities that can lead to supply disruption is essential for community protection and resilience.

The paper identifies opportunities for building stronger public-private partnerships and adapting business mapping practices where appropriate. Private sector owners/operators can also benefit by gaining awareness of how emergency managers may pursue mapping to support the shared mission of supply chain resilience.

What this paper will discuss:

- How mapping provides visibility into the supply chain
- How mapping can be used to strengthen community preparedness
- Challenges and limitations to mapping
- Examples of how mapping has been used
- Lessons learned from the private sector that may have value for public sector managers
- A recommended way forward for the emergency management community

MAPPING PROVIDES VISIBILITY INTO SUPPLY CHAINS

Supply chain mapping is part of the larger process of supply chain risk management. The purpose of mapping is to gain a comprehensive view of the entire supply chain, including all the key supply and demand components and their linkages. This visibility provides insights into where the supply chain is most vulnerable, and that helps target investments and other actions that will have the biggest impact in improving resilience.

From a network science perspective, supply chains are primarily made up of **supply nodes** (where commodities originate), **demand nodes** (where consumers go to get those commodities) and **supply-demand links** (how commodities get from supply nodes to demand nodes). For emergency managers, getting visibility into supply chain operations can be most effectively done by examining these components within the three major dimensions of the system: upstream, midstream, and downstream.

When creating a supply chain map, several elements are typically considered:

1. Suppliers: sources of raw materials, components, or services that are essential for the production process.
2. Processors: facilities or entities responsible for transforming raw materials into finished goods.
3. Distribution Centers/Warehouses: locations where inventory is stored, managed, and distributed within the supply chain.
4. Transportation: routes and modes used to move goods between different locations, including shipping, road transportation, airfreight, etc.
5. Retailers/Distributors: entities responsible for distributing and selling the finished products to the end consumers.
6. Consumers: the end consumers and their demand patterns, which helps in aligning the supply chain to meet customer requirements effectively.

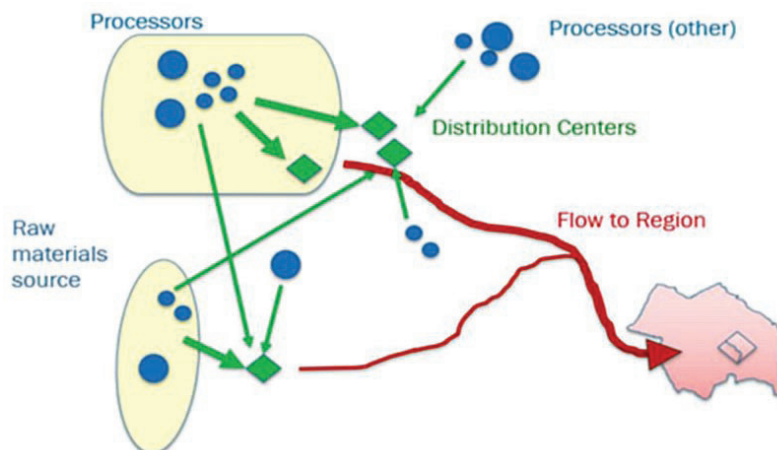


Figure 1: Generic depiction of supply chain mapping

Mapping is particularly useful in documenting the factors that help determine the overall resilience of the system:

- *Geographic distance between supply and demand* – In terms of supply chain performance, shorter paths ensure lower cost and product delivery time and facilitate the delivery of commodities from supply to demand nodes along the network.³ For system resilience, shorter distances between supply and demand nodes reduces exposure to hazards that can disrupt the flow of goods.
- *Relative diversity of supply nodes, demand nodes, and routing options* – System resilience is also influenced by the relative diversity of suppliers, shipping options, and locations for consumers to receive goods. Increasing the diversity of supply locally has been shown to increase a community’s resistance to supply chain shocks.⁴
- *Concentration of production, processing, and distribution capabilities* – It is common for a large percentage of key goods and services serving a densely populated area to depend on small number of distribution centers. These concentrations are fundamental to efficiency, cost-savings, and timely fulfillment of demand. But they can also become chokepoints that seriously complicate and impede flows during extended disruption or destruction of the system.⁵

Since no map can include everything, supply chain mapping requires making choices, and the map’s content will depend on what is being analyzed and what data is available. Given the constantly evolving nature of supply chains and the extensive reach of upstream suppliers, it is most

3 For an in-depth examination of resilience factors, see Sahmueler, Till and Bernd Hellingrath. *Measuring the Resilience of Supply Chain Networks*. Proceedings of the 19th ISCRAM Conference – Tarbes, France May 2022. http://idl.iscrum.org/files/tillsahmueler/2022/2399_TillSahmueler+BerndHellingrath2022.pdf

4 Supply chain diversity provides adaptive options for a city to exploit when some of its supply chains suffer shock, thus boosting resilience to shock. For example, research has demonstrated that cities with a greater diversity of food suppliers have a lower probability of suffering a food supply shock for any reason. Boosting a city’s food supply chain diversity increases the resistance of a city to food shocks of mild to moderate severity by up to 15 percent. (Michael Gomez, Alfonso Mejia, Benjamin L. Ruddell & Richard R. Rushforth (October 2020). *Supply chain diversity buffers cities against food shocks*. <https://doi.org/10.1038/s41586-021-03621-0>)

5 Palin, Philip J. Seven Steps to Counter Catastrophe. *Supply Chain Quarterly*, February 22, 2020. <https://www.supplychainquarterly.com/articles/3152-seven-steps-to-counter-catastrophe>

practical for emergency managers to acknowledge upstream suppliers but to focus their attention on the midstream and downstream components of the system.

It is also not reasonable or necessary to identify all nodes within a supply chain; the sheer size of many supply chains and the limited visibility into deeper sub-tier supply network structures present significant challenges in capturing the essential data for mapping. Emergency managers should instead focus on identifying first-tier suppliers that serve a large proportion of demand, including points of concentration of supply.⁶

Here are steps that public sector managers can take to conduct supply chain mapping⁷:

- *Identify the primary crucial suppliers for the local community.* This information may be obtained through online searches, local community knowledge, and local and regional economic reports. Strategic plans, emergency operations plans, and other guidance documents may also help identify previously identified supply locations.
- *Identify supply chain nodes within the scope of the review.* Supply chains serving urban areas extend into adjacent jurisdictions and regions, and are increasing global. Defining a manageable geographic boundary simplifies the mapping process and keeps the focus on those areas most likely to be influenced by emergency management actions. Boundaries to consider may include a state, a region, and/or focusing mainly on “last mile” delivery.
- *Identify the ultimate destinations of goods.* Each lifeline commodity will have its own distinct locations where end users acquire what they need. Knowing locations of destination sites and their characteristics improves understanding of demand patterns and helps set response priorities during a disaster.
- *Identify the infrastructure systems that provide critical support to supply chain operations.* Emergency managers should identify the infrastructure dependencies of key nodes, along with their physical locations. Electric power, petroleum fuel, natural gas, water and wastewater, and communications are among the most critical infrastructure services needed to maintain and sustain supply chain operations.
- *Overlay key threats and hazards, and other stressors and disruptors, against the identified primary system nodes and links.* Hazard Mitigation Plans can help identify threats and hazards that may interrupt the flow of lifeline commodities. Flood inundation maps and evacuation routes overlaid on a supply chain map will highlight system components in high hazard areas or otherwise prone to disruption.
- *Create supply chain maps in a geographic information system (GIS) or with specialized supply chain risk management software.* This allows spatial depiction of important upstream, midstream, and downstream components and the overall flow of lifeline commodities, providing both situational awareness and a platform for evaluating alternate disruption scenarios.

6 FEMA suggests that because the goal of mapping is to develop a strategic understanding of the local/regional demand and supply network in order to identify key supply chain players with whom to engage, a detailed and comprehensive understanding of the global supply chain is not necessary. See Federal Emergency Management Agency (FEMA). *Supply Chain Resilience Guide*. April 2019. <https://www.fema.gov/sites/default/files/2020-07/supply-chain-resilience-guide.pdf>

7 These steps are more fully explained in the FEMA *Supply Chain Resilience Guide* cited above.

MAPPING ENHANCES COMMUNITY PREPAREDNESS

Emergency management organizations that focus on understanding their lifeline commodity supply chains are better positioned to sense oncoming disruptions, visualize and analyze the impacts, run simulations that allow them to see a full range of options, and act based on the best available alternatives. Specifically, mapping allows emergency officials to:

- **Assess supply chain risks:** Mapping helps assess risks and overall system resilience by revealing locations of suppliers, distribution centers, transportation routes, points of distribution to consumers, and the interactions between them. This allows officials to understand the diversity and concentration of suppliers, determine if key facilities are in high hazard areas, and identify transportation chokepoints and other system vulnerabilities that could limit the flow of commodities during an emergency.
- **Strengthen preparedness:** Knowing the various components and dependencies within their supply network helps identify critical resources, design mitigation strategies, and develop or refine emergency response and recovery plans. This could include stockpiling essential resources; establishing mutual aid agreements with neighboring jurisdictions or private sector partners; and targeting mitigation funding to reduce hazards that could disrupt supply chain operations and to shore up critical infrastructure (such as transportation assets) that are essential to continued operation supply chain operation. Identifying supply diversity helps guide actions to increase that diversity, which will increase resilience.
- **Improve timely response to emergencies:** Having a mapped supply chain lets emergency managers quickly identify sources of supplies to meet immediate community needs and determine the most critical routes for their delivery. The information also helps pre-position response resources along key transportation routes; guides debris removal; and facilitates private sector access and re-entry to restore flow of goods. These actions can significantly speed up response times and ensure that lifeline commodities continue to be available with minimal interruption.
- **Enhance engagement with private sector owners/operators:** Supply chains involve multiple private sector organizations including suppliers, distributors, and logistics providers. Mapping identifies the primary stakeholders that support the supply chain, so officials can work with them during steady state to understand their operations and how best to coordinate and share information during emergencies.
- **Promote inter-jurisdictional coordination:** By their nature, supply chains extend beyond jurisdictional boundaries to areas outside the jurisdiction's control or influence. This creates dependencies because maintaining vital transportation routes is often the responsibility of other local or state governments. Multiple jurisdictions may also rely on the same commodity distribution centers, potentially creating shared shortages during a disaster or catastrophic event. Knowing these dependencies helps determine how to better coordinate preparedness and response and share information during disruptive events.

CHALLENGES AND LIMITATIONS OF MAPPING

While supply chain visibility is an increasingly important focus for emergency managers, mapping a supply chain from the public sector perspective presents several challenges:

- **Lack of data:** Good quality data is crucial to create a true picture of system operations. Comprehensive data about every link in the supply chain will often be incomplete, outdated, or unavailable. Inaccurate information can lead to misleading conclusions and

flawed decision-making. Maintaining data accuracy requires ongoing monitoring and verification.

- *Subjectivity and scope:* Mapping involves making choices about what information to include and how to represent it. For emergency managers, resource availability and bandwidth limitations makes it difficult to gain visibility into upstream components of more complex supply chains. In particular, lack of visibility beyond first-tier suppliers increases the risk of overlooking potential vulnerabilities, since supply chain disruptions may originate with a supplier's supplier, or even further up the supplier chain.
- *Dynamic nature of supply chains:* Supply chains are dynamic systems that change over time. New suppliers, technologies, market conditions, or adaptations made following a disruption can alter the existing supply chain structure, such that mapping the system at a particular point in time will not fully capture its evolving nature. Mapping needs to be regularly updated and adjusted to reflect changes in suppliers, processes, locations, and risks.
- *Reluctance to share information:* Supply chains are made up of multiple private sector entities that together support system operations, and data from them is crucial for successful mapping. However, some may be hesitant to disclose detailed information about their operations due to concerns about revealing sensitive or proprietary information, concerns about competition, or lack of trust in government.

RECENT APPLICATIONS OF MAPPING

Supply chain mapping has been undertaken in recent years within several large urban areas across the United States to highlight supply chain vulnerabilities, inform operational decision-making during emergencies, and identify resilience enhancement options. The following are recent examples:

Case studies from the Washington DC area

Case study #1: Food supply for National Capital Region (NCR) communities⁸

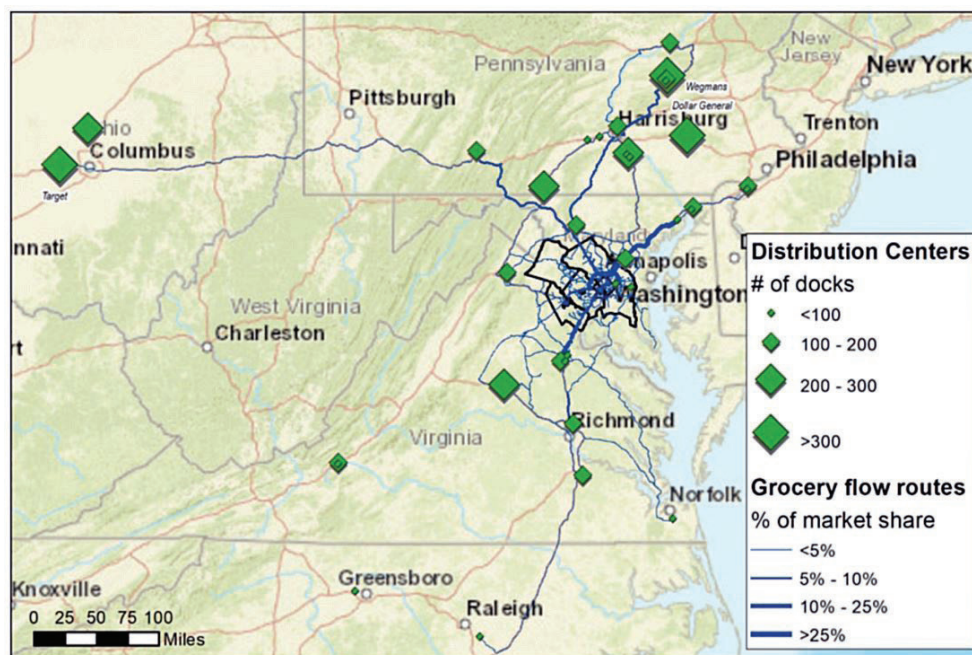
Purpose: Characterize the food supply chain serving the NCR during steady state; identify what shocks could disrupt that supply chain; assess the potential impact of such events on supply chain operations and the affected communities; and identify opportunities to strengthen local and regional capability to prepare for, respond to, and recover from a food supply chain disruption.

Methodology: The foundational step for improving the region's capability for a food disruption was mapping the food supply chain to gain visibility into the various components of the system and understand how the factors of distance, diversity, and concentration affected the relative reliance of the system to a disruption. Mapping of **upstream** components of the system was done using data from the FHWA Freight Analysis Framework to show agricultural commodity flow from around the country into the NCR, and from various USDA databases to show agricultural production and food processing serving the region. For **midstream** components, USDA data and a variety of business databases were used to identify wholesaler locations, locate distribution centers for major grocery providers, and determine relative market share of these providers. This data was overlaid on mapping of regional freight routes identified by Metropolitan Washington Council of Governments (MWCOG), and used to model flow of groceries from distribution centers to retail locations using routing (by least trucking time) as shown below, in order to determine which routes carry the most flow. Mapping of the **downstream** components used multiple databases from USDA, local govern-

8 This project was conducted by the District of Columbia Homeland Security and Emergency Management, with data collected and analyzed by CNA Corporation. Funding was provided by the FEMA Regional Catastrophic Preparedness Grant Program.

ment, and food assistance organizations to characterize the relative importance of food for home use and food consumed away from home.

The following map shows distribution center locations and flow routes for the major grocery providers based on percentage of market share:



Application of study findings: The mapping done through this project has already proved beneficial to regional emergency preparedness:

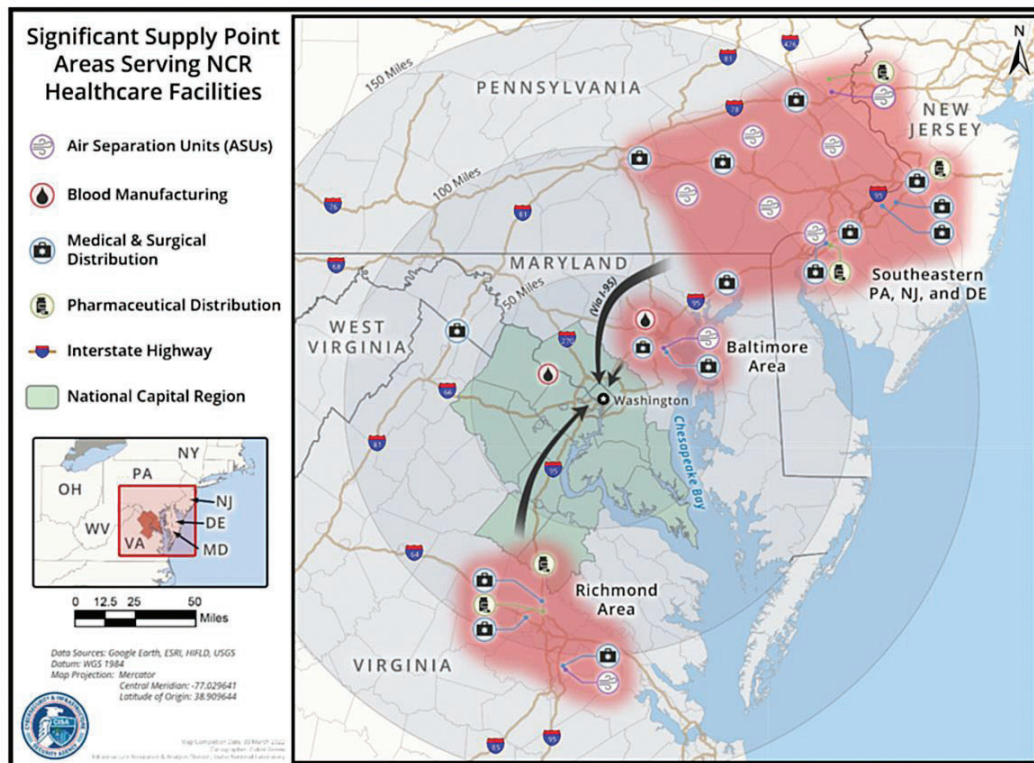
- In January 2022 two major snowstorms passed through the Mid-Atlantic region, including parts of eastern Pennsylvania where mapping showed several food distribution centers supplying the NCR. The severity of the first storm led the Commonwealth of Pennsylvania to close roadways in affected parts of the state to commercial traffic for 24 hours, halting shipments from these centers and resulting in short-term shortages of food on grocery store shelves in the NCR. In advance of a second storm two weeks later, the District of Columbia's emergency management agency overlaid National Weather Service snowfall projections on the agency's food supply chain map and determined that additional impacts to the eastern PA food distribution centers could be expected. This information was shared with NCR emergency managers to help them better prepare for potential disruptions of food supplies for their communities. It also led to improved information-sharing between HSEMA and the Pennsylvania Emergency Management Agency for future events.
- During the March 2022 trucker convoy protest in the Washington DC area, information showing commodity flows over important freight routes was shared with local emergency managers across the NCR. In addition to providing situational awareness, this informed the deployment of local law enforcement and Department of Transportation assets to important locations across the freight network to minimize disruption of the flow of food and other essential commodities using these routes. The potential for disruption from this action also facilitated greater sharing of threat information between emergency managers and the region's major grocery providers for this and future events.

- Results of this mapping showed that Washington, DC, Baltimore MD, and Philadelphia PA share many of the same major commercial food providers. This has led to creation of a Mid-Atlantic Coordination Group to coordinate efforts between jurisdictions and the grocery industry in preparation for future emergency events with regional impact.

Case Study #2: Medical supplies for National Capital Region (NCR) healthcare facilities⁹

Purpose: Identify and map the key suppliers of critical commodities for healthcare facilities in the NCR; identify critical infrastructure dependencies for those facilities; and develop options for enhancing the resilience of the supply chains and infrastructure services.

Methodology: The three Health & Medical Coalitions operating in the NCR identified four essential commodities of concern: blood products, medical gases, medical and surgical equipment, and pharmaceuticals. Using key vendor analyses conducted by the three Coalitions, the project team developed an initial list of these product suppliers and then interviewed hospitals and other healthcare facilities in the region to identify their specific vendors, commodity management practices, and supply vulnerabilities. The team also conducted in-depth interviews with suppliers in each of the four categories to identify their supply management and delivery practices. Mapping of the supplier distribution centers serving the region was conducted as shown below, and resilience enhancement options developed for consideration by the three coalitions and the Council of Governments. A stakeholder workshop was used to share study findings and discuss how healthcare facilities and suppliers can better coordinate efforts during a disaster or catastrophic event in the region.



Application of Findings: Study results were briefed to each Coalition and the regional RESF-8 Healthcare Committee for integration of findings and resilience enhancement options into their

⁹ This project was conducted by the District of Columbia's Homeland Security and Emergency Management Agency and Department of Health, through the Department of Homeland Security/Cybersecurity and Infrastructure Security Agency's Regional Resilience Assessment Program (RRAP)

work plans. Findings from the mapping of facilities supported situational awareness for regional emergency managers and healthcare facilities following two recent events: (1) a snowstorm in January 2022 that closed the major freight transportation route from Richmond VA to Washington DC for over 24 hours, and (2) a tornado in July 2023 that severely damaged a North Carolina pharmaceutical manufacturing facility that provides products to the NCR and several other regions.

Supply Chain Mapping in Texas City of Houston/Harris County

Houston and Harris County have pioneered several public-private engagement processes to coordinate with key critical infrastructure owners/operators across the city, county, and region.¹⁰ This has included in-depth mapping of the region's fuel supply chain to identify potential chokepoints in the system and better prepare for impacts from future tropical storms, and maintaining regular dialogue between local government officials and supply chain partners.

Texas Electricity Map

In 2023 the Texas Electricity Supply Chain Security and Mapping Committee adopted an Electricity Supply Chain Map of critical infrastructure for use during disaster and emergency preparedness and response. The map identifies critical infrastructure facilities that make up the state's electricity supply chain, including electric generation plants and the natural gas facilities that supply fuel to power the plants. It is expected that state emergency management officials will use the map during weather emergencies and disasters to pinpoint the location of critical electric and natural gas facilities and maintain contact with those key facilities. The map is scheduled to be updated twice a year, or more often if necessary.¹¹

Texas Private Sector Advisory Council

In January 2023 the SHSU Institute for Homeland Security submitted recommendations¹² to the Texas Private Sector Advisory Council on legislation and policy measures for building resilience into critical supply chain infrastructures in the state. The recommendations included encouraging organizations to map their supply chains to identify both first tier (direct suppliers/service providers) and second tier (supplier's suppliers) vendors. The objective is to identify the stakeholders, understand the different relationships, timings, and costs, and classify the different supply chain risks that exist. In addition, the map process should provide insight into the strengths and weaknesses of supply chain partners.

Supply Chain Mapping by FEMA

The Federal Emergency Management Agency has proactively addressed supply chain resilience through mapping:

- For several areas of the U.S. prone to catastrophic events, mapping has been used to assess potential impacts and response options, including (1) a proof-of-concept project in 2020 for supply chain resilience in the Puget Sound region, which explored strategies and techniques for facilitating supply chain response and recovery following a catastrophic earthquake; (2) an assessment of emergent supply chain issues in Florida

10 <https://cities-today.com/supply-chain-proves-central-to-houstons-resilience-efforts/>

11 Railroad Commission of Texas. Texas Adopts First-Ever Electricity Supply Chain Map. April 29, 2022. <https://www.rrc.texas.gov/news/042922-joint-rrc-puc-map/>

12 SHSU Institute for Homeland Security. *Building Resilience into Critical Supply Chain Infrastructures*. January 31, 2023. Contact the Institute regarding report availability.

associated with Tropical Storm Ian in 2022; and (3) as a component of the National Strategic Supply Chain Risk Analysis for the 2023 hurricane season.

- FEMA's Supply Chain Analysis Network (SCAN) Team has used mapping to help establish baselines for private sector supply chains of lifeline commodities. These baselines serve as a supply chain intelligence assessment that seeks to define “normal” conditions in order to assess post disaster supply chain questions conditions and determine appropriate federal courses of action.
- FEMA's Technical Assistance Program has also trained multiple jurisdictions across the U.S. on supply chain mapping techniques and application.

Lessons from the Private Sector

Since at least the 1980s, mapping has been an essential strategy for businesses looking to increase their supply chain performance.¹³ Recent research shows that companies with more visibility across their supply chains perform better during periods of disruption. For example, a small minority of companies that invested in mapping their supply networks before the Covid-19 pandemic emerged from that event better prepared to manage disruptions because they had more complete understanding of their supply chains.¹⁴

Many supply chain owners/operators use a combination of structural and dynamic visibility to orchestrate their supply chains for greater efficiency. **Structural visibility** is about knowing what the supply chain looks like. It provides a snapshot of operations at a point in time and helps uncover hidden issues, and includes traditional activities like network mapping, risk assessment, network assessments, and modelling. **Dynamic visibility** is knowing what's happening across the supply chain in real time, enabling a company to monitor and respond to events quickly.¹⁵

For future emergency events, having structural and dynamic visibility means that instead of scrambling at the last minute, supply chain managers have a lot of information to make key operational decisions within minutes of a potential disruption. They know which suppliers, sites, parts, and products are at risk, which allows them to put themselves first in line to secure constrained inventory and capacity at alternate sites.

More recently, private sector supply chain managers have begun leveraging advanced technologies to enhance operational efficiency and decision-making, including increasing visibility through mapping. Artificial intelligence (AI) is playing an increasingly important role in enabling the rapid collection, updating, and integration of data that can be used to automate mapping and allow visualization of supply networks in almost real time. AI-based tools such as digital twins and control towers support the risk prediction and assessment, real-time monitoring, natural disaster and weather analysis, and scenario planning and simulation needed to enhance supply chain performance.¹⁶

Understanding how businesses conduct mapping and deploy advanced technologies to enhance supply chain efficiency may help public sector managers see opportunities to adapt similar technology and data-driven approaches into their emergency management processes. Potential use cases include enhanced risk prediction, real-time monitoring, demand forecasting, supplier risk

13 Muhammad Shujaat Mubarak, Simonov Kusi-Sarpong, Kannan Govindan, Sharfuddin Ahmed Khan & Adegboyega Oyedijo (2023) “Supply chain mapping: a proposed construct”, *International Journal of Production Research*, 61:8, 2653-2669, DOI: 10.1080/00207543.2021.1944390

14 Ibid.

15 <https://www.accenture.com/us-en/blogs/high-tech/how-visibility-boosts-supply-chain-resilience>

16 Ibid.

evaluation, natural disaster analysis, predictive maintenance, scenario planning, and automated decision-making.

While the mission-drivers and resources available are significantly different for the private and public sectors, many of the proven practices of supply chain owners/operators may have value for public sector application. By studying and adapting these practices where appropriate, officials can enhance their preparedness, response, and recovery capabilities, leading to more effective emergency management outcomes.

A WAY FORWARD

Here are three near-term actions public sector officials and emergency managers can take using supply chain visibility to strengthen community resilience:

1. Cities and regions should prioritize mapping the supply chains for their lifeline commodities.

This step begins by identifying the commodities of greatest importance, and seeking out existing data sources and partners to assemble the information necessary to map out each supply chain in accordance with local needs and conditions. Where possible, mapping should include both structural visibility (how the system is now) and dynamic visibility (how the system operates in real time). This step is critical because it will show where the supply chain is most vulnerable, and where actions can be taken to reduce that vulnerability. Once completed, the maps should be made an integral part of the jurisdiction's preparedness framework.

2. Emergency managers should build meaningful partnerships with private sector actors who make up and support the supply chain, and with neighboring jurisdictions who share components of the supply chain.

Following a supply chain disruption, the role of the impacted businesses is to restore flow, while government's role is to do all it can to facilitate that restoration. This requires mutually beneficial and sustained relationships established during steady state, so that disaster response is coordinated and effective. During and after mapping, emergency managers should work toward generating as many touch points with suppliers as possible, and with key infrastructure service providers who support the system. Since the mapping exercise will also identify the supply chain's reach into other jurisdictions and regions, managers can use that information to build or strengthen information sharing and operational coordination with those government entities who share the supply chain.

Artificial Intelligence Tools Supporting Supply Chain Mapping

Digital twin is a virtual replica of a supply chain. A digital twin replicating the typical behavior of the supply chain can be used to simulate and scenario model the supply chain's performance. It allows managers to understand where suppliers and points of production are, what logistics routes are used for which products and customers, and the relationships across the supply chain network.

Supply chain control tower is a cloud-based solution that leverages advanced technologies – such as artificial intelligence (AI), machine learning, and the Internet of Things (IoT) – to proactively manage supply chains. It provides a connected, customized dashboard of data, key business metrics and events across the supply chain, and enables organizations to understand, prioritize and resolve critical issues in real time more fully.

Source: Accenture; SAP

3. Mapping should be used to conduct stress tests (exercises) with private sector participation around potential supply chain disruption scenarios.

Mapping results can best be operationalized by testing how well the jurisdiction can deal with an emergency event that disrupts the availability of one or more of the lifeline commodities. These scenarios should incorporate the findings from mapping results into an existing training and exercise program that evaluates existing plans and capabilities. Involvement of private sector owners/operators in these activities will be essential to success. Beyond identifying strengths and areas for improvement, conducting these “stress tests” will help build trust and strengthen relationships with key private sector partners.

REFERENCES

For a complete listed of article reference, please see the link below to our online publication forum.

Suggested citation: Scott, M. (2023) Supply Chain Mapping for Emergency Management Decision-Making. (Report No. IHS/CR-2023-1027). The Sam Houston State University Institute for Homeland Security. <https://doi.org/10.17605/OSF.IO/T34EP>
One Step Ahead, April 2024, 37-49.

RESILIENCE TO HIGH CONSEQUENCE CASCADING FAILURES OF CRITICAL INFRASTRUCTURE NETWORKS

Arthur Mouco
Benjamin L. Ruddell
Susan Ginsburg
Criticality Sciences

Abstract

Critical infrastructure networks such as telecommunications, power, water, natural gas, diesel, transportation, and cyber networks are interdependent with one another, forming a vast and dauntingly complex web of institutions and physical systems that must be engineered and secured for reliability. No single utility operator, engineering consultant, emergency management organization, financial institution, or local, regional or other government entity is capable of understanding, monitoring, or managing the whole system. Yet, failures are unavoidable, and when those failures cascade through the network the result may be high-consequence cascading “catastrophes” or Black Swan events. In one recent and tragic example, the February 13–17, 2021 Winter Storm Uri in Texas initiated a failure in the natural gas production system that cascaded first to the natural gas power generation system and then to the wider ERCOT power system, the water distribution system, and the petrochemical industry of Texas. No single system operator was responsible, and yet the consequences – including fatalities, recovery challenges, regulatory attention, and extreme costs – are everyone’s problem. As networked interdependencies grow, the likelihood of cascading failures has increased accordingly, necessitating technical solutions tailored to this problem. This report introduces the basic principles of interdependent critical infrastructure networks and reviews approaches for analyzing and mitigating the vulnerability of the network to make it resilient. Resilience and reliability in critical infrastructures are complementary and orthogonal. In resilient networks, the inevitable failures due to “all hazards” stay small and don’t become catastrophes.

THE RESILIENCE CHALLENGE

Resilience can be defined as the ability of a system to absorb, cope, and restore from a disturbance, as well as adapt itself, learning from past disturbances [1]. Moreover, resilience can be associated with the capacity of a system to resist and recover from the impacts of all kinds of failure events, including low probability, high consequence (LPHC) events that often dominate total system risk. LPHC events are the “black swan” events – catastrophic scale events that were not forecast or prepared for in advance of them happening and are considered impossible to predict: the Northeast Blackout, the Fukushima nuclear disaster, and Winter Storm Uri are notorious examples.

LPHC events on engineered network systems, such as power, telecommunication, water, gas, and cyber networks are usually associated with cascading failures. A cascade failure happens when a

failure on one or a few parts of the system spreads to other parts, progressively spreading to the system or multiple systems with extreme consequences. This may happen within a single utility – the Colonial Pipeline failure is an example – and it may also happen across sectors. Critical infrastructure systems that keep cities alive and allow populations to thrive are interdependent, as illustrated in Figure 1 – Interdependent Critical Infrastructure Networks in a City.. Gas delivery, power delivery, communication services, and water delivery are all examples of infrastructures that can, while interrupted during a failure, spread failures on other critical infrastructures and significantly impact society. LPHC events are likely to cause cascading failures and, ultimately, long-term interruption of services with severe consequences to the population and economy, as well as the utility itself. In financial terms, the consequences are both direct (money lost for service not supplied) and indirect (community impacts, legal liability, fines, and reputational damage). Therefore, the practical challenge of resilience for engineers is to keep failures small, and with their emergency management partners, also to recover quickly.



Figure 1 – Interdependent Critical Infrastructure Networks in a City.

Because critical infrastructures are not independent and cannot function alone for an extended period, systems interdependencies in critical infrastructure must be considered when analyzing resilience [2]. The impacts of the Uri storm in Texas in 2021 provide a real example of the effects of failures in interdependent critical infrastructure systems. In that event, failures propagated between power, gas, and water systems generated a death toll of 151 and severe economic consequences, to the order of U\$ 155 billion, as shown in [3] and [4]. Systems interdependencies can propagate cascade failures and must be evaluated, as shown in Figure 2 - System Interdependencies.

Why is interdependent network resilience analysis not a standard feature of reliability engineering and regulatory policy today? Three reasons stand out. One reason is that operations engineering tends to utilize single-sector physically-based models for design and optimization, but physically-based models of multi-sector interdependent infrastructure systems remain in their infancy. Such models are fundamentally challenging and costly to construct and to validate due to the variety and scale of the physics, institutions, regulations, and data sources involved, and also the high computational cost associated with them.

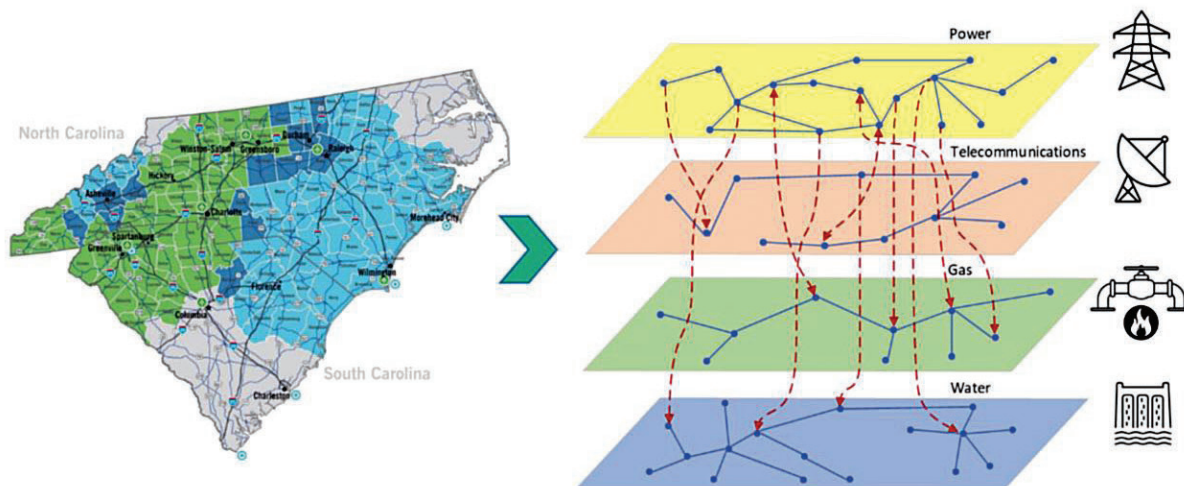


Figure 2 - System Interdependencies

A second reason is that network fragilities stemming from network interdependencies tend to be hidden from any single sector's systems operators, and also to regulatory agencies that focus on one sector of critical infrastructure. Critical infrastructure operations tend to be much better prepared to mitigate vulnerabilities within their own sector and systems operations than they are to absorb vulnerabilities originating from interdependent networked systems. However, what you can't see can hurt you, because failures in other networked systems can easily cascade to create major failures in your system.

A third reason why resilience remains an unsolved problem is that current methods of failure and risk analysis focus more on reliability than resilience (even when the word "resilience" is thrown around). Built into engineering reliability analysis, failure analysis generally considers risk as the possibility of a failure event occurring multiplied by the consequence of that event. Risk can be calculated as a function of different consequences – such as loss of lives, financial, societal, and reputational – and the probability of a failure event happening [5]. The standard methods to mitigate risks are to define the likelihood and consequences of threats and failures in the system using historically observed threat and failure data. These historically experienced risks are then built into engineering models to simulate failure risk. Those simulations, used extensively in critical infrastructure management and constituting the backbone of engineering reliability analysis, require accurate and detailed physics-based network models along with accurate characterization of the probability of the threats facing the system.

This type of failure analysis works well for reliability in the face of routine threats but works poorly for resilience to rare, unpredictable, and catastrophic threats- and also works poorly for cascading failures once they obey a different set of risk principles and physics. Reliability is, by definition, the ability to be trustworthy or perform consistently well. Reliability is generally accepted as the characteristic of an asset expressed by the probability that it will perform a required function under stated conditions for a stated period [5]. Investing in reliability to prevent failures caused by routine threats does not guarantee resilience during LPHC events. As an illustration, Figure 3 – New York City, 2003 Northeast Blackout (Frank Franklin II/Associated Press) presents a photograph of Manhattan, New York during the 2003 Northeast Blackout that affected 55 million people in eight US states and parts of Canada, with electric power being lost for anywhere from a few hours to several days. This LPHC event started with a single software bug in the alarm system that prevented operators from quickly becoming aware of an overload on a high-voltage transmission line and, following human error, a manageable problem developed into a large-scale blackout [6].



Figure 3 – New York City, 2003 Northeast Blackout (Frank Franklin II/Associated Press)

Black Swan events with their uncertainty and extreme features are more common than we expect, and they seem to have become more frequent in the 21st century. Climate factors are associated with some of the most notable events affecting critical infrastructure in recent decades. The consequences of extreme weather events, such as hurricanes, storms, and floods, are increasing in severity, leading to community and ecological challenges in every region of the United States [7]. It may be that globalized and interdependent networks along with climate change have made Black Swans more common, or it may be that we are only now beginning to appreciate their prevalence as we collect systematic failure data for the first time in human history. Regardless, they cause extreme damage to critical infrastructure, resulting in loss of life, generating severe social impacts, extreme financial burdens, legal liability, national security compromises, and reputational damage. For all these reasons, it has become paramount to adopt a methodology to increase critical infrastructure systems resilience, identify critical assets associated with such failures and mitigate those risks so that failures due to unforeseen disruptions are kept small and recovery can be rapid.

A final important contributing factor to the resilience challenge is the primary focus in recent decades on increasing efficiency within individual systems. It has become clear that maximizing efficiency under routine operating conditions can decrease the system's resilience to unexpected high-consequence events [8]. This factor creates an unfortunate "race to the bottom" or "tragedy of the commons" in an unregulated competitive marketplace where less resilient operations out-compete more resilient operations on short term cost and price. Resilience is therefore a regulatory challenge, in addition to a technical problem.

The power transmission system fully reflects the gap in resilience considerations. The power system is an essential infrastructure for the operation of fundamental societal functions. All other critical infrastructures depend on continuous electrical energy availability [1, 2], making the power grid among the "most critical" of infrastructures. The push for efficiency was translated into new methodologies to operate the system close to its capacity. Investments in system asset expansion are being postponed in exchange for additional monitoring and more flexible procedures, relying

on state-of-the-art simulations using digital twins and pre-defined reliability criteria. Those new procedures allowed flexibility in real-time operation limits. However, this means that there is less margin for error, whether traceable to humans or models, a combination of both, or to other factors. More importantly, the system is less robust to respond to unpredicted failures and prone to cascade failures caused by black swans.

Engineering models to prevent failure in power systems center on achieving reliability. They do so by simulating the loss of any single asset on the system at a time representing failures of known intensity, duration, and frequency. This reliability methodology is well established for power systems planning and real-time operation, commonly cited as the “N-1” criteria. N-1 is sometimes extended to N-k when expanded to combinations of failures. Power systems reliability is also expressed in two terms: adequacy and security. Adequacy is the balance between generation and load, and security is the ability of the system to respond to disturbances and transients. Those disturbances, usually frequent and associated with single asset failure, have relatively good statistical predictability. The standard measures to increase reliability mainly focus on preventing component failure by hardening assets against known hazards and preventive maintenance. From the financial perspective, reliability methodology leads to a cost/benefit analysis to address known types of events that can lead to expected revenue losses, planned recovery and new prevention requirements.

Unlike frequent or at least relatively predictable events with consequences that can be anticipated, LPHC events on the power grid are usually associated with extreme weather, such as hurricanes, ice storms and floods, and increasingly forest fires. They can also be initiated by cascading failures from other infrastructure systems, accidents, physical attacks by insiders, domestic attackers, or external adversaries, cyber-attacks, electromagnetic pulses, or failures in multiple internal computing and control networks. Those so-called black swans in power systems have low-frequency occurrence (e.g. years to decades), extremely low predictability, and present extreme costs and burdens to utilities and society [9, 10]. As discussed, LPHC events present elevated risks of loss of life, legal liability (insured and non-insured), and extended asset damage for the utilities that may lead to bankruptcy. A critical aspect of power grid resilience is the capacity to restore service quickly after LPHC events. There is reason to believe that LPHC events drive total risk and cost in critical infrastructure systems, and that building resilience to LPHC events simultaneously enhances resilience to routine failures.

Resilience to rare and severe events is the weak point in the predominant power engineering reliability paradigm. Despite all developments in technology, protection systems, availability of accurate models, and processing power for reliability and resilience simulation analysis, the frequency of power outages in the US has been increasing in the last decades. As shown in Figure 4 - US Power Outages [12]. The number of customers affected by outages (blue) and the fraction of customers affected per year (red) are both increasing over time in the United States, despite increasing investment in protection, modeling, maintenance, and more advanced technology for the grid. This may be due to increases in LPHC cascades., created from data provided in [11], the overall frequency of outages with energy interruption in the last decades is still increasing, as well as the number of people affected by those interruptions (over 2% growth on average). Resilience has therefore become a prerequisite for reliability.

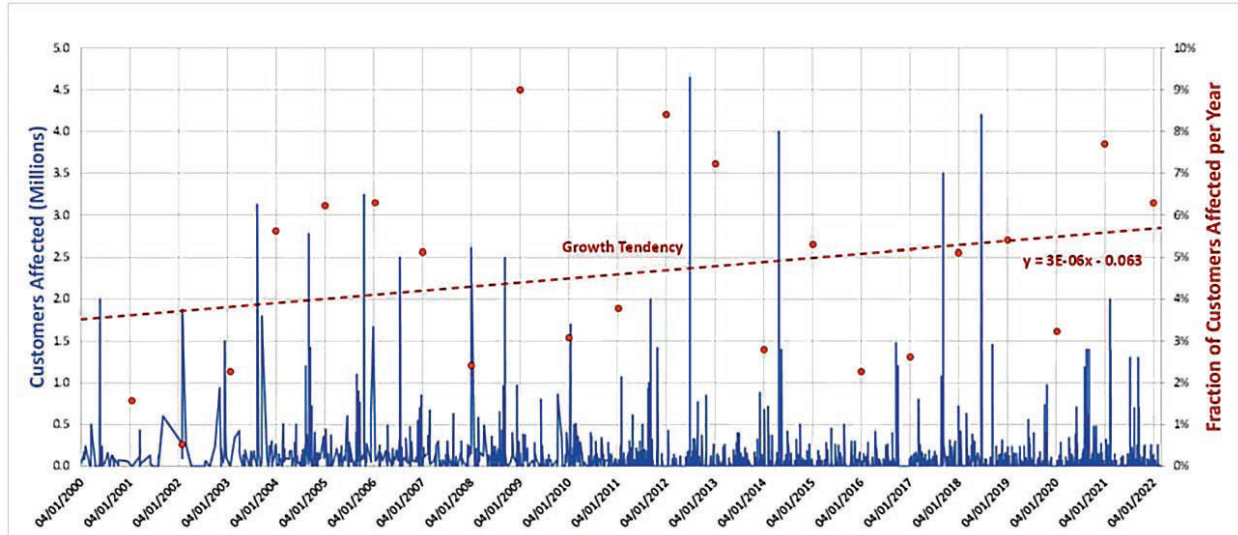


Figure 4 - US Power Outages [12]. The number of customers affected by outages (blue) and the fraction of customers affected per year (red) are both increasing over time in the United States, despite increasing investment in protection, modeling, maintenance, and more advanced technology for the grid. This may be due to increases in LPHC cascades.

RESILIENCE DEFINITIONS AND METRICS

Resilience has many definitions, from its historical, foundational meaning tied to the dynamics of life itself and the natural environment, to features of organizations and human psychology, to process definitions and practical engineering metrics that are being brought into the forefront of the design and operation of critical infrastructure. Resilience is fundamentally an adaptive learning process undertaken by societies and organizations. Resilience can be technically measured using standard threat-specific risk metrics (e.g. RAMCAP and similar), or with quantification of the “three R’s” of robustness, recovery, and resistance. Resilience can and must be approached using both threat-specific and all-hazard techniques. In Table 1 - Several Definitions of Resilience from Energy Sector Entities are presented some resilience definitions from energy sector entities [13]. Note that there is still not a standard (sectoral or cross-sectoral) definition of resilience in place. These definitions have a shared common element: focusing on enhancing infrastructure systems to not only operate reliably under normal conditions, but also adapt, withstand, and more rapidly recover from a growing number of LPHC events.

Table 1 - Several Definitions of Resilience from Energy Sector Entities

| Authority / Publishing Entity | Definition |
|---|---|
| National Association of Regulatory Utility Commissioners (NARUC) | “Robustness and recovery characteristics of utility infrastructure and operations, which avoid or minimize interruptions of service during an extraordinary and hazardous event.” |
| Federal Energy Regulatory Commission (FERC) | “The ability to withstand and reduce the magnitude and/or duration of disruptive events, which includes the capability to anticipate, absorb, adapt to, and/or rapidly recover from such an event.” |
| Presidential Policy Directive Critical Infrastructure Security and Resilience (PPD) | “The ability to prepare for and adapt to changing conditions and withstand and recover rapidly from disruptions. Resilience includes the ability to withstand and recover from deliberate attacks, accidents, or naturally occurring threats or incidents.” |
| National Renewable Energy Laboratory (NREL) | “The ability to anticipate, prepare for, and adapt to changing conditions and withstand, respond to, and recover rapidly from disruptions through adaptable and holistic planning and technical solutions.” |
| Electric Power Research Institute (EPRI) | “In the context of the power system, resiliency includes the ability to harden the system against— and quickly recover from—high-impact, low frequency events.” |
| PJM Interconnection | “Resilience, in the context of the bulk electric system, relates to preparing for, operating through and recovering from a high-impact, low-frequency event. Resilience is remaining reliable even during these events.” |
| National Academies of Sciences, Engineering, and Medicine (NASEM) | “Resilience is not just about lessening the likelihood that that these outages will occur. It is also about limiting the scope and impact of outages when they do occur, restoring power rapidly afterwards, and learning from these experiences to better deal with the events in the future.” |
| National Governors Association (NGA) / National Association of State Energy Officials (NASEO) | “The ability to withstand disasters better, respond effectively, and recover more quickly and to a more improved state.” |

Resilience is an Adaptive Learning Process

The concept of a resilient system is based on ecological theory developed decades ago in the 1960's. Underlying all technical definitions of resilience is the foundation of an effective adaptive learning process, based upon observations about how life thrives in nature.

All organizations, public and private, can enhance their resilience by building the capacity to adapt to disruptive events. Organizational resilience is the ability to bounce back from crises, but this ability is based on proactive preparation and adaptive capacity. Literature describes four key capabilities that underpin organizational resilience: anticipation, monitoring, responding, and learning [14].

Anticipation centers on the ability to perceive and correctly respond to risk. Risk perception is influenced by various factors, including organizational culture, leadership, and external influences. Organizations with robust accounting systems and proactive risk assessment mechanisms are better equipped to identify and respond to risks effectively. Integrating risk perception and accounting practices is vital for enhancing the resilience of organizations in the face of uncertainties and challenges [15]. Building the technical capacity of an organization to accurately measure risk is a key part of its adaptive learning cycle supporting resilience.

Successful resilience planning also requires a shift in mindset from reactive practices to proactive strategies that integrate people, natural and technical processes, and economic considerations. In addition to risk assessment, collaboration, stakeholder engagement, and adaptive management are necessary to building in resilience to our collective infrastructure. The resilience planning process requires integrating diverse knowledge systems, promoting learning and experimentation as well as adapting existing governance structures to new needs [16].

Two well established examples of resilience defined as an adaptive learning process are the "OODA Loop" and the "RAAG" or Resilience Analysis Grid [17, 18]. The emphasis of these definitions is that effective resilience is created by accelerating the learning cycle wherein we (1) accurately sense what is happening around us, (2) learn based on how well our previous decisions are performing, (3) anticipate what will happen next, and (4) take adaptive action based on what we anticipate will happen. The faster and better we complete this adaptive learning cycle, the more resilient we are. In the context of critical infrastructure, data collection and transparency are the key to (1); science and honest debate are the key to (2); science and engineering are the keys to (3), and engineering and leadership are the keys to (4).

Whereas engineering and operations professionals are trained to isolate and control a system, to keep it from changing and to protect it from shocks, the ecological systems definition emphasizes social, economic, and environmental change as the structure of the system adapts to maintain its basic functions. The literature on social-ecological resilience [19, 20] proposes a shift in perspective to recognize the dynamic and interconnected nature of social-ecological systems. Key elements of resilience include the ability to absorb disturbances, adapt to change, and transform when necessary, and the importance of understanding the interactions and feedback loops between social and ecological components in shaping system resilience.

The engineering and operations management communities are just beginning to explore the implications of ecological resilience for their work [21]. The standard engineering approach to resilience through hardening and redundancy is an efficient way to handle routine shocks that are well understood, but when shocks and changes are large and unexpected (e.g. Black Swans), the ecological systems resilience concept is more relevant. It is paramount for planning, engineering, and operations professionals to gain the perspective that their daily work toward the implementation of cost-effective and reliable systems exists in the context of a larger adaptive socio-ecological

system that sets the rules guiding daily decisions. But when big shocks or changes happen in the system, those rules should and will change as the larger ecological system adapts and learns. What happens to your finely tuned operations when the system breaks and the rules change- for example, when the Colorado River ran out of water in 2022, when the insurance companies pulled out of California and Florida to avoid covering fires and hurricanes, or when the power went out for Texas water utilities during Winter Storm Uri? Ecological resilience and adaptive learning cycles are a deeper resilience that underpin and shape technical engineering and operations resilience.

The adaptive learning process driving critical infrastructure resilience includes customs and traditions, government law and regulation, engineering design standards, monitoring and data collection, transparency with performance data, and the policies and actions of people and organizations including, for example, the federal government, major industry organizations, utilities, and individuals. The technical definitions and metrics of resilience are tools to support the adaptive learning cycle by measuring and helping to improve resilience. Resilience's many technical measures and definitions include measures of the system's reliability, its ability to resist damage from a hazard, and its ability to quickly recover from damage.

Technical Metrics for Resilience: RAMCAP R=TVC, the “Three R’s”, and All-Hazard metrics

Stakeholder engagement, community preparedness, and effective governance are all required to enhance resilience through adaptive learning [22,23,24,25]. But making this process work requires technically accurate metrics to operationalize. This includes technically accurate financial measurement of risk and of mitigation so that investments in resilience can be financed and weighed against competing priorities.

Engineering and operations management professionals do not yet have all the needed tools in hand. The current focus is on measuring and managing disruptions to systems using three classes of technical metrics, the “three R’s” [26]: resistance to change, robustness to a wide range of hazards and recovery or reorganization time after a shock. Performance on the first two R’s is typically measured using the RAMCAP (Risk Analysis and Management for Critical Asset Protection) risk-based performance process ($\text{Risk} = \text{Threat} \times \text{Vulnerability} \times \text{Consequence}$), and the third R is typically the domain of operations and of emergency management professionals who measure recovery in terms of cost and time to restore functions after a disruption. This approach to resilience is already widely implemented under the rubric of “reliability”. Much of current research seeks to advance the state of reliability by modeling a wider variety of hazards and interdependencies between more types of infrastructures.

Department of Energy (DOE) and Department of Defense (DOD) funded institutions, as well as elements of the Department of Homeland Security and Department of Commerce, have created and published definitions of resilience, as presented in Section . These definitions have similarities, but there is no consensus in the scientific, engineering, or financial communities on how to define resilience in the context of critical infrastructure, especially for practical purposes of cost-based engineering metrics. The most widely accepted metric for hazard-specific risk measurement and engineering is RAMCAP. The American Society of Mechanical Engineers (ASME) developed the method now known as RAMCAP Plus, that is widely used today by critical infrastructure organizations like utilities and their engineers. This hazards-based approach catalogs historically observed hazards and their consequences data along with models of future hazards to specify design requirements for the intensity, duration, and frequency of threats that the system should be designed to resist. Robust design and operations solutions that cost-effectively handle a wide range of threats are preferred over those that require highly precise threat predictions, that only address a narrow spectrum of threats, or that are costly. For example, it is cost-effective for a civil engineer to design a bridge that withstands the expected loads from rush hour traffic and from the expected

intensities of storms and earthquakes, but it is not cost-effective or feasible for the engineer to anticipate a contractor parking all the construction equipment to overload a single support beam; this black swan event was the bridge collapse in Minneapolis, MN in 2007.

The RAMCAP approach is effective and efficient for engineering resilience via resistance to and recovery from common hazards, but robustness to a wide range of hazards is a limitation of RAMCAP. Several features of today's security landscape for critical infrastructure limit RAMCAP's usefulness for achieving deep and broad resilience. "Knightian Unknowns" represent unknown, unknowable, or unusually severe hazards for which accurate anticipation is impossible based on historical data. "Nonstationarity" [27] refers to a future that will not reliably look like the past – even for well-observed historical hazards such as coastal flooding, that is worsening over time. Asymmetric adversarial threats that manifest themselves as rare or unknown hazards as the adversary actively seeks "soft" targets within a system, have become increasingly important since Al Qaeda's September 11th, 2001 attacks. For all these reasons, RAMCAP is insufficient by itself as a basis for critical infrastructure systems resilience. (see detailed discussion of RAMCAP in Section below).

Whether Black Swans originate due to extreme weather, cyber features, and/or adversary attacks, the sheer complexity and scale of interdependent systems also may both trigger and worsen an initial disruption. An all-hazards methodology to measure resilience must also consider interdependent vulnerabilities among critical infrastructure systems and the possibility of cascade failures propagating from one system to another, whether internally or across sectors. As portrayed in Figure 2 - System Interdependencies, most critical infrastructures have interdependencies and can be affected by multiple systems, with cascades spreading from one system to another, internally and externally.

Understanding the consequences and impacts of the failure events is as fundamental for determining investment in resilience mitigation as assessing the system propensity to cascade failure. Direct financial consequences are easily identified during failure events, usually associated with lost revenue, repair, and immediate recovery cost. However, utilities may be exposed to many indirect consequences – loss of life, morbidity, legal liability, reputation damage, uninsured liabilities, that can generate tremendous costs and damage, possibly leading to bankruptcy and/or imposition of new regulatory requirements. The population that the utility serves as well as the utility itself may suffer losses that go well beyond what may be captured by the authority to fund mitigation represented in existing rate and other financial processes.

Due to the hazards-oriented limitations of RAMCAP and similar, engineering and operations resilience must be complemented with "all-hazards" approaches to resilience that rely on different assumptions and do not require accurate anticipation of the intensity, duration, or frequency of a hazard to achieve resilient outcomes. For example, engineers and operators can create a diversity of options by arranging for multiple decorrelated systems or sources [28] to increase the probability that adequate adaptive options will remain available after an unanticipated threat impacts the system. Moreover, engineers and operators can achieve resilience by focusing on designing systems that resist "cascading failure" through the system's network regardless of the cause of the original failure, keeping the consequences of failure localized and small, instead of focusing exclusively on resisting the primary failure caused by a specific kind of threat [29]. For example, an all-hazards design for the Minneapolis MN bridge would have resulted in the contractor's overloading equipment falling into the river when the beam failed, but that would not have taken down the entire bridge in a cascading collapse. Or, an all-hazards design would have recovered the damage of the failed beam quickly enough to prevent the failure of the rest of the bridge. An all-hazard approach assumes the failure of critical system components, and then proceeds to de-

velop engineering and operations solutions to limit the spread of the damage and contain overall consequences of the failure.

The hazard-specific and all-hazard approaches have complementary advantages, and when used together these approaches yield systems that are both very efficient in their resistance to common hazards while also providing robust resilience to unanticipated hazards. The hazards-agnostic approaches bring an important dose of perspective and technical humility to bear on the problem of resilience. We need both hazard-specific and all-hazard technical metrics in order to build resilient systems.

From Reliability to Resilience

Reliable service is the central goal of critical infrastructure systems and their operators and reliability performance is measured and regulated in most jurisdictions (and by most supplier service contracts). However, reliability in the face of unexpected and severe events requires resilience. Resilience supports and improves reliability under extraordinary circumstances, but reliability may not support and improve resilience under extraordinary circumstances. “Uptime” under routine operating conditions including routine threats is a common measurement of reliability. Consequence (or risk) created by failure is a better measure of resilience. In other words, reliability focuses on minimizing service failures, and resilience focuses on minimizing the consequence (or risk) created by service failures. Reliability is focused on routine circumstances, and resilience on extraordinary circumstances. If a utility operator is forced to choose one metric, choose resilience, because risk is the more fundamental measurement, and because the catastrophic life-and-death consequences of major failures in critical infrastructures outweigh the inconvenience of routine outages. Fortunately, we may pursue both reliability and resilience, and the two complement each other. Figure 5 - Reliability VS Resilience provides a table comparing reliability and resilience.

| | RELIABILITY | RESILIENCE |
|-----------|--|--|
| Timeframe | <ul style="list-style-type: none"> • Daily (statistical predictability) | <ul style="list-style-type: none"> • Decades (unpredictable “Black Swans”) |
| Costs | <ul style="list-style-type: none"> • Lost revenue • Contractual costs • Repair • Recovery • Prevention | <ul style="list-style-type: none"> • Loss of life • Extreme costs • Uninsured liability • Bankruptcy • Reputational injury • Prosecution • Political and regulatory response |
| Focus | <ul style="list-style-type: none"> • Asset failure • Hardening against anticipated hazards • Preventative maintenance and replacement • Limited customer differentiation • Annual budgeting | <ul style="list-style-type: none"> • Critical function failure • Mitigation for unanticipated events • Containing and recovering cascading failures • Critical customer protection and recovery • Variable budgeting |
| Metrics | <ul style="list-style-type: none"> • Well established quantitative standards • Each sector measures its own performance • Service reliability metrics • Asset service life & optimal replacement schedule • Reliability ROI for Capital and Rate Planning | <ul style="list-style-type: none"> • Emerging quantitative standards • System interdependency analysis • Cascade risk and resilience scoring • Interdependent system resilience mitigation & optimization • Critical customer & recovery order planning • Resilience ROI for Capital Improvement and Rate Planning |

Figure 5 - Reliability VS Resilience

Figure 2 - System Interdependencies Resilience Standards in Use Today

American Society of Mechanical Engineers (ASME): Risk Analysis and Management for Critical Asset Protection (RAMCAP Plus Process, or R=TVC)

The American Society of Mechanical Engineers (ASME) program called RAMCAP is in widespread use as a set of updated standards for risk and resilience assessment in critical infrastructure systems. These standards are in reality a process to provide a framework for assessing and improving the resilience of these systems to disruptions. The standards themselves are not primarily quantitative; instead, they are designed to be flexible and adaptable to the specific needs of individual systems by providing a systematic approach for identifying vulnerabilities, assessing risks, and implementing measures to improve resilience.

The ASME RAMCAP standards are divided into three main categories: assessment, design, and operation. The *assessment* standards provide a process for identifying the potential vulnerabilities and risks to a system, and for evaluating the current level of resilience. The *design* standards provide guidance on how to design systems that are more resilient to disruptions, including guidelines for selecting materials and components, and for implementing redundancy and diversity. The *operation* standards provide guidance on how to operate and maintain systems to ensure they remain resilient over time.

Importantly, the standards cover a variety of different types of disruptions, including natural hazards, cyber threats, and human-caused events, whether accidental or adversarial. They also address the importance of considering the entire lifecycle of a system, from design and construction, through operation and maintenance, to eventual decommissioning.

While the ASME RAMCAP standards are not embodied in law or regulation and are voluntary, they are widely recognized and used in the power industry as a best practice for resilience. As we will discuss below, the water industry has also adapted RAMCAP for its needs through its J100 resilience standard. RAMCAP standards are designed to be flexible and adaptable to the specific needs of different types of systems and organizations, and provide a systematic approach for identifying vulnerabilities, assessing risks, and implementing measures to improve resilience.

In summary, the ASME RAMCAP resilience standards provide a framework for assessing and improving the resilience of critical infrastructure systems to disruptions, by providing guidelines for identifying vulnerabilities, assessing risks, and implementing measures to improve resilience. These standards are widely recognized and used in the industry as a best practice for resilience and provide a systematic approach to improve the resilience of different types of systems and organizations.

The ASME RAMCAP defines “risk” as a product of the likelihood of a threat attacking a system asset (a probability), the vulnerability of that system component to that threat (a probability), and the proximate consequences of the failure of that component due to that threat (or, $R=TV C$). Risk is therefore expressed as an expected loss due to a specific threat, using the same units as the consequence, e.g. dollars or lives lost.

Risk = Threat x Vulnerability x Consequence

Resilience is broadly defined as the ability to function through an attack or natural event or the speed at which an asset can return to virtually full function (or a substitute function or asset provided) [30]. Resilience as a concept is still being formalized. Some prefer to measure resilience using time, from time of event until return to full function, but this ignores partial service denial (severity), which is generally much more common than complete loss of function, and the value of the services denied. For the purposes of the RAMCAP Plus process, resilience is defined in different ways for the asset owner and community, respectively.

From the narrow or “direct” perspective of the system asset’s operator, the consequences are limited to a combination of lost revenue, legal liabilities, recovery costs, reputational costs, and reg-

ulatory fines. From the broad or “total”, societal” perspective, consequences additionally include public morbidity and mortality, lost revenue and income by businesses and their employees, security failures and crimes, and long term losses from foregone economic development. Some key definitions follow: **Lost revenue** – the product of the duration of service denial (in days), the extent of service denial (in units of service denied per day) and the price (in dollars per unit, estimated at pre-event levels), which are all essential parts of estimating the owner’s financial loss.

Lost Economic Activity in the Community – the amount of decrease in the loss of output to direct customers and the indirect losses (multiplier effect) throughout the economy of a given region due to denial of service. It is estimated as a function of the asset’s lost revenue and the duration of the service denial using an economic model. One application used a static application of basic regional economic data and an input-output table, modified to reflect the resilience of the respective business sectors.

Threat – Any indication, circumstance or event with the potential to cause the loss of, or damage to, an asset or population. In the case of terrorism risk, threat is based on the analysis of the intention and capability of an adversary to undertake actions detrimental to an asset or population and the attractiveness of the asset or population relative to alternative assets or populations. In the case of natural hazards, threat refers to the historical frequency of the specific natural event to which the asset(s) may be subjected. In both cases, threat is summarized as the likelihood the event will occur.

Vulnerability – Any weakness in an asset or infrastructure’s design, implementation or operation that can be exploited by an adversary or contribute to functional failure in a natural disaster. Such weaknesses can occur in building characteristics, equipment properties, personnel behavior, locations of people, equipment and buildings or operational and personnel practices. In risk analysis, vulnerabilities are usually summarized as the conditional probability that, given an attack or natural event, the estimated consequences will ensue, i.e., the attack will succeed or the natural event will cause the estimated damage.

Consequence – The outcome of an event occurrence, including immediate, short and long-term, direct and indirect losses and effects. Loss may include human fatalities and injuries, financial and economic damages and environmental impacts, which can generally be estimated in quantitative terms. Consequences may also include less tangible and less quantifiable effects, including political ramifications, decreased morale, reductions in operational effectiveness or military readiness or other impacts.

National Institute of Standards and Technology (NIST): Interdependent Networked Community Resilience Modeling Environment (IN-CORE)

According to The National Institute for Standards and Technology (NIST), resilience refers to the ability of a system, community, or organization to prepare for, withstand, and rapidly recover from disruptions. This includes the ability to anticipate, absorb, adapt to, and/or rapidly recover from the effects of an adverse event, while maintaining the continuity of essential functions.

NIST sees resilience as important because disruptions can have significant negative impacts on individuals, communities, and organizations. These impacts can include loss of life, property damage, economic disruption, and more. By building resilience, we can reduce the likelihood and severity of these impacts and minimize the overall disruption caused by an event. NIST sees resilience not as a one-time or static state, but rather as a continuous process of adaptation and improvement in a world where unexpected disruptions may occur swiftly and with major impact. In NIST’s view, organizations, communities, and systems need to be constantly assessing and updating their resilience plans and strategies in response to changing risks and vulnerabilities.

Resilience, according to this approach, has three main components: preparedness, response, and recovery. *Preparedness* involves taking steps to anticipate and mitigate the potential impacts of disruptions. This can include processes like risk assessments, emergency planning, and training. *Response* involves taking action during and immediately after a disruption to minimize the impacts and protect lives and property. *Recovery* refers to the process of returning to normal operations after a disruption. This can include things like restoring damaged infrastructure, providing aid to affected individuals, and conducting after-action reviews to learn from the event and improve future preparedness and response.

NIST sees effective community resilience metrics as addressing two key questions:

- How can community leaders know how resilient their community is?
- And how can they know if their decisions and investments to improve resilience are making a significant difference?

NIST defined in [31] its community resilience metrics. Currently, NIST accepts a wide variety of community resilience approaches as valid: descriptive or quantitative; based on interviews, expert opinion, engineering analysis, or making use of pre-existing datasets; presented as an overall score or as a set of separately reported scores across physical, economic, social, and environmental dimensions. NIST has concluded that time to recovery of function is the most important resilience metric to be employed, because other resilience methods are insufficiently validated.

Noting the variety of approaches to resilience in use, the National Academies Committee on Increasing National Resilience to Hazards and Disasters and the Committee on Science, Engineering, and Public Policy in 2021 evaluated seventeen approaches to measuring various aspects of resilience. The authors concluded that none of the seventeen existing methodologies satisfactorily addressed both of the two basic questions posed by NIST noted above. One of the report's six main recommendations therefore is the development of a "national resilience scorecard, from which communities can then develop their own, tailored scorecards".

Other recent reviews of hazard risk reduction and resilience make similar recommendations for flexible scorecards [32] that permit a tailorable or locally relevant scorecard, concluding that a single prescriptive scorecard may not be appropriate for the wide range of US communities, from small agriculture communities to large industrial cities.

NIST and its partners from 12 universities, led by Colorado State University, established the Community Resilience Center of Excellence [33]. The objective is to accelerate the development of system-level models to support community resilience decision-making. A dynamic platform was developed to support resilience analysis based on research, development, and modeling relating to communities. The Interdependent Networked Community Resilience Modeling Environment (IN-CORE) is an open-source software platform that incorporates a risk-based approach to decision-making, enabling quantitative comparisons of alternative resilience strategies [34]. IN-CORE allows users to optimize community disaster resilience planning and post-disaster recovery strategies intelligently, using available data and physics-based models of inter-dependent physical systems combined with socio-economic systems.

National Academies

The National Academies (NA), non-profit institutions providing expert advice publicly, including the National Academy of Sciences, the National Academy of Engineering, and the National Academy of Medicine, established a program on Risk, Resilience, and Extreme Events (Resilient America) in 2014. NA founded the Resilient America program after the National Research Council's 2012 publication of the report "Disaster resilience: A national imperative".

FEMA in 2020 asked Resilient America to convene a committee on hazard mitigation and resilience-applied research topics as part of its efforts to reduce the immense human and financial toll of extreme events. NA released a consensus study report in 2022 defining resilience as “The ability to prepare and plan for, absorb, recover from, and more successfully adapt to adverse events.” [35]. To prepare this report NA engaged with the academic, public, and private sectors at national and local levels to achieve the following goals:

- Increase understanding of complex risks and extreme events in a changing environment, and the exposure of communities, infrastructure, and natural systems to these threats.
- Investigate and strengthen attributes of equitable, resilient systems and communities, including their interconnections and interdependencies.
- Test, communicate, and strengthen implementation of equitable strategies for adapting to changing risks and robust recovery from disruptions.
- Share accessible science and data for strengthening resilience and adaptive action, including policies, tools, best practices, and metrics.
- Connect and facilitate partnerships among scientists, data providers, practitioners, and decision makers.
- The National Academy of Engineering hosted a workshop in October 2022: “Creating A Sustainable National Electric Infrastructure While Maintaining Reliability and Resiliency of the Grid”. Several ISOs, transmission companies and power utilities participated, and a report was released afterwards. Some of the recommendations include:
 - New tools are necessary for integrated resource and T&D planning and investment prioritization.
 - The creation of grid resilience standards is necessary.
 - Probabilistic assessments are necessary to account for LPHC event impacts on power grids.

Department of Energy (DOE): Voluntary Action Program for Resilience (VARP)

Drawing on the work of its associated national laboratories, the U.S. Department of Energy has adopted a definition of resilience that applies to a wide range of critical infrastructure sectors, including energy, transportation, and telecommunications, as well as the built environment and other essential systems. The DOE places a particular emphasis on the importance of energy resilience, highlighting the central role of energy systems in supporting critical infrastructure and enabling economic growth and development.

DOE defines resilience as “the ability to prepare for and adapt to changing conditions and withstand and recover rapidly from disruptions through adaptable and holistic planning and technical solutions.” This definition emphasizes the importance of anticipating and adapting to changing conditions, as well as the need for a holistic and integrated approach to resilience that includes both planning and technical solutions. It also emphasizes the importance of rapid recovery from disruptions, which requires the ability to quickly assess and respond to the impacts of disruptive events. Collaboration among stakeholders, effective risk management and planning, and the integration of advanced technologies and tools are all paramount, as is incorporating resilience into long-term planning and decision-making processes.

To help communities and organizations build resilience to the impacts of natural and man-made hazards, DOE launched Voluntary Action Program for Resilience (VARP) as a voluntary program in 2016. VARP provides a framework for communities and organizations to assess their current level of resilience, identify areas for improvement, and develop and implement plans and strategies

to enhance their resilience. The program is designed to be flexible and adaptable to the unique needs and priorities of different communities and organizations, and to encourage innovation and collaboration in the resilience planning process.

VARP participants may include local governments, businesses, academic institutions, and community groups. Participants commit to following a set of core principles for resilience planning, including:

- **Collaboration:** Participants agree to collaborate with other stakeholders in the resilience planning process, including other organizations, community groups, and government agencies.
- **Assessment:** Participants agree to conduct a comprehensive assessment of their current level of resilience, including an analysis of their risks, vulnerabilities, and capabilities.
- **Planning:** Participants agree to develop and implement plans and strategies to enhance their resilience, based on the results of their assessment.
- **Monitoring and Evaluation:** Participants agree to monitor and evaluate the effectiveness of their resilience plans and strategies, and to make adjustments as needed.

DOE's VARP is a resource for communities and organizations seeking to build resilience to a wide range of hazards, including natural disasters, cybersecurity threats, and other disruptive events.

Cyber Resilience

Cyber security and cyber resilience, including relating to Supervisory Control and Data Acquisition systems (SCADA) and the interface of cyber and physical operating systems generally, has become an urgent topic due to the potential of cyber threats to manifest as Black Swans [36]. A US Executive Order (EO) issued in May 2021 declared key themes in cybersecurity strategy and foundational ideas linked to the need for greater resilience [37]. The objective is to identify opportunities to enhance, measure, and sustain long-term resilience against the impacts of malicious cyber activity, at the entity level and systemic level, including continuity of the economy. The EO is expected to be implemented through cyber security strategy performance goals issued in 2023 [38,39].

The Executive Order states something fundamental to all considerations of critical infrastructure resilience: metrics are needed because investments in resilience can be expensive, with benefits that may be realized only intermittently because “black swan” events are unusual, making it return on such investments difficult to calculate. This can make resilience investment an uphill battle in the context of budgeting, capital raises, and rate applications [40]. For this reason, a viable strategy for resilience requires more than predictions about hazards and identification of vulnerabilities; it also requires decision frameworks for understanding what can and should be made resilient, how resources should be allocated, and, most importantly, an ability to quantify the value of investments in terms of resilience over time.

Department of Homeland Security (DHS): Cybersecurity and Infrastructure Security Agency (CISA) and Federal Emergency Management Agency (FEMA): Resilience Analysis and Planning Tool (RAPT)
The Department of Homeland Security (DHS) oversees two agencies increasingly relevant to resilience. DHS' Cybersecurity and Infrastructure Security Agency (CISA) with its National Risk Management Center, and its Federal Emergency Management Agency (FEMA), share a common definition of resilience as the ability to prepare for, withstand, and rapidly recover from disruptions [41]. This definition highlights the key components of resilience, which include the ability to anticipate potential disruptions, prepare for them in advance, and quickly adapt and recover when they

do occur. In the context of emergency management and national security, resilience refers to the ability of individuals, communities, and critical systems and infrastructure to withstand and recover from natural or man-made disasters and to ensure the continuity of essential services during and after disruptions. This includes not only physical systems such as power grids and transportation networks, but also social systems such as communities and organizations. Both anticipatory mitigation for low probability high consequence events and well-instituted emergency management procedures are essential to ensure resilience in the face of potential disasters.

FEMA has developed the Resilience Analysis and Planning Tool (RAPT), a web-based software to help communities assess their resilience to natural and man-made hazards and plan for future events. RAPT provides a standardized framework for communities to identify and evaluate their risks, capabilities, and vulnerabilities, and to develop plans and strategies to enhance their resilience. RAPT focuses primarily on the assessment and planning phases of the resilience process and, as with the DOE tools, requires significant time, effort, and resources to use effectively, including the collection and analysis of data, stakeholder engagement, and the development of resilience plans and strategies. This may be a challenge for communities with limited resources or expertise.

American Water Works Association (AWWA) and Water Environment Foundation (WEF): Water Resilience Framework (J100)

The Water Resilience Framework J100 is a voluntary standard that emerged out of RAMCAP in response to the requirement of a risk and resilience analysis set forth in the federal American Water Infrastructure Act of 2018. The American Water Works Association (AWWA) and the Water Environment Federation (WEF) developed J100 through the Joint Committee on Water Utility Resilience, established in 2015 to help water utilities better understand and prepare for the impacts of natural and man-made hazards, and to promote the development of more resilient water systems. J100 defines resilience in the water sector as “the ability of a water system to adapt to changing conditions and to withstand and recover from disruptions, stresses, and acute events.”

The J100 framework recognizes that disruptions and stresses are inevitable and that water systems must be able to adapt and respond effectively to these challenges to maintain their essential functions and services. The standard highlights the importance of adaptability and the ability to withstand and recover from various defined threats – potential disruptions, stresses, and acute events, such as droughts, floods, power outages, chemical spills, and cyber-attacks. It requires utilities to define threat-asset pairs, for example, a flood in relation to a particular pump station, and then to prioritize risks in terms of threats and asset vulnerabilities, for purposes of mitigation and emergency preparedness.

J100 is an assessment process that focuses on building capacity and capabilities that enable water systems to respond effectively to a range of known potential disruptions and stresses. J100 is being continuously updated, most recently in 2021 and has recently introduced the idea of addressing risk from interdependencies in water systems.

CIGRE Working Group C4.47

CIGRE is a global professional power engineering community committed to the collaborative development and sharing of end-to-end power system expertise. CIGRE Working Group C4.47 has defined resilience as the “ability of an electrical system to prepare for, absorb, recover from and adapt to a disturbance, while maintaining its essential functions, structure, and identity” [1]. This definition emphasizes the ability of the power system to not only withstand and recover from disruptions but also to adapt and evolve to changing conditions over time.

CIGRE Working Group C4.47’s definition of resilience includes several key components, such as the importance of maintaining the essential functions of the power system, the need to preserve the overall structure and identity of the system, and the requirement for effective preparation, absorption, and recovery from disruptions. This definition highlights the importance of a holistic and system-level approach to resilience in the electric power system context, including the integration of advanced technologies and tools, effective risk management and planning, and collaboration among stakeholders. Figure 6 - CIGRE WG C4.47 Resilience Trapezoid [1]6 presents a graphical description of CIGRE’s resilience definition for power systems disturbances.

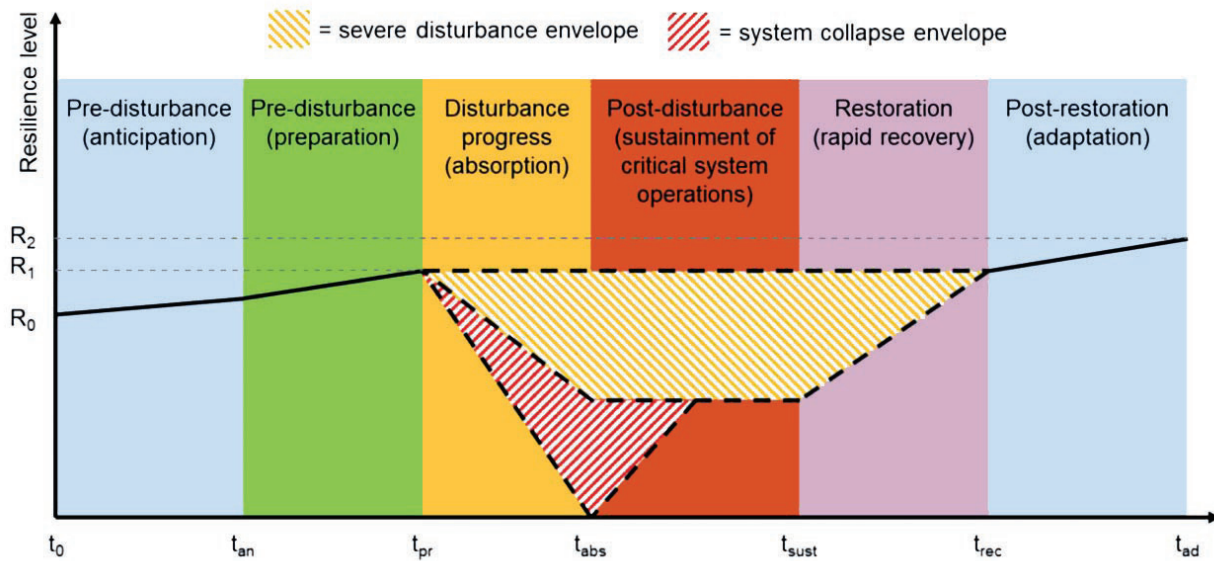


Figure 6 - CIGRE WG C4.47 Resilience Trapezoid [1]

The Institute of Electrical and Electronics Engineers (IEEE)

The Institute of Electrical and Electronics Engineers (IEEE), the electrical sector’s leading professional organization, does not have a single definition of resilience, rather the organizations members apply the concept of resilience differently to a wide range of fields and applications. However, in the context of the IEEE’s work related to electric power systems, the organization has developed a definition of resilience that focuses on the ability of the power system to withstand and recover from disruptions.

According to the IEEE, resilience in the electric power system context is “the ability to withstand and reduce the magnitude and/or duration of disruptive events, which includes the capability to anticipate, absorb, adapt to, and/or rapidly recover from such an event” [42]. This definition emphasizes the need for effective planning and preparation, as well as the ability of the power system to adapt to changing conditions over time.

The IEEE’s definition of resilience includes several key components, such as the importance of maintaining essential functions and services during disruptions, the need for effective response and recovery, and the importance of collaboration among stakeholders. This definition highlights the importance of a holistic and system-level approach to resilience in the electric power system context, including the integration of advanced technologies and tools, effective risk management and planning, and collaboration among stakeholders. Figure 7 - IEEE Time Varying Resilience Multi-Phase Trapezoid [42]7 presents a graphical description of IEEE’s resilience definition for power systems disturbances.

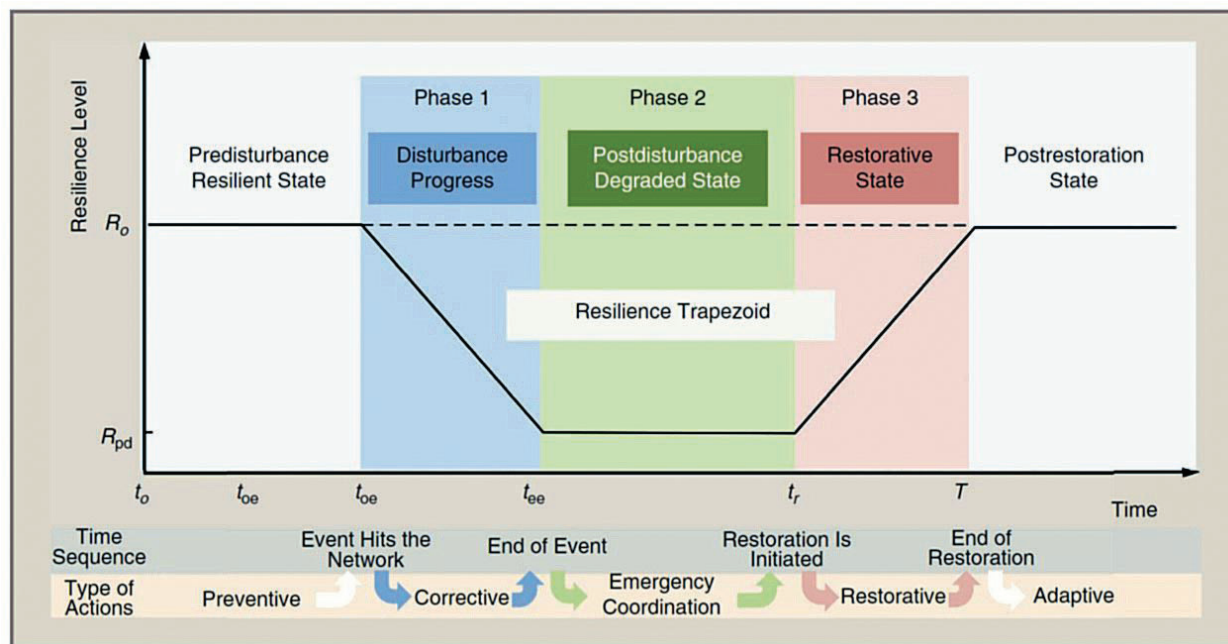


Figure 7 - IEEE Time Varying Resilience Multi-Phase Trapezoid [42]

Eastern Interconnection Planning Collaborative (EIPC)

The Eastern Interconnection Planning Collaborative (EIPC) is a collaboration among electric utilities, their regulatory agencies (ISO's and RTO's), and other stakeholders in the Eastern Interconnection region of the United States. EIPC is one of three major power grids in North America [43], together with the Electric Reliability Council of Texas (ERCOT), and the Western Electricity Coordinating Council (WECC). The EIPC has developed a definition of resilience for the electric power sector and the Eastern Interconnection region.

According to the EIPC, resilience is “the ability of the Eastern Interconnection to prepare for, withstand, and recover from high impact, low frequency events that could cause significant disruption to the electricity system and to the broader economy.” Such events might include severe weather events, cyber-attacks, physical attacks, or other disruptive events that could cause widespread power outages.

The EIPC's definition of resilience also emphasizes the importance of both preparing for and responding to such events. This includes taking steps to enhance the power system's resilience, such as through the use of advanced technologies, improved planning and coordination among stakeholders, and investments in infrastructure and equipment. It also includes having effective response and recovery plans in place, which can help to minimize the impacts of disruptive events and facilitate a rapid return to normal operations.

Electric Power Research Institute (EPRI)

The Electric Power Research Institute (EPRI) defines resilience, in the context of power systems, as “the ability to harden the system against - and quickly recover from - high-impact, low-frequency events” [44]. Such LPHC events can threaten lives, disable communities, and devastate generation, transmission, and distribution systems, as well as interdependent systems such as natural gas pipelines and other fuel transport and telecommunications. Some examples of such events are severe weather or natural events (hurricanes and consequent flooding, tornadoes, earthquakes and consequent tsunamis, wildfires, ice storms, etc.), severe geomagnetic disturbances, cyber-at-

tacks, physical attacks, coordinated cyber and/or physical attacks, electromagnetic pulse (EMP), high-altitude EMP, intentional electromagnetic interference attacks and pandemics.

EPRI defines resiliency as described above but also acknowledges diverse definitions of resilience associated with different systems, areas of actuation and interdependencies, including in the context of climate preparedness and resiliency.

EPRI has developed a Resilient System Investment Framework (RSIF). The objective of this framework is to help transmission planners assess the impacts and consequences resulting from LPHC contingency events on their systems. RSIF is based on the Siemens PTI PSS®E – a software system – which is intended to apply and solve extreme contingency events for a given power flow case, evaluating the resulting impacts to determine possible paths of cascading failures and the associated consequences. RSIF thus can determine the risk of adverse system impacts emanating from the extreme contingency event analyzed.

NetResilience

Resilience engineering literature for critical infrastructure systems does not make available a standard scientific definition and related industry guidelines for objective resilience metrics, especially metrics that consider critical infrastructure as an interconnected set of systems. One company is filling this gap by providing a new scientific method to evaluate resilience, using an objective scale to show risk of cascade failures that engineers can use to make improvements in system resilience, and relating this resilience score to dollar values that estimate the risk exposure of a system to LPHC events for use in cost-benefit analysis and capital planning¹.

This supplies a standardized methodology to evaluate resilience against LPHC events in critical infrastructure. The technique is based on engineering analysis, network sciences, and probabilistic measures, observing asset-to-asset risk in independent systems (e.g. power grid) or interconnected, interdependent systems (e.g. power grid and gas distribution or water distribution and connected SCADA and power supply). This provides utilities and other organizations including industrial sites and communities with a real measure of the system resilience considering all-hazard and LPHC events. The score is an intuitive zero to ten scale as presented in Figure 8 - Lewis ScoreSM [12]. Networked systems with a status below the score of “5” (in red) tend to propagate and exacerbate initial failures to create high-consequence cascading failures. A Lewis ScoreSM that is confidently above this “tipping point” at 5 indicates that a networked system tends to suppress cascades, containing failures to the immediate vicinity and consequences of the primary failure, and avoiding high consequence failure⁸. This methodology and metrics are discussed in [12] with an example of a large-scale power system’s resilience analysis.

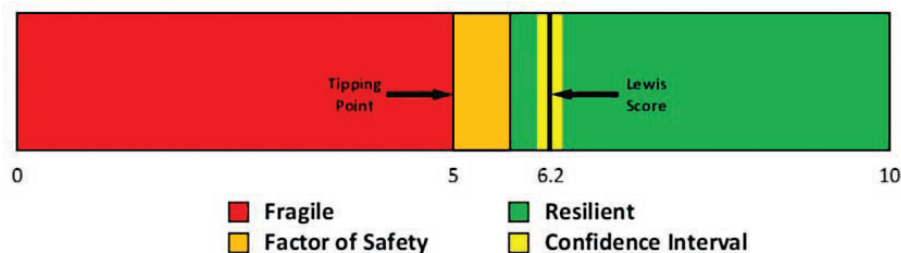


Figure 8 - Lewis ScoreSM [12]. Networked systems with a status below the score of “5” (in red) tend to propagate and exacerbate initial failures to create high-consequence cascading fail-

¹ <https://www.critsci.com/>

ures. A Lewis ScoreSM that is confidently above this “tipping point” at 5 indicates that a networked system tends to suppress cascades, containing failures to the immediate vicinity and consequences of the primary failure, and avoiding high consequence failure.

This method identifies critical assets – assets critical specifically for risk of cascade failures – and proposes mitigation options and recovery order, also optimizing these investments and providing benchmark comparisons to the Lewis ScoreSM and a financial risk measure for LPHC events. The methodology focuses on hardening and/or reconfiguring the system against cascade failures caused by unpredictable black swans. It recommends budget allocation opportunities that increase the system’s resilience against LPHC cascade failures, avoiding the severe consequences caused by such events, and showing how these reduce financial risk to the utility and their customers.

The risk measurement for financial exposure to loss from extreme events like Winter Storm Uri, is called maximum probable loss (MPL RiskSM). MPL RiskSM is a statistic of the consequence distribution estimated for all possible cascading failure events in the system. It is a function of the exceedance probability for cascade failure and marginal consequence, as presented in Figure 9 - Maximum Probable Loss (MPL RiskSM) [12], an essential statistic of a complex networked system’s expected failure consequence distribution. MPL RiskSM indicates a level of risk that is both relatively severe and also relatively common. MPL RiskSM has units of expected loss, such as dollars (\$) or lives lost.⁹ It provides a value for the most likely cascade failure with the highest consequence (direct and/or indirect) in a given system.

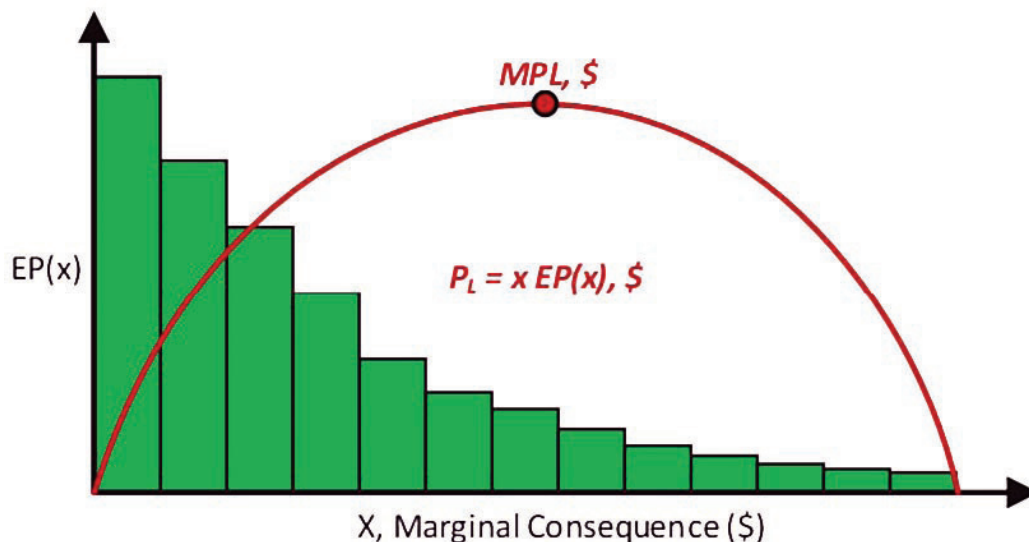


Figure 9 - Maximum Probable Loss (MPL RiskSM) [12], an essential statistic of a complex networked system’s expected failure consequence distribution. MPL RiskSM indicates a level of risk that is both relatively severe and also relatively common. MPL RiskSM has units of expected loss, such as dollars (\$) or lives lost.

HOW CAN STAKEHOLDERS COOPERATIVELY MITIGATE CASCADING FAILURE RISK?

To achieve resilience at community, regional and national scale, and beyond, and reduce the consequences of potentially catastrophic events— whether in operations, money, the natural and built environment, or life and health -- multiple stakeholders must develop a common understanding of catastrophic risk and how to mitigate it. These stakeholders include: engineering and operations

personnel involved in designing and running the systems; emergency managers who maintain coordination and recovery capacity for utilities and engage with governmental emergency personnel and others in the private sector; finance and insurance professionals who determine budgets, investments, and insurance; regulators who set rates and standards and monitor or enforce compliance; public officials at the local, State and federal levels directing or regulating utilities and promoting resilience; and researchers who drive progress in utilities and their supporting engineering companies, universities and governmental and nonprofit institutions.

Today these groups jointly create and manage day to day reliability in engineered systems including power, water, and telecommunications. To enable proper allocation of resilience investments, it is essential to augment reliability with resilience to large scale cascading failures by using a straightforward resilience metric to quantify the level of resilience in a given system that all stakeholders can agree upon. That method must apply to all hazards, including human threats, and must evaluate interdependent critical infrastructure.

The method described here, using a Lewis ScoreSM and risk metrics, takes advantage of network science, a relatively new concept, to solve problems of interdependency, and uses probability science to address black swan risk. The use of network science to evaluate power systems' resilience to cascading failure has been discussed in the literature [29, 45], but has received far less attention than the standard power engineering paradigm. The network-based approach would typically employ the (interdependent) network topology, and among other features a mathematical approach to identify the critical assets on the system which tend to contribute to cascading system failures. Cascading failure probabilities are empirically determined, as are the direct (to the utility) and total (societal) consequences of critical infrastructure failure.

For larger and more complicated networked systems, interdependent systems can be modeled together using network science far more feasibly and simply with the probabilistic and topological approach than with the physics-based engineering modeling approach [46, 47]. Nevertheless, the network approach has both advantages and disadvantages compared to the physics-based modelling approach. Interdependency of systems is one element that favors the simpler and more flexible network approach. Overall, the network approach provides a largely complementary and orthogonal view into interdependent network resilience; it can be used to critique and corroborate the standard engineering approach, adding robustness and confidence when used in tandem. The system is greater than the sum of its parts, so analysis of the interdependent networks yields fundamentally different and superior resilience findings [48].

The following example, presented in [12], demonstrated the network resilience method for a major national power transmission system- in this case, the Brazilian interconnected system. The Brazilian transmission system supplies the entire nation of Brazil and has approximately 170,000 km of high-voltage transmission lines, as seen in Figure 10 - Brazilian Interconnected System [12]. It has 176 GW of installed generation capacity and attends to a population of roughly 213 million. This system is heavily dependent on renewable generation, with approximately 86 % of its energy matrix based on hydro, wind, solar, and biomass generation.

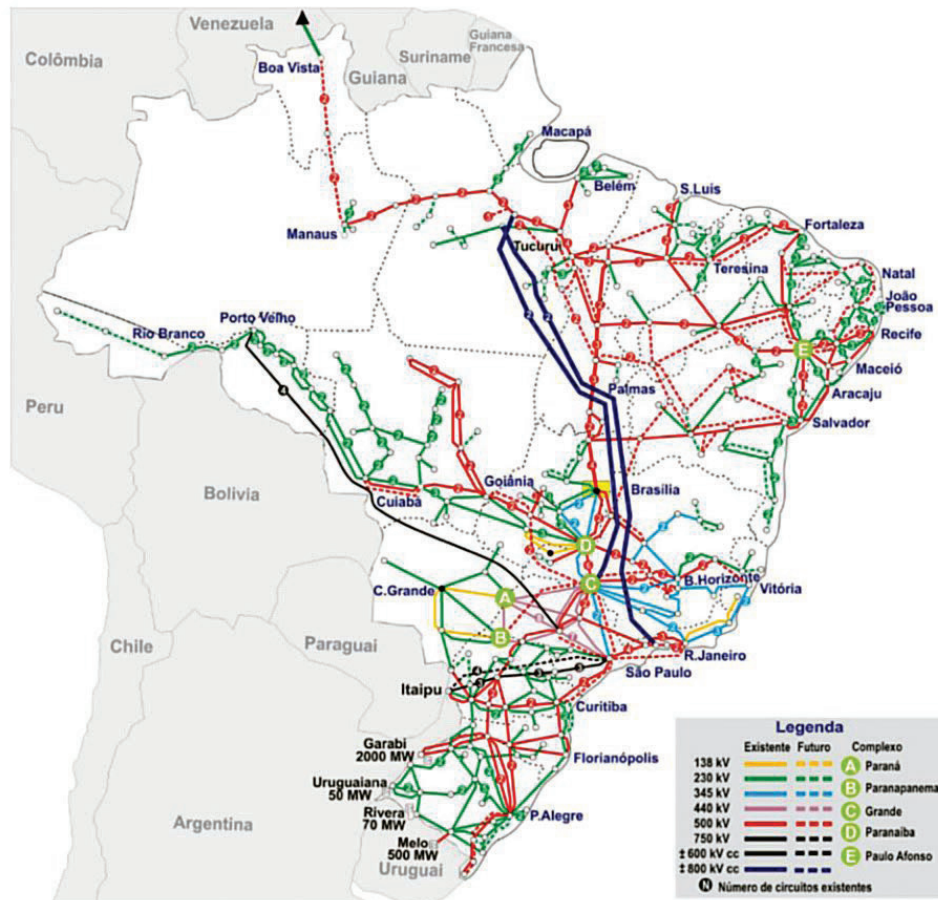


Figure 10 - Brazilian Interconnected System [12].

Software and advanced computing enable the estimation of cascading failures extent and severity for all possible primary failure initiation events, resulting in a distribution of consequences (US\$/h) for many thousands of simulated failures, along with statistical results for the tendency of each network component to participate in LPHC cascading failures. The probability of cascading failures between components- a key input to the system is directly estimated from historical failure data of the same Brazilian system. The consequences of failure are calculated based on the load and generation connected to all substations on a typical day, and the cost per hour of service failure is based on the highest energy cost observed in 2021 for the Brazilian system energy market.

The method provides a cost per hour for the likely cascade failure with the highest direct consequence (loss of revenue), as well as a static risk representing the direct loss per hour to the system operator for a complete service failure in Brazil, without taking into account the broader societal consequences. The simulation found a maximum probable loss (MPL RiskSM) from cascading failure events of US \$12.5 million per hour, which is roughly one-quarter of the static risk of US \$55.8 million per hour.

This method also measures the system's resilience to cascading failure events using the Lewis ScoreSM normalized scale. The Lewis ScoreSM ranges from zero to ten and has a "tipping point" of five. Below this tipping point any random failure on the network has the tendency to "blow up" into a LPHC event and the network is "fragile". Above the tipping point the network tends to naturally suppress the spread of failures, so consequences stay small and the network is "re-

silient". Simulations on the Brazilian system estimate its Lewis ScoreSM as 6.2, so the Brazilian Interconnection is resilient to cascading failure events. However, that score as well as MPL RiskSM could still be significantly improved by restructuring the network topology and hardening critical assets that tend to disproportionately participate in LPHC cascading failure events, as indicated in Figure 11 - Critical Assets Heat Map for the Brazilian Power Transmission System [12].1.

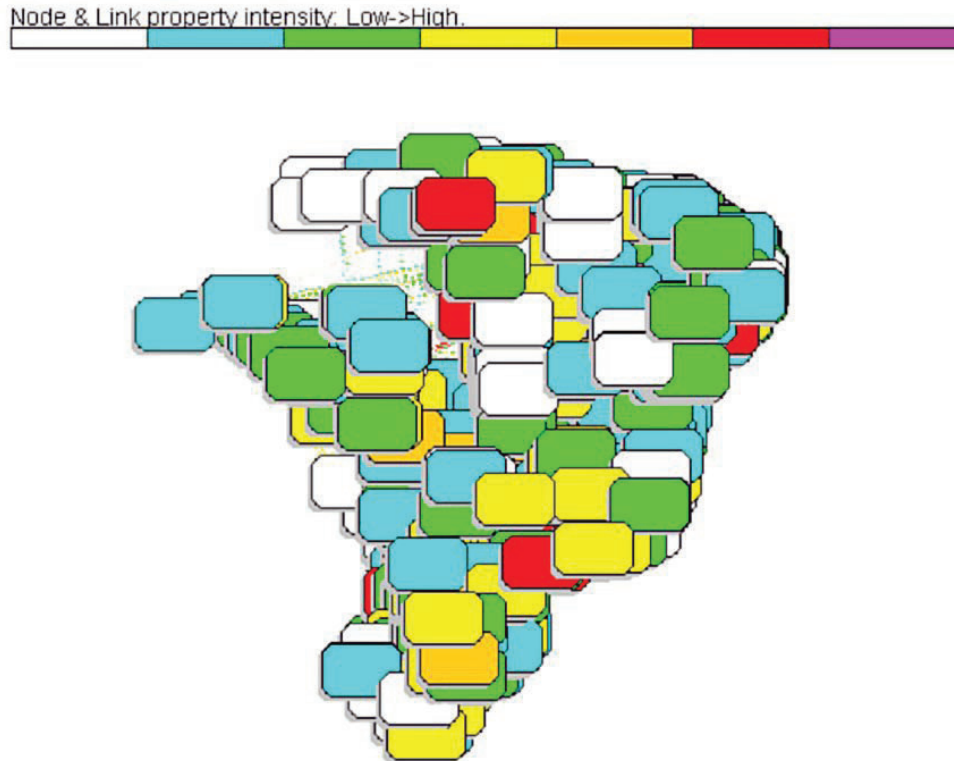


Figure 11 - Critical Assets Heat Map for the Brazilian Power Transmission System [12].

Utilities and communities, and larger regional systems, such as ERCOT, EIPC and WECC, as well as the nation and its regional partners, can benefit from application of an objective resilience methodology. As shown above, many federal agencies are exploring and developing resilience and related security approaches to the challenges of interdependency, Black Swan events, and cascading failures.

At the utility level, it is important for each stakeholder to take charge of their own resilience procedures. For example, local public utility authorities whether municipal or investor owned, can obtain their own internal measurements, and use these to inform their own engineering and investment priorities. They can also collaborate to look at systems at a larger scale, for example, combining assessments by a university and its surrounding locality or among co-owned water, power, and/or gas providers. Engineers will benefit from an identification of critical assets for cascade failures and relevant mitigation; financial planners can use financial risk metrics to evaluate the cost-benefits of mitigation for internal and external financial purposes; and emergency managers can use recovery times associated with LPHC events as a baseline for process improvements, for understanding risk faced by critical customers, and for risk mitigation through resource and recovery order planning. Those focused on energy transition can treat grid resilience as a tool to support that process and well as protect consumer populations.

CONCLUSIONS

This report discusses resilience standards for interconnected critical infrastructure, especially focused on power systems. It also discusses approaches to resilience established and embraced by related institutions, funded by the DOE and DOD, as well as elements of the Department of Homeland Security and Department of Commerce.

A probabilistic based resilience standard for the industry is deemed necessary for regulation and standardization. The ideal solution would effectively handle interdependent network failures, mitigate unpredictable “Black Swan” events (i.e. all-hazard failures), establish clear guidance on whether or not a network is adequately resilient, and would have a theoretical basis that is orthogonal and complementary to the dominant power systems engineering and modelling approach, that could be extended for water and other critical infrastructure systems. The presented method and the Lewis ScoreSM satisfy these criteria by providing practical, robust measurement for resilience to LPHC events, including an objective cascade resilience score, maximum probable financial loss, critical asset identification and prioritized mitigation for capital improvement planning, emergency management, and rate applications. Collectively, these provide a new toolset to augment day to day reliability with resilience to unanticipated, large-scale events.

APPENDIX

Definitions of Resilience in Selected US National Laboratories

US national laboratories associated with the DOE and DOD have recognized a need for resilience solutions for energy and defense infrastructure especially because of climate related disasters and grid related technical challenges associated with distributed energy. The focus of these national laboratories is less on community resilience and more on resilience approaches for energy and defense infrastructure, including a parallel focus on cyber infrastructure and to a lesser extent water infrastructure. In their approaches to the problem, some of the laboratories have proposed resilience methods for general use based on their definitions. We have noted those below.

Sandia National Laboratories

According to the Sandia National Laboratories, sponsored by DOE, Resilience is defined as “the ability to adapt to changing conditions and withstand and rapidly recover from disruptions. Resilience includes the ability to withstand and recover from deliberate attacks, accidents, or naturally occurring threats or incidents.” [49]. This can refer to physical systems, such as infrastructure, or social systems, such as communities or organizations. In the context of national security and emergency management, resilience refers to the ability of individuals, communities, and critical systems to withstand and recover from natural or man-made disasters.

Sandia National Laboratories has developed resilience metrics for the electric power system [50], following a Presidential policy directive defining the energy sector as a uniquely critical infrastructure [51], recognizing that most essential societal functions taken for granted are dependent on energy infrastructure. Communications, transportation, industrial production, banking and finance, and almost every aspect of modern life relies on energy availability and the continuous operation of the electrical power grid. Sandia’s proposed approach creates a correlation to associate different consequence categories with specific resilience metrics, dividing them into direct and indirect consequences, as shown in Table 1.

Table 2 - Consequence Categories VS Resilience Metrics from [51]

| | Consequence Category | Resilience Metric |
|----------|-----------------------------|---|
| Direct | Electrical Service | Cumulative customer-hours of outages Cumulative customer energy demand not served Average number (or percentage) of customers experiencing outage during a specified time period |
| | Critical Electrical Service | Cumulative critical customer-hours of outages Critical customer energy demand not served Average number (or percentage) of critical loads that experience an outage |
| | Restoration | Time to recovery Cost of recovery |
| | Monetary | Loss of utility revenue Cost of grid damages (e.g. repair or replace lines, transformers) Cost of recovery Avoided outage cost |
| Indirect | Community Functions | Critical services without power (e.g., hospitals, fire stations, police stations) Critical services without power for more than N hours (e.g., N > hours of backup fuel requirement) |
| | Monetary | Loss of assets and perishables Business interruption costs Impact on Gross Municipal Product (GMP) or Gross Regional Product (GRP) |
| | Other critical assets | Key production facilities without power Key military facilities without power |

Idaho National Laboratory

The Idaho National Laboratory (INL), sponsored by DOE, defines resilience as “the ability to anticipate, prepare for, and adapt to changing conditions and withstand, respond to, and recover rapidly from disruptions” [52]. This definition highlights the key components of resilience – the ability to anticipate potential disruptions, prepare for them in advance, and quickly adapt and recover when they do occur. INL’s focus is the resilience of critical infrastructure and systems, such as energy, transportation, and communications systems, to ensure the continuity of essential services during and after disruptions.

INL has developed an All-Hazards Analysis (AHA) framework [53] for use critical infrastructure organizations. AHA is a dynamic analysis framework that identifies dependencies and associated risks. The intention is to enable threat discovery and related decision support by providing decision-makers and emergency managers with a comprehensive view of interconnected infrastructure systems.

AHA offers an optimized framework to collect, store, analyze, and visualize critical infrastructure information. It uses a function-based approach to present information as nodes (infrastructure) and links (dependency relationships). AHA can learn to blend general and facility dependency profiles with new information and changes in network structures; this is intended to support modeling and analysis of consequences relating to threats and risks on an infrastructure and sector basis.

INL has also developed a methodology for cyber resilience that is commercializing with partners. The concept is a consequence-driven, cyber-informed engineering (CCE) methodology. CCE was developed because engineering methods traditionally used in the water and other critical infrastructure sectors do not adequately account for cyber-risk and “bolt-on” cybersecurity solutions designed for information technology systems do not work well for digital ICS. CCE’s goal is to improve Industrial Control Systems (ICS) cyber-resilience and reduce the potential for severe consequences and threats in cyber-enabled sabotage [54].

Argonne National Laboratory

The Argonne National Laboratory, sponsored by DOE, presents two aspects of the definition of resilience, one that considers only “after the adverse event” and the second one that also considers “before the adverse event,” including assets, resistance, protection, anticipation, and preparedness. An accepted definition for resilience “after the adverse event” is “the capacity of a system to absorb disturbance, undergo change, and retain essentially the same function, structure, identity, and feedbacks.” Regarding also “before the adverse event,” an accepted definition is the ability to minimize the costs of a disaster, to return to a state as good as or better than the status quo ante, and to do so in the shortest feasible time. Resistance is used to mean the ability to withstand a hazard without suffering much harm. Resilience in this paper will include resistance but will also include the ability to recover after suffering harm from a hazard [55].

Lincoln National Laboratory

A proper definition of Resilience from Lincoln National Laboratory (LNL), sponsored by DOD, could not be found. However, LNL has performed a study evaluating and applying a resilience framework to military installations for the DOD [56]. According to the DOD guidance [57], resilience is defined as “the ability to prepare for and recover from energy disruptions that impact mission assurance on military installations.” In the LNL study, availability and reliability were the key metrics to measure different energy resilience solutions and ensure continuous critical mission operations.

Pacific Northwest National Laboratory

Pacific Northwest National Laboratory (PNNL), sponsored by DOE, defines resilience as the ability of a system, organization, or community to prepare for, withstand, adapt to, and recover from disruptions, whether they are acute shocks or chronic stresses. PNNL just released a report to define a framework for quantitative evaluation of resilience solutions to determine the value of resilience for a particular site [58]. The report uses a broader definition of resilience, applied by the Federal Energy Management Program’s Technical Resilience Navigator (TRN): “the ability to anticipate, prepare for, and adapt to changing conditions and to withstand, respond to, and recover rapidly from disruptions through adaptable and holistic planning and technical solutions”. The TRN is a free software that helps organizations manage the risk to critical missions from disruptions in energy and water services. It provides a systematic approach to identifying energy and water resiliency gaps and developing and prioritizing solutions that reduce risk.

REFERENCES

For a complete listed of article reference, please see the link below to our online publication forum.

Suggested citation: Mouco, A. & Ruddell, B. L., Ginsburg, S. (2023) Resilience to High Consequence Cascading Failures of Critical Infrastructure Networks. (Report No. IHS/CR-2023-1015). The Sam Houston State University Institute for Homeland Security. <https://doi.org/10.17605/OSF.IO/5R2H6>
One Step Ahead, April 2024, 50-76.

HONORABLE MENTION

This round, we received 28 industry-oriented papers on a multitude of infrastructure related topics. Since printing is limited, The Institute for Homeland Security at Sam Houston State University would like to give honorable mention to the following:

German, A. (2023) Supply chain Risks at US/Mexico Border. (Report No. IHS/CR-2023-1008). The Sam Houston State University Institute for Homeland Security. <https://doi.org/10.17605/OSF.IO/VCWG2>

Clay, E. (2023) The Rise of Workplace Violence: Addressing Healthcare's Greatest Threat Driving Transformational Change in Healthcare Security. (Report No. IHS/CR-2023-1004). The Sam Houston State University Institute for Homeland Security. <https://doi.org/10.17605/OSF.IO/J8EBV>

Mastrangelo, M. (2023) Improving Texas Homeland Security: A Practical Framework for Joint Hospital -Chemical Industry Emergency Planning. (Report No. IHS/CR-2023-1019). The Sam Houston State University Institute for Homeland Security. <https://doi.org/10.17605/OSF.IO/U4DFR>

Munoz, G. (2023) Safe & Secure Addressing Workplace Violence. (Report No. IHS/CR-2023-1009). The Sam Houston State University Institute for Homeland Security. <https://doi.org/10.17605/OSF.IO/SA7R3>

The Institute for Homeland Security

Future Topics in Research

Enhancing Crisis Resilience in Healthcare Supply Chains: A Strategic and Tactical Framework for Crisis Management Readiness Assessment.

Practical Artificial Intelligence (AI) Guide for the Texas Power Grid for Normal and Emergency Operations, including Cybersecurity.

Examining the Role of Drones in Emergency Management Services across Texas: Current Knowledge, Guidance, and Future Directions.

Geographic Information System (GIS) Analysis of the Patterns of Failures of Public Water and Wastewater Systems in Texas in Relation to Demographics.

A Unique Win-Win: Bolstering Texas' Energy Security by Leveraging Infrastructure To Effectively Decarbonize.

Public Health and Healthcare: A shared goal of HCID Preparedness.

A Playbook for Cyber Attack Operational Response in Healthcare.

Leveraging Artificial Intelligence for Crisis Management Readiness.

Assessing the Feasibility of Portable Solar Charging Systems for Electric Vehicles: A Sustainable Approach to Alleviate Grid Load.


Development of an Intelligent Anti-Scamming System for Wire Transfer.

Workplace Violence: Developing a comprehensive workplace violence prevention program that complies with civil law.

Benchmarking Best Practices for Preventing Phishing Cybersecurity Breaches in Hospitals and Health Organizations in South Texas.

For More Information on Events, Training or Research Opportunities find us at ihsonline.org



The background of the page is a photograph of a university campus. In the foreground, there is a low brick wall. Behind it, several large, leafy trees with green and some yellowing leaves are visible. The sky is a clear, bright blue. In the upper left corner, there are some branches with leaves hanging down. The overall scene is bright and sunny.

The Institute for Homeland Security at Sam Houston State University is focused on building strategic partnerships between public and private organizations through education and applied research ventures in the critical infrastructure sectors of Transportation, Energy, Chemical, Healthcare, and Public Health.

The Institute is a center for strategic thought with the goal of contributing to the security, resilience, and business continuity of these sectors from a Texas Homeland Security perspective. This is accomplished by facilitating collaboration activities, offering education programs, and conducting research to enhance the skills of practitioners specific to natural and human caused Homeland Security events.



Criminal Justice Center
SAM HOUSTON STATE UNIVERSITY

MEMBER THE TEXAS STATE UNIVERSITY SYSTEM