Hazards Associated with Cyber Threats to Infrastructure

Christian Keyes, Luke Gonzalez,
& Natalie Webb

Introduction to Key Points

❑ Cybersecurity is a rapidly growing sector

❑ Increased demand for understanding in this field…

❑ The importance of robust cybersecurity defense systems has been highlighted at the corporate, national and supranational levels

❑ The technology that makes our lives easy, also creates vulnerability

What is Critical Infrastructure?

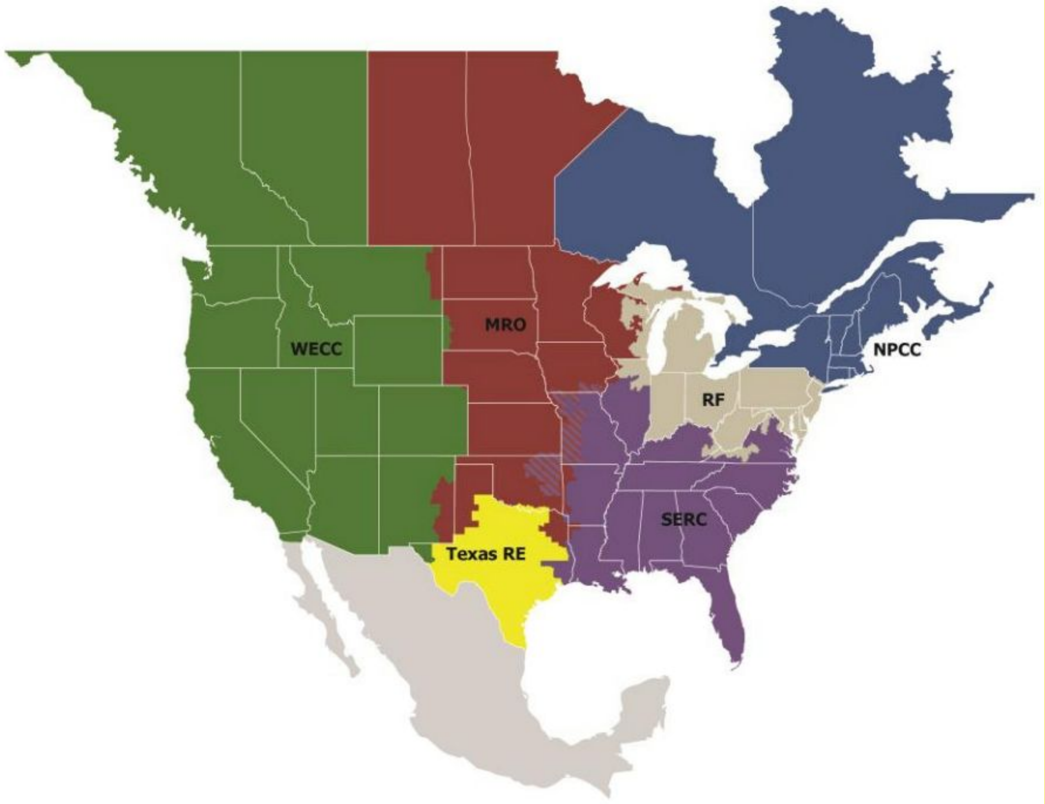
“The assets, systems, and networks that provide functions necessary for our way of life”- CISA

Background and Context

There are 16 critical infrastructure sectors whose assets, systems, and networks, whether physical or virtual, are considered so vital to the United States that their incapacitation or destruction would have a debilitating effect on security, national economic security, national public health or safety, or any combination thereof. - NIPP

- ➢ Chemical Sector
- ➢ Commercial Facilities Sector
- ➢ Communications Sector
- ➢ Critical Manufacturing Sector
- ➢ Dams Sector
- ➢ Defense Industrial Base Sector
- ➢ Emergency Services Sector
- ➢ Energy Sector
- ➢ Financial Services Sector
- ➢ Food and Agriculture Sector
- ➢ Government Facilities Sector
- ➢ Healthcare and Public Health Sector
- ➢ Information Technology Sector
- ➢ Nuclear Sector
- ➢ Transportation Systems Sector
- ➢ Water and Wastewater Systems Sector

Connectivity → Vulnerability



Infrastructure Vulnerabilities

Inadequate cybersecurity in critical infrastructure sectors can expose the country to debilitating attacks, threatening national security, public health, safety, as well as social & economic stability.

- ➢ **Digital Dependency:** Sectors heavily rely on digital systems, exposing them to cyber threats, glitches, and failures.
- ➢ **Interconnectedness:** Disruptions in one sector can cascade to others, caused by cyberattacks or natural disasters.
- ➢ **Aging Infrastructure:** Outdated components are vulnerable to both cyber threats and physical damage.
- ➢ **Human Error:** Mistakes in digital systems and incident responses pose risks.
- ➢ **Climate Change Impact:** Increased natural hazards can damage digital infrastructure and disrupt services.

Hazards of Digital Infrastructure

Cyber Attacks:

- ➢ Vulnerability of digital critical infrastructure to cyber attacks, including hacking, malware, and denial-of-service attacks.
- ➢ The risk of disruption or compromise of essential services, such as power grids and transportation systems.

Natural Disasters:

- ➢ Exposure to natural hazards like hurricanes, earthquakes, floods, and wildfires that can damage digital infrastructure.
- ➢ Potential for widespread service outages, affecting communication, transportation, and emergency response.

Interdependency Risks:

- ➢ The interconnected nature of critical infrastructure systems, where disruptions in one sector can cascade into others.
- ➢ The challenge of managing risks and dependencies across various digital infrastructure components.

Data Breaches and Privacy Concerns:

- ➢ The risk of data breaches and unauthorized access to sensitive information stored within digital infrastructure.
- ➢ Concerns related to privacy, data protection, and regulatory compliance in the event of a breach.

Resilience and Recovery Challenges:

- ➢ Difficulty in quickly restoring digital infrastructure after cyber attacks or natural disasters.
- ➢ The need for robust disaster recovery plans, redundancy, and cybersecurity measures to enhance resilience.

Costly Remediation and Downtime:

- ➢ The financial burden associated with addressing vulnerabilities, recovering from incidents, and upgrading digital infrastructure.
- ➢ Potential economic losses due to extended downtime and reduced productivity during recovery efforts.

Case Studies and Examples

SolarWinds - Orion IT software Cybersecurity Breach (2020)

Sophisticated Cybersecurity Breach

- ❑ SolarWinds breach identified as a highly complex hacking campaign.
- ❑ Russian Foreign Intelligence Service attributed to the attack.

Infiltration through Software Updates

- ❑ Malicious code injected into SolarWinds' Orion software updates.
- ❑ Distributed to around 18,000 customers, including government agencies.

Exploiting the Backdoor

- ❑ Compromised updates provided threat actor with remote access and allowed unauthorized entry and exploitation of affected systems.

Discovery and Response

- ❑ FireEye detected intrusion in November 2020.
- ❑ Microsoft reported breaches in its cloud platforms.
- ❑ Federal agencies informed of unauthorized access, leading to mitigation efforts.

Government-Wide Coordination

- ❑ CISA issued an emergency directive to federal agencies.
- ❑ Cyber Unified Coordination Group activated for a coordinated response.

Digital Vulnerabilities Highlighted by Texas Winter Storm (2021)

Dependency on Digital Infrastructure

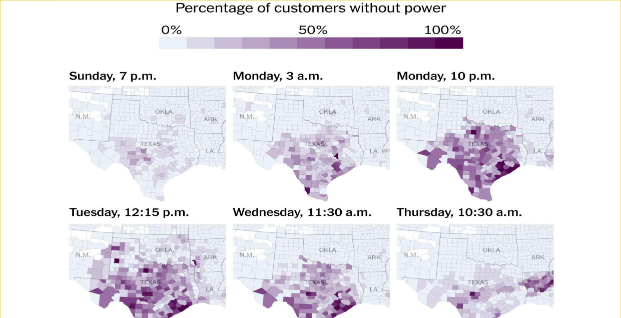
- Most critical infrastructure relies on digital technology for monitoring and control.
- Power grids use digital systems for electricity management.

Vulnerability to Extreme Weather

- Severe winter storms can disrupt digital infrastructure.
- Frozen equipment or ice on power lines can impact these digital-dependent systems.

Cascading Failures

- Interconnected digital components can lead to widespread outages.
- Failures in one part of the grid trigger a domino effect.



Percentage of customers without power

Sunday, 7 p.m.

Monday, 3 a.m.

Monday, 10 p.m.

Tuesday, 12:15 p.m.

Wednesday, 11:30 a.m.

Thursday, 10:30 a.m.

Lack of Redundancy and Resilience

- Digital systems require backup mechanisms.
- Resilience planning essential for coping with extreme weather.

Impacts on Daily Life

- Loss of electricity affects heating, communication, transportation, healthcare.
- Highlighting reliance on digital infrastructure for daily necessities.

Lessons for Cybersecurity

- Emphasizes the need for robust cybersecurity in digital infrastructure.
- Protection against natural disasters and cyber threats in the digital age.

Cyber Attack on Ukraine's Power Grid (Dec. 2015)

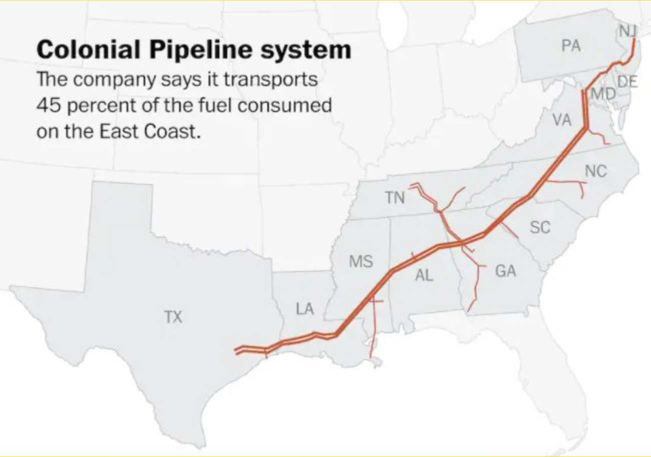
Attack Details

- Ukrainian capital Kyiv
- **Impact:** Over 250,000 Ukrainians left without electricity
- Widely attributed to Russian state-sponsored hackers
- **Initial Compromise:** Phishing emails targeting power company employees
- **Malware:** BlackEnergy and KillDisk malware used for intrusion and data destruction.
- Highlighted the potential for state-sponsored cyber warfare in future wars.

Case Studies Cont.

Cyber Attack:

Colonial Pipeline Ransomware Attack (2021)
In May 2021, the Colonial Pipeline, one of the largest fuel pipelines in the U.S., was hit by a ransomware attack carried out by the DarkSide hacking group (FBI, 2021). The attack disrupted fuel supplies to the East Coast, leading to gas shortages and highlighting the vulnerability of critical energy infrastructure to cyber threats.


Colonial Pipeline system
The company says it transports 45 percent of the fuel consumed on the East Coast.
PA
NJ
DE
MD
VA
NC
TN
SC
MS
AL
GA
TX
LA

Natural Hazards:

California Wildfires: California has experienced a series of devastating wildfires in recent years. These wildfires have at times threatened critical infrastructure such as power lines, leading to planned power outages to prevent fires. In some cases, wildfires have damaged or destroyed infrastructure, impacting communities and utility services. (Ex. Paradise,CA)

Hurricane Laura (2020): Hurricane Laura struck the Gulf Coast in August 2020, causing significant damage to infrastructure in Louisiana and Texas. The hurricane disrupted oil and gas production, leading to the shutdown of refineries and chemical plants. This demonstrated the vulnerability of energy infrastructure to natural disasters.

Economic Impact - Limitations

- **Data availability** = severely limited
  - Not many firms and organizations are willing to reveal that they were attacked or share information on the extent of the damage
- **60%** of organizations in the technology sector are worried about disruptive cyber attacks
  - **Only 48% attempt to quantify the damage**
    - Not likely to reflect the full picture - only consider the direct impact
  - Lack of clarity in which costs and benefits should be considered
  - Lack of tools and frameworks that could be readily applied to such analysis
- **National security** may require a layer of secrecy around cybersecurity/cyber attacks in the case of critical infrastructure
- **The US Treasury Department**
  - Loss of **$1.2 billion** to US financial institutions in **2021**
    - Tripling its 2020 level of $416 million

Social and Economic Impact

Direct Costs:

- Operational disruption, replacement or upgrading of damaged goods, equipment, and infrastructure
- Business income disruptions
- Insurance charges
- Intellectual property (IP) losses
- Recovery process
- Risk assessment
- Damage to trade name
- Lost customer relationships/contracts
- IT staff and external contractors working to bringing organization systems back to full functionality
- Legal complaints/security product license fees
- Loss of human life and health

Indirect Costs

- A decline in future revenues
- Insurance
- Market failures = may also impact cyber security regulations which have a consequent economic effect
- Government activities associated with the cyber-attack
- Lost productivity
- Privacy violations and future privacy protection
- The recovery process
- Increased cyber security investment
- Stock market losses
- Loss of investors

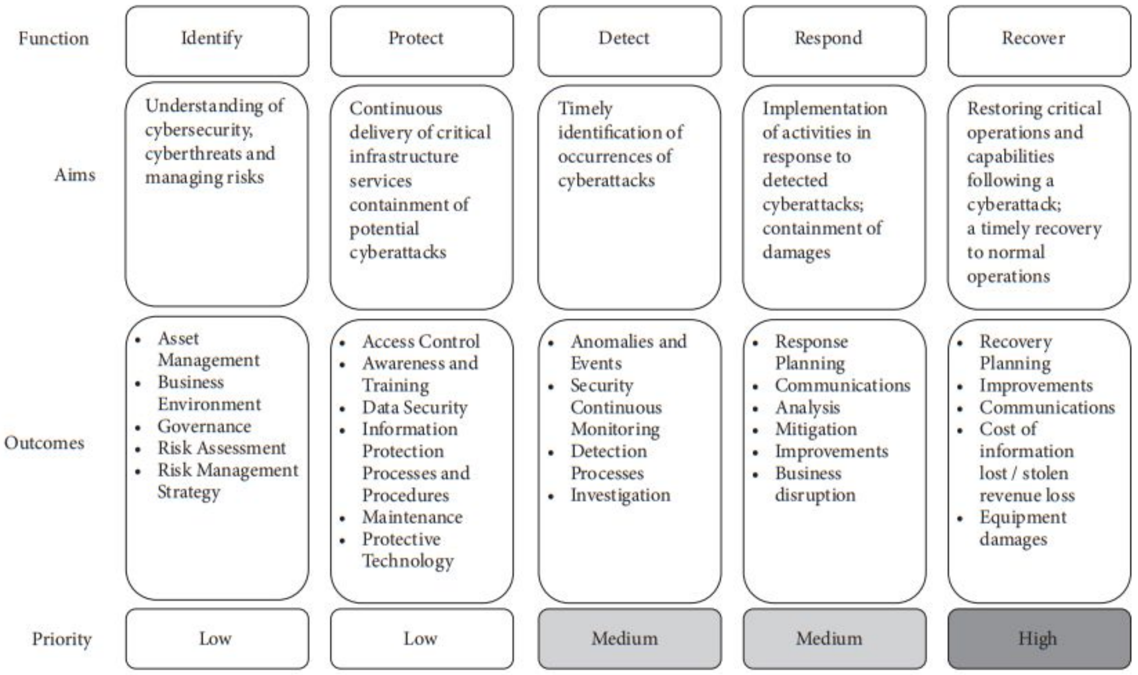
Possible Economic & Insurance Impact

- Severe, yet plausible cyber-attack against the US Power-grid = **$240 billion**
  - Possibly even rising to more than $1 trillion
- Report from Lloyd's and the University of Cambridge's Centre for Risk Studies - Business Blackout:
  - Attackers are able to inflict physical damage on **50 generators**
    - Supply power to the electrical grid in the Northeastern US
  - This triggers a wider blackout = leaves **93 mill people** without power
- Insurance claims arise in over 30 lines of insurance
  - Total insured losses = **$20 billion**
  - Most extreme version = $70 billion

Social Impact

- **Consumer mistrust**
  - 2 out of 3 Americans said they were worried about their information being breached during the 2020 holiday season
- **Psychological harm**
  - Widespread anxiety
  - Loss of confidence in cyber/technology
  - Increase stress and fear in employees
    - Afraid of messing up the protocols they need to routinely follow
- **Widespread disruption**
  - In 2019, 22 towns in Texas sharing a software vendor were the target of a cyber attack = residents could not access records or pay utility bills
- **Changing regulatory landscape**
  - Puts pressure on businesses and has an impact on the customer experience

Possible Solutions (Management)



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 • Business Environment • Governance • Risk Assessment • Risk Management Strategy	• Access Control • Awareness and Training • Data Security • Information Protection Processes and Procedures • Maintenance • Protective Technology	• Anomalies and Events • Security Continuous Monitoring • Detection Processes • Investigation	• Response Planning • Communications • Analysis • Mitigation • Improvements • Business disruption	• Recovery Planning • Improvements • Communications • Cost of information lost / stolen revenue loss • Equipment damages
Priority	Low	Low	Medium	Medium	High

Figure 1. The “Identify, Protect, Detect, Respond and Recover” framework

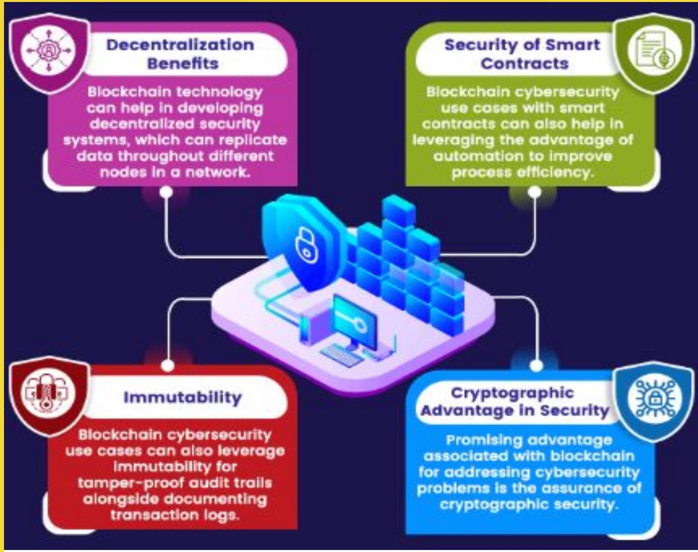
Source: (Mendel, 2018).

1) **“Identify, Protect, Detect, Respond, Recover” (IPDRR)**
   a) A holistic risk and security management framework that focuses on using business drivers to guide cybersecurity activities and considers cyber threats as a part of the organization’s risk management process
      i) Not a one-size-fits-all approach

Possible Solutions (Technology)

2) Application of blockchain technology in critical infrastructure

- Only users with specific permissions can access the data
- The security is enhanced by maintaining two distinct ledgers:
  - A ledger with individually encrypted data
  - A transaction ledger which stores encryption access keys to the related data
- A cost-effective tool to track/secure the complete history of data transactions
  - security breach => facilitate data recovery/integrity



Decentralization Benefits

Blockchain technology can help in developing decentralized security systems, which can replicate data throughout different nodes in a network.

Security of Smart Contracts

Blockchain cybersecurity use cases with smart contracts can also help in leveraging the advantage of automation to improve process efficiency.

Immutability

Blockchain cybersecurity use cases can also leverage immutability for tamper-proof audit trails alongside documenting transaction logs.

Cryptographic Advantage in Security

Promising advantage associated with blockchain for addressing cybersecurity problems is the assurance of cryptographic security.

3) End-to-end cybersecurity for critical infrastructure

- Encapsulates a range of technologies and services
- Conducts a cyber resiliency health assessment designed by a reputable third party

Future Outlook

.

- The White House has come up with a **National Cybersecurity Strategy** = 2023
  - **Pillar One: Defend Critical Infrastructure**
    - Establish cybersecurity regulations to secure critical infrastructure
    - Harmonize and streamline new and existing regulation
    - Integrate Federal cybersecurity centers
    - Update Federal incident response plans and processes
    - Modernize Federal Defenses
- The U.S. Treasury Department is looking into insurance for catastrophic cyber risk

To be truly effective, **critical infrastructure providers must fold cybersecurity into the fabric of their organization**. As our reliance on technology and infrastructure grows, so does the risk and consequences of cyber attacks. Therefore, there is a definite need for us to focus on improving our cyber security and preparing our society and economy for possible cyber attacks.

Sources

https://nychazardmitigation.com/hazard-specific/cyber-threats/what-is-the-hazard/

https://www.gao.gov/blog/securing-u.s.-electricity-grid-cyberattacks

https://www.internetandtechnologylaw.com/cybersecurity-power-grid-concerns/

https://www.ncbi.nlm.nih.gov/pmc/articles/PMC8473297/

https://securityaffairs.com/38765/cyber-crime/cyber-attack-power-grid.html#:~:text=In%20this%20scenario%2C%20the%20researchers,grid%20compromised%20by%20the%20attack.

https://www.cfr.org/report/cyberattack-us-power-grid

https://www.energy.gov/policy/articles/cyber-threat-and-vulnerability-analysis-us-electric-sector

https://sciendo.com/downloadpdf/journals/raft/26/1/article-p69.xml

https://www.gao.gov/blog/solarwinds-cyberattack-demands-significant-federal-and-private-sector-response-infographic

https://sciendo.com/article/10.18559/ebr.2019.2.2

https://commercial.allianz.com/news-and-insights/expert-risk-articles/cyber-attacks-on-critical-infrastructure.html#:~:text=Research%20estimates%20the%20economic%20and,more%20than%20a%20%241trn.

https://www.whitehouse.gov/wp-content/uploads/2023/03/National-Cybersecurity-Strategy-2023.pdf