Christian Keyes

Luke Gonzalez

Natalie Webb

HAZ 458

Dr. Rodrigue

08 Dec 2023

## Introduction

Changes to the social fabric imprinted by the industrial revolution have reverberated to nearly every corner of civilization. When extrapolating the advancements made in industry, communication, and infrastructure, it is apparent that in a relatively short time frame; life on earth has changed drastically. Upon considering the novelty of this experience it is crucial to contextualize that much of the observed growth in America has occurred in the past 100 years alone. Amidst this shift from a largely agrarian culture, to a highly modernized city structure, there have been a host of advancements that have made life easier for the average person. Put simply, technology can be accredited for most of the conveniences that are enjoyed in the 21st century. However, the same technologies that have made life easier, have inherently made modern life extremely vulnerable. In other words, while the connections weaved together by power grids and communication systems are mutually beneficial in ideal conditions, in the event of a disaster or natural hazard they can lead to cascading destruction. Pertinently, such vulnerabilities have also become the target of attacks both nationally and globally. With such an emphasis placed on critical infrastructure, there is a ripening need for research and interpretation in the field of cyber attacks. To achieve adequate insulation against attack, the critical infrastructure sector must adapt to become more resilient by conducting regular audits, implementing end-to-end practices, and carrying out proper cyber hygiene.

## Defining Critical Infrastructure

To properly assess the state of cyber security in America, it is pertinent to first define the importance of critical infrastructure. Critical infrastructure is the backbone of our society as we know it. To say that critical infrastructure is taken for granted, would be a wholesale understatement. Ranging from power grids, to transportation matrices, and essential communication systems, all these technologies ensure that society is able to operate smoothly. While the critical classification is implied with more common services, other sectors like nuclear power, wastewater systems, and information technology sectors all fit within this definition. Especially here in America, these modern services are trivialized because of their ubiquity and reliability. In considering the role of critical infrastructure, the vulnerabilities to their systems must be accounted for. Interruptions, failures, or dread to consider, attack; all pose serious hazards to civilizations and human life. The margins between smooth operation and failure are all that stand between society unravelling. According to research reported by the Federal Energey Regulatory Commision, failures; incidental or coordinated, to just nine of 55,000 power transmitters could result in coast to coast blackouts in America (FERC). And it is through this lens that critical infrasturue graduates to a matter of national security. Safeguarding critical infrastructure is integral in maintaining the nation's economic stability, safety, and sovereignty. Recognizing its vitality, policymakers and emergency planners can enhance protections and emergency response plans to prevent cascading breakdowns.

## Natural Hazard Vulnerabilities and the Texas Winter Storm

Critical infrastructure faces a multifaceted range of vulnerabilities that collectively challenge its resilience and security. These vulnerabilities include a heavy reliance on digital systems, interconnectedness between sectors, aging infrastructure with outdated components, the potential for human error in managing digital systems and responding to incidents, and the increasing impact of climate change-induced natural hazards. The pervasive use of digital technology in critical systems exposes them to a variety of risks, including cyber threats, technical glitches, and system failures, while the interdependencies among sectors mean that disruptions in one area can lead to widespread consequences. Aging infrastructure compounds these issues, making it susceptible to both cyber threats and physical damage. Moreover, the potential for human error further magnifies these risks. Climate change exacerbates the situation by increasing the frequency and severity of natural disasters, which can inflict substantial damage on digital infrastructure and disrupt essential services.

The Texas winter storm of 2021 and the subsequent power grid failures serve as a poignant example of these vulnerabilities in the face of natural hazards. While the winter storm itself was a natural disaster, its impact on the power grid highlighted several crucial aspects of digital vulnerabilities. In today's interconnected world, critical infrastructure, including power grids, heavily relies on digital technology for monitoring, control, and distribution. The Texas power grid is no exception, with digital systems playing a pivotal role in managing electricity generation and distribution. However, this dependency on digital infrastructure exposed vulnerabilities that became glaringly evident during extreme weather events. Severe winter storms can disrupt digital infrastructure by causing frozen equipment, ice accumulation on power lines, and other weather-related issues, resulting in power outages. Furthermore, the digitalization of critical infrastructure has introduced complexities and interdependencies that can lead to cascading failures when one component fails, resulting in widespread outages. The Texas power grid's lack of redundancy and resilience in the face of extreme weather underscores the importance of robust backup mechanisms and contingency plans. The loss of electricity during the winter storm highlighted how deeply embedded digital technology is in our daily lives, impacting essential services like heating, communication, transportation, and healthcare. This dependence on digital infrastructure underscores the need for comprehensive cybersecurity measures to ensure resilience and security against not only natural disasters but also potential cyberattacks targeting these vulnerabilities.

## The Hazards of Cyber-Attacks

The hazards associated with cyber-attacks are vast and continuously evolving, presenting an ever-increasing threat to critical infrastructure and national security. Cyber-attacks can disrupt essential services, compromise sensitive data, and inflict severe financial and reputational damage on organizations. These attacks exploit vulnerabilities in digital systems, leaving no sector immune to potential breaches. One of the prime examples of this hazard was the SolarWinds cybersecurity breach, which began in September 2019 and unfolded as one of the most extensive and sophisticated hacking campaigns in recent history. Attributed to the Russian Foreign Intelligence Service, this breach involved the injection of malicious code into SolarWinds' Orion software updates, which were unknowingly distributed to approximately 18,000 customers, including high-value targets like federal government agencies. The compromised updates acted as a backdoor, granting threat actors remote access to affected systems, allowing for further exploitation.

The discovery of the SolarWinds breach and subsequent response efforts shed light on the critical importance of cybersecurity vigilance and preparedness. FireEye and Microsoft played pivotal roles in detecting and reporting the intrusion in November 2020, prompting swift action. Federal agencies were promptly informed of unauthorized access to their unclassified systems, leading to the implementation of mitigation measures. The Department of Homeland Security's Cybersecurity and Infrastructure Security Agency (CISA) issued an emergency directive, and the Cyber Unified Coordination Group coordinated a government-wide response. Congressional hearings were convened to gather insights into the SolarWinds hack, IT supply chain security, threat actors, and future cybersecurity measures. The Government Accountability Office (GAO) has maintained its examination of the breach, underscoring the urgent need for improvements in the nation's cybersecurity posture—a concern that has persisted since 1997. These incidents serve as stark reminders of the hazards posed by cyber-attacks and emphasize the critical importance of bolstering our cyber defenses to safeguard critical infrastructure and national security.

In addition to the SolarWinds breach, another significant example illustrating the hazards of cyber-attacks is the Colonial Pipeline Ransomware Attack that occurred in 2021. This attack targeted the Colonial Pipeline, a critical piece of infrastructure responsible for transporting a substantial portion of the East Coast’s fuel supply. DarkSide, a ransomware group, was responsible for the attack, which led to the temporary shutdown of the pipeline. The attackers encrypted the company's data and demanded a ransom for its release, disrupting fuel distribution across several states and causing panic buying and fuel shortages. This incident highlighted the vulnerability of critical infrastructure to ransomware attacks and underscored the potential for cybercriminals to impact not only digital systems but also the physical supply chain, posing significant threats to national security and public safety. The Colonial Pipeline attack serves as another compelling example of the urgent need for robust cybersecurity measures and enhanced resilience in safeguarding our critical infrastructure against evolving cyber threats.

## Economic Implications

It is also imperative to look at this hazard from an economic and management perspective. According to a study done in 2019 by the Ponemon Institute LLC, “90% of organizations that rely on operational technology, including critical infrastructure providers, experienced a cyberattack,” half of which was forced to shut down because of an attack. Which is interesting, because most organizations and companies are not willing to reveal that they were attacked or provide information on how much damage was caused. Additionally, even though “60% of organizations in the technology sector are worried about disruptive cyber attacks” only “48% attempt to quantify the damage,” and even those that do, fail to include both direct and indirect impacts. Also, because cyber attacks are still a relatively new threat, there is a lack of clarity on what costs should actually be considered, as well as what economic framework should be used to quantify the damage. Plus, it is extremely important for there to be a layer of secrecy around the level of cybersecurity critical infrastructure has, because we do not want information on our infrastructure’s weaknesses to get into the wrong hands. Therefore, specific data on cyber attacks is difficult to find, but there are some overall averages for the global and U.S. economy. Estimates show that “cybercrime costs the global economy up to $575 billion annually” and “extracts up to 20% of the value created by the internet” (Lis and Mendel, 2019). According to the U.S. Treasury Department, in 2021, U.S. financial institutions lost around $1.2 billion, which tripled the amount in 2020, which was $416 million (Pagan and Iribarren, 2023). Based on recent reports, these numbers have only been growing through 2022 and 2023, and will most likely continue increasing in years to come due to the increased amount of cyber attacks predicted to occur in the future.

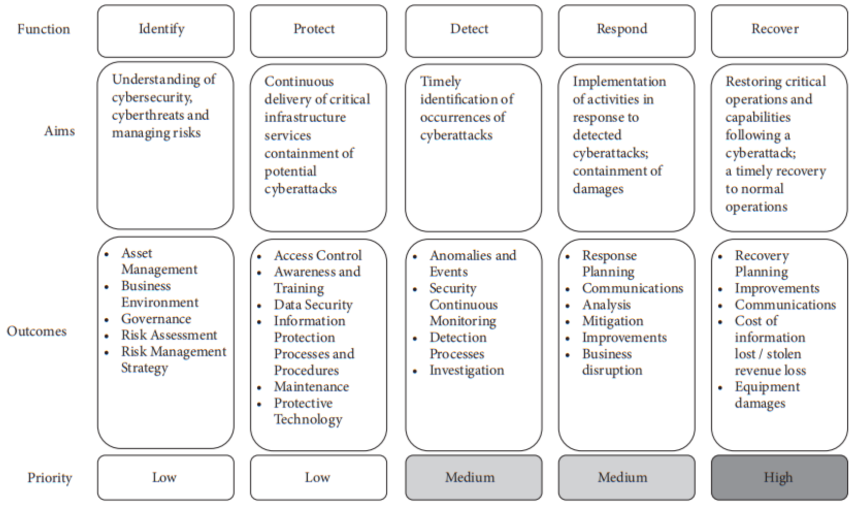
## Social Implications

On top of the economic impacts, there are of course social impacts. For the most part, cyber-attacks are more likely to do psychological, rather than physical harm. First and foremost, these attacks create widespread anxiety among everyday people, as well as the actual employees who are on the front lines. Cyber attacks are such a new threat that it feels very unknown and scary to most people. It is also a threat that is developing so fast, that it is hard to tell if we are staying ahead or even keeping up with it. The stress and fear for the employees especially is important to note. Management needs to ensure it has a risk management plan that doesn't put a lot of pressure on individual employees to not make a single mistake. Human error must be taken into consideration when setting up defenses against cyber threats. Furthermore, the direct impacts that cyber attacks have on the people that it affects can range from minor inconveniences to life threatening situations. It could be that some people just can't access their records or pay their utility bills, or they literally are cut from the world and common resources like fuel, food, power, and water.

## Possible Solutions

When it comes to critical infrastructure, it is very difficult to actually come up with solutions to protect them from cyber threats. For instance, although most of our infrastructure needs drastic technological updates because they were designed before cyber attacks were even a thing, it is not very easy to actually do. The only way most infrastructures can be updated is if they are shut down for a period of time, and many operators cannot afford that downtime. It would also indirectly and directly impact citizens and their everyday lives. Imagine if the power grid had to be shut down for a day or two in order to install an upgrade. It would be a shock to the system to say the very least. So this detail, along with many others, makes finding a solution difficult. However, that does not mean solutions do not exist.

In order to really come up with a solution to a hazard that is basically inevitable, one must look at it from the managerial and technological point of view. Critical infrastructure organizations need to have a risk and security management framework as well as integrate layers of defense into the technology. An example of a possible risk management plan that organizations can utilize is the “Identify, Protect, Detect, Respond, Recover” (IPDRR) framework. This is a holistic risk and management approach that aims “to help organizations to align their cybersecurity efforts with business requirements, risk tolerances and resources” (Lis and Mendel, 2019). It is important to note that this strategy is not a one-size-fits-all approach, but rather a tool that can be used to help guide managers to figure out what plan would be best to implement for their specific company or organization. Figure 1 and Figure 2 depict how the framework actually works, and what could be included and how many things should be considered.



| Function | Identify | Protect | Detect | Respond | Recover |
|---|---|---|---|---|---|
| Aims | Understanding of cybersecurity, cyberthreats and managing risks | Continuous delivery of critical infrastructure services containment of potential cyberattacks | Timely identification of occurrences of cyberattacks | Implementation of activities in response to detected cyberattacks; containment of damages | Restoring critical operations and capabilities following a cyberattack; a timely recovery to normal operations |
| Outcomes | • Asset Management<br>• Business Environment<br>• Governance<br>• Risk Assessment<br>• Risk Management Strategy | • Access Control<br>• Awareness and Training<br>• Data Security<br>• Information Protection Processes and Procedures<br>• Maintenance<br>• Protective Technology | • Anomalies and Events<br>• Security Continuous Monitoring<br>• Detection Processes<br>• Investigation | • Response Planning<br>• Communications<br>• Analysis<br>• Mitigation<br>• Improvements<br>• Business disruption | • Recovery Planning<br>• Improvements<br>• Communications<br>• Cost of information lost / stolen revenue loss<br>• Equipment damages |
| Priority | Low | Low | Medium | Medium | High |

**Figure 1. The “Identify, Protect, Detect, Respond and Recover” framework**
Source: (Mendel, 2018).

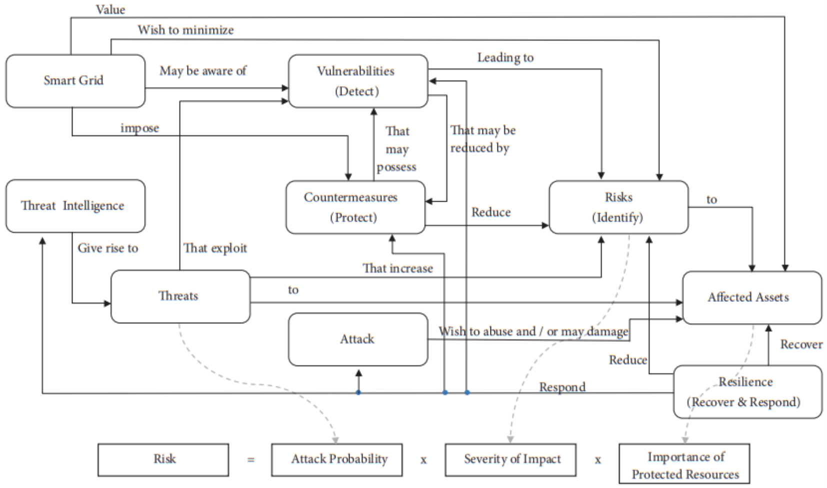


**Figure 2. Operationalizing the IPDRR framework**
Source: (Mendel, 2018).

There are many technological solutions out there, but for the sake of this paper we are going to focus on two: blockchain technology and end-to-end cybersecurity. Implementing blockchain technology into critical infrastructure's software could provide a strong level of protection while also being cost-effective. Basically, this technology only allows users with specific permissions to access the data (Lis and Mendel, 2019). It provides an extra layer of security by maintaining two distinct ledgers, "a ledger with individually encrypted data" and "a transaction ledger which stores encryption access keys to the related data" (Lis and Mendel, 2019). This strategy is also a great option because it "secures the complete history of data transactions" (Lis and Mendel, 2019). Additionally, if a security breach does occur, this technology can facilitate both data recovery and data integrity. End-to-end cybersecurity, on the other hand, is basically where a third party provides a range of technologies and services to identify and address vulnerabilities within the infrastructure. Some examples of these services are disaster recovery, data protection, unified threat detection and response technologies, secure cloud architecture, and conducting a cyber resiliency health assessment (Lis and Mendel, 2019).

This technological strategy takes the pressure off the managers of the organizations and gives the responsibility to people who specialize in the issue.

## Conclusion

Although this threat is prominent and growing, the future is not entirely bleak. The White House has acknowledged cyber attacks as a serious threat and have come up with a National Cybersecurity Strategy in March of 2023. One of the first pillars discussed in the document is about defending critical infrastructure. Their plan includes establishing cybersecurity regulations, harmonizing new and existing regulation, integrating Federal cybersecurity centers, updating Federal incident response plans, and modernizing Federal defenses (The White House, 2023). Therefore, if our government follows through with this plan and critical infrastructure providers fold cybersecurity into the fabric of their organization in both the managerial and technological means, our future will definitely be a little brighter.

## Executive Summary

- ❏ There has been a sharp increase in demand for understanding in the realm of cybersecurity, and subsequently cyber attacks
- ❏ The same technologies that make our lives easy, also create vulnerabilities
- ❏ Critical infrastructure vulnerabilities: heavy reliance on digital systems, interconnectedness between sectors, aging infrastructure prone to cyber threats and physical damage, human error magnifying risks, and heightened impact from climate change-induced natural hazards.
- ❏ Texas winter storm of 2021: showcased digital vulnerabilities in critical infrastructure, notably in power grids heavily dependent on digital technology.
- ❏ Impact on power grids: severe weather disrupting digital infrastructure, causing outages and revealing complexities leading to widespread failures.
- ❏ Importance of resilience: highlighted the necessity for robust backup measures, contingency plans, and comprehensive cybersecurity to protect essential services against natural disasters and potential cyber threats.
- ❏ Attacks on operational technology: 90% of critical infrastructure organizations faced attacks, with half forced to shut down; however, many incidents remain undisclosed or unquantified, complicating cost assessments.
- ❏ Cybercrime costs the global economy up to $575 billion annually, extracts 20% of internet value; in 2021, U.S. financial institutions lost $1.2 billion, tripling the previous year's losses, with continual growth projected due to increasing cyber threats

## Bibliography

Biden, Joe. “National Cyber Workforce and Education Strategy - the White House.” *The White House*, 1 Mar. 2023, www.whitehouse.gov/wp-content/uploads/2023/07/NCWES-2023.07.31.pdf.

CopyCEI. “The Consequences of Cyber Attacks and Their Impact on Cybersecurity.” *CEI*, 9 Mar. 2023, copycei.com/the-consequences-of-cyber-attacks-and-their-impact-on-cybersecurity/#:~:text=The%20greatest%20concern%20of%20a,be%20used%20by%20terrorist%20organizations.

“FERC: Nationwide Blackout Could Happen If 9 Key Substations Are Knocked Out.” *Utility Dive*, https://www.utilitydive.com/news/ferc-nationwide-blackout-could-happen-if-9-key-substations-are-knocked-out/238630/. Accessed 8 Dec. 2023.

Lis, Piotr, and Jacob Mendel. “Cyberattacks on Critical Infrastructure: An Economic Perspective.” *Economics and Business Review*, Sciendo, Apr. 2019, ideas.repec.org/a/vrs/ecobur/v5y2019i2p24-47n2.html.

Pagan, Cassandra. “The Economic Consequences of Coordinated Cyber-Attacks.” *IHS Markit*, 4 Apr. 2023, www.spglobal.com/marketintelligence/en/mi/research-analysis/the-economic-consequences-of-coordinated-cyberattacks.html.

Dawson, M., Bacius, R., Gouveia, L. B., & Vassilakos, A. (2021). Understanding the Challenge of Cybersecurity in Critical Infrastructure Sectors. *Land Forces Academy Review*, *26*(1), 69–75. https://doi.org/10.2478/raft-2021-0011

*The Great Texas Freeze: February 11-20, 2021*. (2023, February 23). National Centers for Environmental Information (NCEI). https://www.ncei.noaa.gov/news/great-texas-freeze-february-2021#:~:text=On%20February%2011%2D20%2C%202021

U.S. Government Accountability Office. (2021, April 22). *SolarWinds Cyberattack Demands Significant Federal and Private-Sector Response (infographic)*. Www.gao.gov. https://www.gao.gov/blog/solarwinds-cyberattack-demands-significant-federal-and-private-sector-response-infographic