2024
PUBLIC-PRIVATE
ANALYTIC EXCHANGE PROGRAM

IMPLICATIONS OF EXTREME WEATHER EVENTS ON U.S TELECOMMUNICATIONS INFRASTRUCTURE

2024 PUBLIC-PRIVATE ANALYTIC EXCHANGE PROGRAM

Implications of Extreme Weather Events on U.S. Telecommunications Infrastructure

Every year extreme weather events cause significant damage and economic loss in the United States. Since 1980, the U.S. has endured 391 extreme weather events, 102 of which have occurred in the last five years.[1] Recent studies indicate that extreme weather events such as hurricanes, floods, fires, extreme heat, extreme cold, drought, extreme temperature fluctuations, and sea level rise are likely to become more frequent and intense with anthropogenic climate change.[2] As a result, potential impacts on international and domestic telecommunications infrastructure are quickly becoming a national security issue.

Fiber-optic telecommunications infrastructure facilitates the high-speed transmission of data. The capacity of fiber-optic cables has increased significantly in recent years making it the backbone of U.S. communications systems. Fiber-optic telecommunications enable high-speed internet access, telephony, Voice over Internet Protocol (VoIP), mobile communication networks, television, and streaming video. Extreme weather events can disrupt telecommunications infrastructure, halting communications and preventing access to data centers and critical data applications, potentially impacting each of the 15 other critical sectors and hindering disaster response and recovery efforts.

Sector Specific Impacts of Telecommunications Disruptions	
Chemical & Hazardous Materials	This industry relies on telecommunications for environmental monitoring, ensuring safety through real-time data transmission and coordinating emergency responses to hazardous situations. (Example: lack of effective communications systems significantly degraded response to a chemical plant accident in Atchison, KS in 2016).
Commercial Facilities	Telecommunication systems are essential for day-to-day operations and enabling communication within and between facilities. Many commercial facilities use telecommunications networks to operate security systems, including surveillance cameras and access control systems.
Critical Manufacturing	Telecommunication services provide the backbone for supply chain logistics, allowing for the tracking of materials and products from production to delivery. It also allows for real-time monitoring and control of the manufacturing process, leading to increased operational efficiency.
Dams	Reliable telecommunication services ensure the safety, efficiency, and continuity of dam operations. Telecommunications networks enable the remote operation and control of dam facilities, which is essential for managing water levels and flow rates. In the event of an emergency, such as a potential dam failure, telecommunications services are crucial for alerting authorities and coordinating evacuation and response efforts.

Homeland Security

Defense Industrial Base	The Defense Industry relies on secure communications to coordinate operations and enable rapid deployment of national defenses. This industry is particularly vulnerable to cyberattacks.
Emergency Services	Phone and internet services allow for the delivery of police, fire, and emergency responder services. Telecommunications are critical for communication during disasters and allows emergency responders to coordinate efforts and provide timely assistance to US citizens.
Energy	Telecommunication networks facilitate the efficient operation of energy systems, allowing for real-time monitoring and control of energy production and distribution. There is a significant interdependence between the energy sector and telecom; the power grid requires reliable telecommunications networks for control, while telecommunications networks depend on the power grid for energy.
Financial Services	Fiber-optic networks are used for high-frequency trading (HFT) and financial market data transmission, where ultra-low latency connections are essential for executing trades quickly and efficiently.
Food & Agriculture	America's agriculture industry relies on advanced technologies and internet connected devices such as sensors and drones to provide critical data on weather forecasting, crop health, and livestock conditions to increase efficiency and yield. Remote monitoring and automated equipment also rely on stable internet connections.
Government Services & Facilities	Phone and internet services are crucial for essential government operations. In addition to providing the infrastructure for secure data transmission, telecommunications is also used for inter-agency communications and public service delivery.
Healthcare & Public Health	Fiber-optic networks support telemedicine applications, hospital management databases, and medical imaging services that require high-speed and reliable data transmission.
Information Technology	The IT industry's reliance on telecommunications is extensive and multifaceted, with telecommunications serving as the backbone for a wide range of IT services and operations. It is the foundation for internet connectivity, IT operations, cloud services, and data transmission.
Nuclear Reactors, Materials & Waste	The nuclear sector depends on telecommunications for monitoring and controlling reactors, managing waste, and ensuring the secure transport of materials.
Transportation	Telecommunications enables the real-time coordination of transportation services, including fleet management, scheduling, and route optimization. It also provides the necessary communication channels for navigation systems,

	safety alerts, and tracking, which are vital for the safe operation of vehicles.
Water & Wastewater	Telecommunication enables the Supervisory Control and Data Acquisition (SCADA) systems to monitor and control water treatment processes, ensuring the proper operation of these systems and limiting the risk of overflow and malfunction. Several Internet of Things (IoT) systems are used to collect and analyze data related to water purification systems and operational efficiency.

TEAM INTRODUCTIONS

MEMBERS	COMPANY
Cindi Venters	*Presidential Management Fellow — US Forest Service*
Patrick B.	*Department of Defense*
Ritabeth Crague	*Lumen Technologies*
Greg Brannan	*United Services Automobile Association*
Daniel Devery	*Assurant, Inc.*
Ellen Rose H. - Champion	*Department of Defense*

Undersea Cable Network & Landing Station Threat Environment

The undersea cable network is a system of fiber-optic cables that transmit data and power between land-based locations across oceans and other bodies of water. Today there are seventeen transatlantic cable systems (twelve in service) and eighteen transpacific cable systems currently in operation or under development.[3][4] The fiber-optic cables are laid and operated by dozens of companies with hundreds of subcontractors and minimal international legislation. The cables carry over 95% of international data and voice communication, including email, webpages, and video calls.[5] This includes the majority of civilian, military, and government offshore communications traffic. Undersea cables make landfall at landing stations where they connect to terrestrial telecommunication networks.

The undersea cable network and cable landing stations are vulnerable to seismic activity and changes in water flow. Earthquakes and underwater landslides can cause cable breaks and structural damage to landing stations. Strong currents and tidal forces, often caused by hurricanes and tsunamis, can put stress on undersea cables, leading to damage or breaks over time. Landing stations concentrated in coastal areas may face additional environmental hazards such as erosion and saltwater corrosion.[6] In recent years, telecommunication companies have invested in a variety of methods to quickly identify and remedy weather-related damage and harden infrastructure. For example, it has become common practice to strengthen cables by adding a protective layer to shield the fiber optic and copper from environmental damage. In addition, telecommunications companies have begun burying lines up to 30 feet beneath the seabed rather than laying them on the ocean floor.[7]

The undersea cable network also relies on embedded alarm and trigger mechanisms, which notify operators of disruptions, provide approximate geo-coordinates of the event, and may indicate the type of damage. When service is interrupted, companies can reroute through redundant pathways and hardware. Network repair ships are also strategically placed around the world to investigate disruptions and repair damage. However, simultaneous events or events that impact a large portion of the network could cause a significant service disruption to a region. In the U.S., landing stations are geographically concentrated in New York, New Jersey, Virginia, South Carolina, Florida, Seattle, Portland, and Los Angeles, and vary in their physical architecture. For example, New York landing stations are located in more industrial areas while landing stations in New Jersey and Virginia Beach appear to be standalone installations with minimal physical resilience (Figure 1). Cables buried, sometimes in clusters, in near-shore shallow waters and initial landfall junctions are easily accessible and often not monitored. If a catastrophic storm were to interrupt landing station operations in New York and New Jersey (Figure 2), an adversary could exploit the event and sabotage cables landing in Miami to successfully disrupt communications along the entire East Coast.

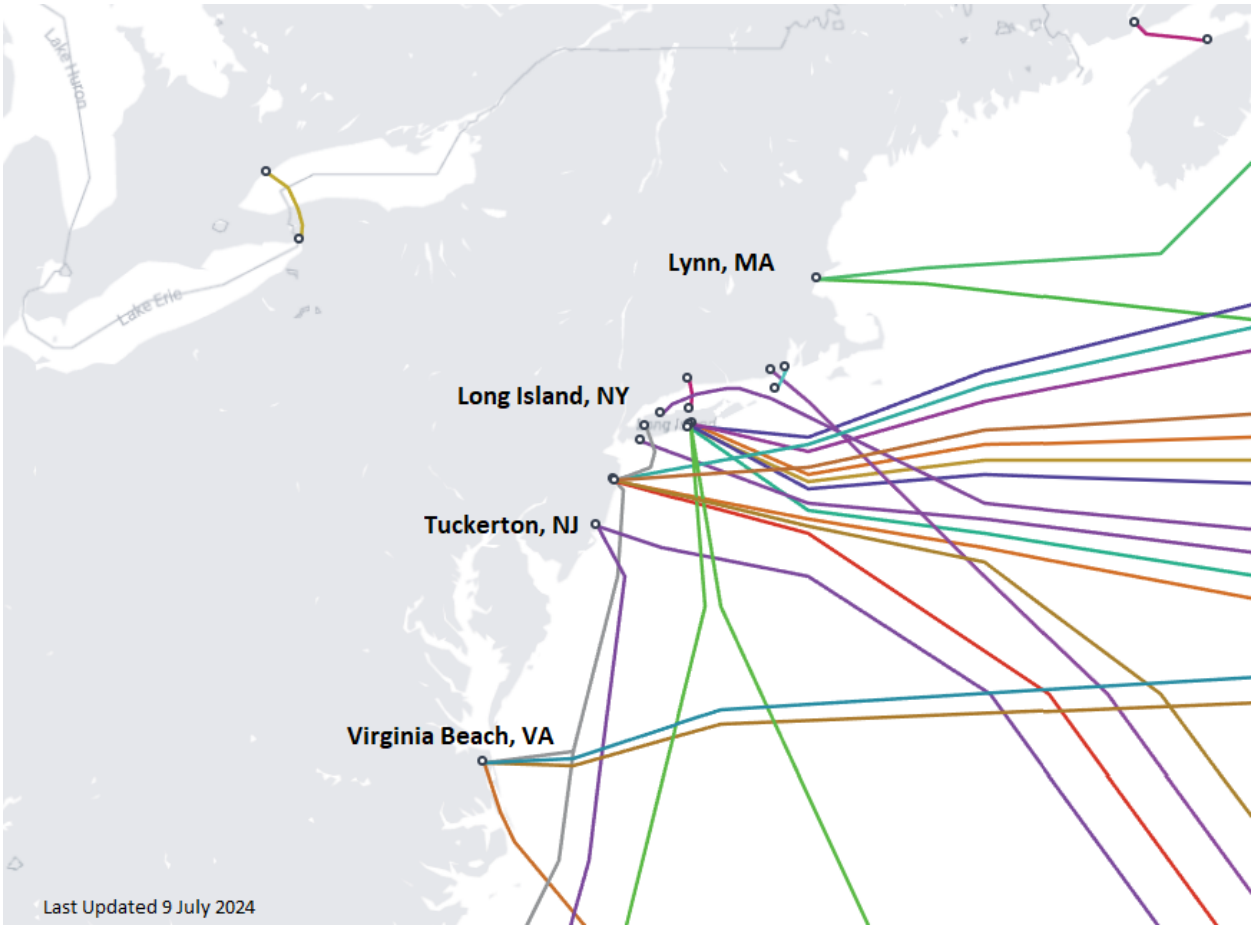

Figure 1 – Cable landing stations and associated cable paths in the Northeast US.[3]

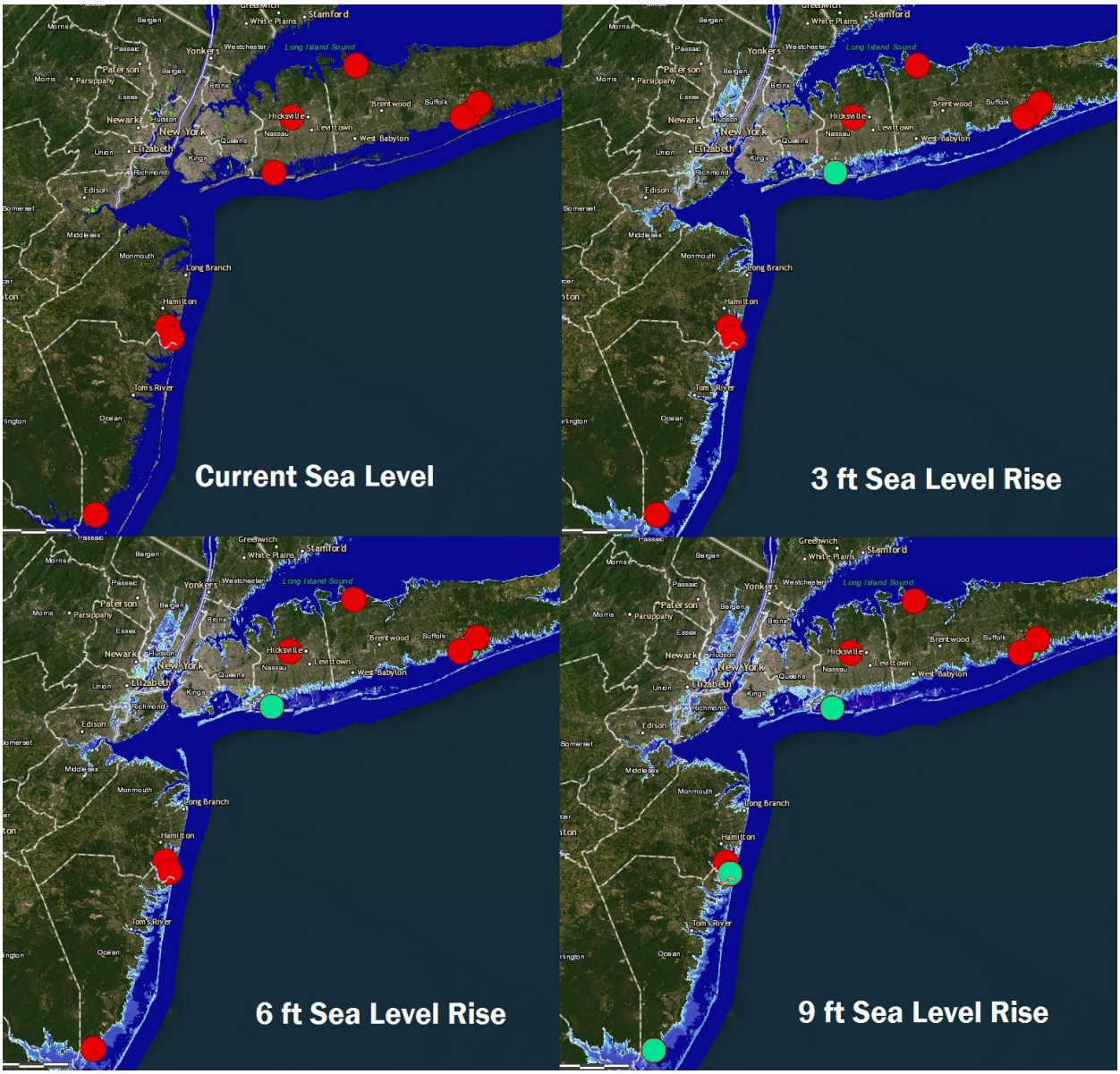

Figure 2 – Cable landing stations in New York and New Jersey and the inland extent of potential sea level rise.[8] Stations change from red to teal when inundated. The sea level rise data does not consider changes in coastal and shoreline geomorphology such as erosion or subsidence.

Terrestrial Cable Network Threat Environment

The terrestrial cable network consists of underground and aerial cables carrying telecommunications signals over land. Hurricanes, tornadoes, thunderstorms, flooding, and windstorms can cause significant damage to terrestrial cable infrastructure. High winds can knock down trees and utility poles, leading to cable breaks. Winter storms can cause snow and ice to coat cables and equipment, increasing their weight which leads to sagging, breakage, or collapse of power lines and telecommunication cables. Flooding can inundate

terrestrial cable infrastructure, submerging underground cables or damaging above-ground equipment. Floodwaters can compromise cable insulation, corrode connectors, and disrupt signal transmission, leading to service outages. Heavy rainfall or seismic activity can trigger landslides or mudslides, which can damage buried cables, conduits, or junction boxes along hillsides or mountainous terrain—and hinder access for repair crews. Wildfires also pose a threat to terrestrial cable infrastructure, particularly in regions prone to dry conditions and forest fires. Flames, smoke, and heat can damage above-ground cables, utility poles, and transmission towers, while firefighting efforts may inadvertently cause further damage to cables and equipment. Prolonged periods of extreme heat can stress terrestrial cable infrastructure, causing materials to expand and contract, leading to cable sagging, equipment malfunction, or insulation degradation. Overheating of underground cables can also occur in urban areas with high heat retention. Heat lightning can damage terrestrial cable infrastructure, causing power surges, equipment failures, or cable insulation breakdown. Electromagnetic pulses (EMPs) caused by heat lightning can also disrupt signal transmission and affect network performance. Likewise, freezing temperatures can affect the performance and reliability of terrestrial cable infrastructure, particularly in regions experiencing deep freezes or polar vortex events. Cold temperatures can cause cable shrinkage, brittle materials, and freezing of moisture within cables, leading to signal degradation or cable failure.

Underground fiber is shielded from the winter elements because it is buried below the depth where soil freezes. As an industry standard most fiber optic cables are buried between 18” to 24” for residential use and 3’- 6’ for commercial use depending on the location and application. While the obvious solution to many of these problems might be to bury all fiber-optic cable, this conversion is often not feasible due to costs. It is much cheaper to harden overhead transmission lines by building stronger poles, and using storm guying, push braces, pole class uprating, shorter spans, smaller conductor sizes, fewer attachments, and increased vegetation management.[9] In addition, underground transmission lines are still vulnerable to extreme weather, such as storm surges, and generally are more difficult to repair. Instead, most companies develop storm-hardening roadmaps which are a multi-year plan that gradually hardens the system in a targeted and cost-effective manner. A typical roadmap will identify and harden areas which have experienced repeated degradation or are particularly critical. But because the system is only as strong as the weakest link, it is important to ensure redundancy by investing in multiple paths.

Data Center Threat Environment

Data centers play a critical role in supporting business continuity and disaster recovery efforts for organizations across various industries. Many data centers are moving closer to the population centers near the shoreline to enable edge computing where data processing occurs closer to the source of data generation or consumption. This distributed computing paradigm improves application performance, reduces bandwidth usage, and enhances data

privacy by processing sensitive data locally instead of transmitting it over long distances to centralized data centers. In addition, moving data centers closer to shorelines reduces latency and improves connectivity to terrestrial and undersea fiber optic-networks. Coastal areas also offer opportunities to harness renewable energy sources such as wind, solar, or tidal power to power data center operations and natural water-based cooling. Several companies are currently looking for ways to increase data center performance and reliability, including testing underwater and lunar based locations.[10][11]

With the move to coastal locations, data centers become more vulnerable to extreme weather that commonly impacts the coasts including hurricanes, tornadoes, and severe thunderstorms which can cause power outages by damaging electrical infrastructure such as power lines, transformers, or substations. In addition, these natural disasters can cause high winds which can cause structural damage to data center buildings, roofs, or external equipment such as cooling towers or antennas. Falling debris or projectiles propelled by strong winds can also damage exterior walls, windows, or rooftop equipment. Flooding can inundate data center facilities, causing water damage to equipment, electrical systems, and infrastructure. Even minor leaks or water seepage can disrupt operations and compromise the integrity of data stored in servers.

Data centers also require precise temperature and humidity controls to ensure optimal operation of servers and networking equipment. Extreme heat or cold snaps can strain cooling systems, leading to overheating or equipment failure. Similarly, excessive humidity or dry conditions can cause condensation or static electricity buildup, posing risks to sensitive electronics. Extreme weather events may lead to transportation disruptions, making it difficult for staff, suppliers, or service providers to access data center facilities for maintenance, repairs, or equipment replacement. Extreme weather events often lead to power outages, during which data centers rely on backup generators to continue operations.[12][13]

To mitigate the impact of extreme weather events, data center operators implement a range of measures such as developing site selection criteria, upholding building design and construction standards, installing pumps, infrastructure hardening, backup power systems, redundancy in cooling and networking infrastructure, and comprehensive disaster preparedness plans. Regular risk assessments, monitoring, and maintenance are also essential for identifying vulnerabilities and ensuring the resilience of data center facilities in the face of extreme weather challenges.

KEY FINDINGS

The Implications of Extreme Weather Team traveled to New Orleans, LA to conduct field research in arguably the most challenging telecommunications environment in the U.S. due to the prevalence of extreme weather and the confounding impact of the Mississippi River and Gulf of Mexico. The team met with a community-based organization, an international telecommunications company, a federal agency, a local government agency, and an academic institution. Each entity provided a unique perspective into the dynamic and evolving challenge of providing telecommunications service continuity. We found that building mechanisms for redundancy, monitoring, routine maintenance, and planning into operations were key to withstanding extreme weather events such as Hurricane Ida.

Redundancy - Both the global undersea and terrestrial cable networks are extensive, offering numerous opportunities for redundancy. Despite this, the telecommunications industry often falls short in establishing cooperative agreements that would allow for the utilization of alternative routes through other companies' infrastructure during outages. Telecommunications companies have instead addressed this challenge by integrating physical and logical redundancies into their operational frameworks. Physical redundancies mitigate hardware disruptions. Undersea cables often consist of two or more separate cables between landing stations so that a single cable fault will not disrupt that cable's communications. Each cable will often branch into two separate cables miles offshore and terminate at two different beach manholes, reducing the risk of cable faults which most often occur close to shore. Data centers, landing stations, and telecommunication facilities are equipped with backup batteries, air conditioning units, spare hardware, and cables, all of which are portable and can be transferred to other sites as needed. Moreover, these redundancy measures undergo regular testing and are under continuous surveillance for any Loss of Redundancy (LOR), ensuring timely maintenance and repairs. Logical redundancies address disruptions in software or network protocols, where multiple paths are available for data transmission in the event of congestion or transmission issues. These redundancies can utilize multiple equal-cost transmission paths and varying network protocols, often automatically so there is no loss of data to the end user. Data rerouting is typically confined to a cable operator or company network, so widespread disruptions can still adversely affect customers. While this strategy of prioritizing physical and logical redundancy is effective for small, isolated outages, cooperative agreements should be established to overcome widespread outages.

Monitoring and Routine Maintenance - The telecommunications company that we interviewed utilizes a weather monitoring system that automatically generates service tickets, prompting the deployment of direct support technicians to locations that may be affected by impending weather conditions. This preemptive action allows for the timely inspection and maintenance of essential equipment, such as generators, to ensure they are operational and ready to withstand extreme weather events. The company also actively monitors the ambient temperature within its facilities, adjusting climate control systems as needed to counteract the effects of extreme temperatures and safeguarding sensitive

equipment from the potential damages caused by excessive heat or cold, which could otherwise lead to service disruptions.

Planning - In advance of extreme weather, the telecommunications company distributes satellite phones to ensure technicians can communicate throughout the duration and aftermath of the event. Current standard operating procedures mandate that technicians report at least every 2- 4 hours to give an update on their status and current actions. After a storm passes, technicians return to the locations and conduct damage assessments. As outages are reported, technicians receive manual and automated outage tickets and immediately deploy to find solutions. During larger events, technicians from neighboring regions are dispatched to assist in response and recovery efforts. The company credited its resilience to utilizing direct support technicians with years of experience working at their assigned sites which is a rarity in an industry known for its high turnover and in contrast with many other large telecommunications companies that utilize service contracts for routine and emergency maintenance and repairs with stipulated expertise and response times. Because technicians are so familiar with sites, they are often able to find solutions faster than contractors or subcontractors who might be navigating the equipment for the first time. Additionally, the response and recovery of communities could be delayed by higher priority customers with emergency contracts, as their repairs would be completed only after the priority repairs are finished. The telecommunications company that we interviewed also stressed the importance of business continuity planning for rapid response and recovery. The company conducts a large exercise prior to severe weather season. Additionally, station supervisors continuously test and evaluate their technicians to keep their skills honed year-round and not just prior to a storm. The company's internal Business Continuity Program owners also participate in disaster preparedness calls with other industry providers where they collaborate and share best practices from previous years' activities.

Consistent Gaps

Prioritization - The team found that while the telecommunications industry was generally well-prepared for extreme weather events, many companies could benefit from using a tiered priority system to restore service. Certain sectors, such as emergency services and health care providers, should be serviced before other sectors that have less of an impact on the loss of life in the aftermath of a natural disaster. Telecommunications providers should also focus on sectors that support other critical infrastructure. Extreme weather events can cause cascading failures across critical infrastructure, meaning that as one sector loses function, that loss of function can cascade down to other sectors that are needed to keep a city running. For example, telecommunication operators rely on the availability of energy to function. Loss of the telecommunications sector could be particularly damaging as this sector provides the enabling function of communication that many other critical infrastructure sectors rely on to operate. A tiered system, informed by local knowledge, would help operators pre-determine which customers to restore first during an outage. Without such a system, operators might waste valuable time deciding priorities during an outage, potentially favoring high-paying customers or personal connections over actual need.

Supply Chain Optimization - The U.S. fiber-optic telecommunications infrastructure is reliant on multiple components which are sourced and produced overseas in areas that are vulnerable to extreme weather. Currently, there is a critical shortage of undersea cable repair ships due to rising interest rates and shortages of key back-deck equipment that makes it difficult to finance new builds.[14] In addition, semiconductor shortages have impacted 5G deployments for Intel, AT&T, CommScope, and Juniper according to quarterly reports.[15][16][17][18] Research by TXO—a telecommunications hardware provider—revealed that 85 percent of operators have experienced project timeline disruptions due to shortages for critical hardware such as optical fiber, transmitters, receivers, amplifiers, multiplexers/demultiplexers, and switches/routers.[19] Operators have begun using refurbished equipment to avoid long waits, save money, and support their sustainability goals. Telecommunications operators are also increasing their stock levels, expanding the network of suppliers they buy from, repairing and reusing existing equipment, and redesigning their network architecture to reduce reliance on manufacturers. Supply chain orchestration can coordinate activities from sourcing raw materials to delivering finished products. Once data is organized, advanced analytics should be utilized to forecast demand, predict disruptions, manage inventory, and improve overall supply chain visibility.

Data Analytics - Overhead fiber lines are typically replaced through attrition. When an event damages a section of these lines, crews determine the feasibility (time, money, and resources) to replace the broken segment by placing it underground versus its original location. The telecommunications industry could benefit from the use of data analytics when deciding which parts of the network to harden and what techniques to use. For example, studying the flow of water, land coverage, and soil condition to develop machine learning models can help the telecommunications industry assess risk and create structural changes such as creating or enhancing a wetland to reduce flooding. However, these solutions are difficult to develop and implement without robust data. Academic institutions and federal agencies are eager to develop models to facilitate adaptation, but they lack data that is readily available to telecommunications service providers, local government agencies, and community-based organizations. All of the entities the IEWE team met with would likely benefit from opportunities to collaborate with a focus on data collection and analysis to address challenges posed by extreme weather.

IMPACT TO GOVERNMENT AND PRIVATE SECTOR

The public and private sector are both critically dependent on telecommunications but often unaware of the potential impact of a widespread outage and their options for recovery.[20] Both public and private entities would benefit from developing business continuity plans that identify critical functions dependent on telecommunication services and consider contracting with multiple providers, stipulating preparedness, mitigation, response, and recovery for extreme weather within acquisition documents to ensure resiliency. By stipulating requirements for routine maintenance, monitoring, and emergency repairs in contracts, telecommunications companies will be able to respond and recover from events faster. In addition, public and private sector entities should consider entering contracts with satellite providers for limited access during events.

Figure 3 – Global interconnected telecommunications network.

There is no single federal agency that is dedicated to securing the undersea cable network and landing stations, terrestrial cable network, or data centers—despite the evolving threat landscape. Instead, there is a heavy reliance on the private sector to audit business and security practices and those of their supporting vendors and companies. Often conglomerates will "own" the fiber lines but cables, landing stations, and data centers are owned by separate, much smaller companies that have fewer resources to expend on operations. In 2023, it was estimated there are over 2.5 billion miles of fiber optic cables of various sizes spread around the world.[21] When a break in transmission or error occurs on the line, the task of locating and repairing the fiber is sometimes the easiest task. The challenge, especially with undersea fiber, is who owns the financial responsibility and will make the repair to the damaged segment of fiber. There are several organizations that have attempted to provide oversight to the global telecommunications infrastructure including the International Cable Protection Committee (ICPC), the Communications Security Reliability, and Interoperability Council (CSRIC) and associated working groups, and the North American Submarine Cable Association (NASCA). At the federal level, both the Committee on Foreign Investment in the United States (CFIUS) and Department of Homeland Security (DHS) navigate issues that arise in this field. But until there is a single entity responsible for investigating flagged issues (e.g. unusual observed maritime activity), and facilitating issue resolution, there will likely be shortfalls.

Funding for resiliency typically is not allocated until after a natural disaster occurs. Yet the investment in prevention, mitigation, response, and recovery determines the size and

duration for most outages. The telecommunications industry is in a constant state of modernization, providing opportunities to re-evaluate their approach to extreme weather. In recent years, the focus has shifted from resilience to adaptation when it comes to planning and preparing for extreme weather. While resilience focuses on withstanding the immediate impacts of a disaster, adaptation involves proactive adjustments to mitigate and manage risks before they escalate. This transition demands foresight and strategic planning. By prioritizing adaptation, the telecommunications industry and the government agencies, businesses, and communities that they serve can effectively reduce vulnerabilities and enhance their ability to cope with immediate impacts but also lay the groundwork for sustainable development that can withstand the challenges posed by a changing climate over the long term.

FORECASTS

Opportunistic Cyber Attacks as a Threat Multiplier - Extreme weather events often cause disruptions within communities and the telecommunication companies that serve them, offering increased opportunities for physical and cyber-attacks. Although fiber optic cables are one of the safest means to transport sensitive data, malicious actors can easily use the opportunity provided by a natural disaster to access and damage unsecured fiber optic cable to limit the effectiveness of response and recovery efforts. Malicious actors can easily gain access to cable and equipment through unsecured street access plates and telecommunication sites for which there are currently insufficient legal penalties. Tapping into fiber is an arduous process that takes an experienced hand, specialized tools, and often increases the attenuation by a detectable amount but if done correctly can result in all signals within the fiber being collected. Malicious actors may also be motivated to gain access to fiber to simply disrupt communications or prolong and/or broaden outages by damaging fiber or their communication nodes, thus making troubleshooting and repairs time consuming and costly. The telecommunication industry could likely benefit from burying fiber-optic cable in concrete where practical and allowed by law, welding shut manhole covers, and securing wiring closet doors, riser access panels, and elevator shafts where network cabling exist. In addition, they should invest in continuous data monitoring to detect and identify anomalies, loss of signal, or other indicators of instability. By installing additional alarms, cameras, and detection systems to deter and investigate disturbances, though these are used to identify when a fiber cable has been compromised. However, monitoring and ticketing systems become soft targets which could easily provide insight into where cables are buried, site locations, and even offer opportunities to remotely degrade or disable operations.

Polycrisis Events That Compound and Exploit Near-Shore Vulnerabilities - Undersea cables close to shore have the highest risk of damage due to ship anchors or other maritime operations and are equipped with armor plating and buried in trenches to protect the fragile cables from significant damage. In 2012, Hurricane Sandy knocked out several key transatlantic cables, disrupting internet traffic for hours. In 2011, the Fukushima earthquake in Japan had similar impacts. In the short-term, the U.S. telecommunications infrastructure could benefit from avoiding the practice of cable clustering. In the long-term, companies should consider increasing the geographic distributing new landing stations to avoid concentration. While the fiber itself is resilient, the facilities housing it may not be. Global sea levels are projected to rise 1 to 4 feet by 2100, thus increasing coastal flooding probabilities and the risk for fiber facilities to flood increase (Figure 4). With climate change and extreme weather frequencies increasing, companies should consider the long-term impacts due to severe weather when planning for fiber installation.

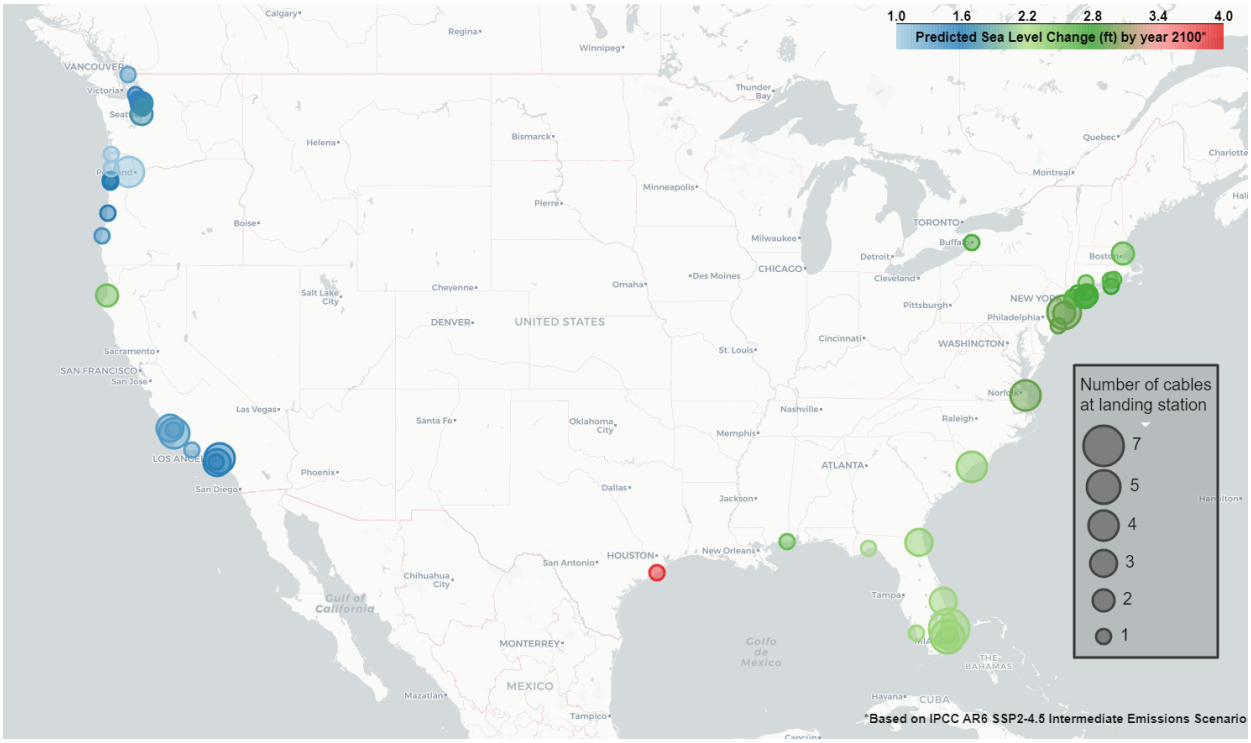

Figure 4 – United States cable landing station locations and associated predicted sea level rise based on IPCC AR6 SSP2-4.5 Intermediate Emissions Scenario.[22]

ANALYTIC DELIVERABLE DISSEMINATION

Office of the Director of National Intelligence, National Intelligence Council

Department of Homeland Security, Critical Infrastructure Security Agency

Department of Defense, Strategic Environmental Research and Development Program (SERDP), Environmental Security Technology Certification Program (ESTCP) & U.S. Army Corps of Engineers

Lumen Technologies

Tulane University

Water Works, L3C

Orleans Parish Communications District

Analysis and Resilience Center for Systemic Risk

The International Cable Protection Committee (ICPC)

The Communications Security Reliability, and Interoperability Council (CSRIC)

The North American Submarine Cable Association (NASCA)

Previous participants in the AEP and IC Analyst-Private Sector Program

Appendix 1: Recent Weather-Related Outages & Impacts

2012 Hurricane Sandy: Telecommunication services were disrupted in the Northeast region of the U.S. due to power outages and flooding caused by Hurricane Sandy. This resulted in spotty phone service and internet service. Approximately 25% of the region's wireless cell towers were impacted rendering many 911 call centers inoperable.[23]

2018 Sulawesi Earthquake and Tsunami: 4G networks were disrupted as the result of a 7.5 magnitude earthquake and tsunami. Network availability took almost two weeks to return to normal.[24]

2020 California Wildfires: Fires in Sonoma and Napa charred more than 46,000 acres damaging internet and cell phone infrastructure and impeding evacuation communications. To restore service, utility poles and fiber optic cable had to be re-installed.[25]

2022 Extreme Heat in London: Google and Oracle data centers experienced outages due to cooling system failures during a record-breaking heat wave in the United Kingdom. The incident disrupted cloud-computing services and took 19 hours to resolve.[26]

[1] National Oceanic and Atmospheric Administration National Centers for Environmental Information (NCEI) (2024). U.S. Billion-Dollar Weather and Climate Disasters. Retrieved from: https://www.ncei.noaa.gov/access/billions/, DOI: 10.25921/stkw-7w73.
[2] Environmental Protection Agency (2024). Climate Change Indicators in the United States: Fifth Edition. Retrieved from: https://www.epa.gov/climate-indicators/climate-change-indicators-united-states-fifth-edition.
[3] TeleGeography Submarine Cable Map (2024). Retrieved from: https://www.submarinecablemap.com/.
[4] Threats to Undersea Cable Communications (2017). Private-Public Analytic Exchange Program.
[5] Fast Company (2024). Nearly All Data That Moves Around the World Goes Through These Undersea Cables. Retrieved from: https://www.fastcompany.com/91072728/internet-undersea-cables-data
[6] Bruns, A. (2020). How Undersea Cables Drive Onshore Site Decisions. Site Selection Magazine. Retrieved from: https://siteselection.com/issues/2020/mar/data-centers-how-undersea-cables-drive-onshore-site-decisions.cfm.
[7] Threats to Undersea Cable Communications (2017). Private-Public Analytic Exchange Program.
[8] National Oceanic and Atmospheric Administration Office for Coastal Management (2024). Sea Level Rise Inundation. Retrieved from: https://www.coast.noaa.gov/arcgis/rest/services/dc_slr.
[9] Griffin, J. (2010). 'Hardening' Power Lines. Underground Infrastructure Magazine, 65(7). Retrieved from: https://undergroundinfrastructure.com/magazine/2010/july-2010-vol-65-no-7/features/hardening-power-lines.
[10] Roach, J. (2020). Microsoft finds underwater datacenters are reliable, practical and use energy sustainably. Microsoft. Retrieved from: https://news.microsoft.com/source/features/sustainability/project-natick-underwater-datacenter/.
[11] Ariosto, D. (2024). Data Centers Could Soon Break Lunar Ground. Electronic Engineering Times. Retrieved from: https://www.eetimes.com/data-centers-could-soon-break-lunar-ground/
[12] Miller, R. (2021). Louisiana Data Centers Rely on Generators in Wake of Hurricane Ida. Data Center Frontier. Retrieved from: https://www.datacenterfrontier.com/colo/article/11427982/louisiana-data-centers-rely-on-generators-in-wake-of-hurricane-ida.
[13] Armstrong, B. (2024). Weather the Storm: A Comprehensive Guide to Data Backup and Recovery During Hurricane Season. FOGO Solutions. Retrieved from: https://fogosolutions.com/storm-backup/.
[14] Clark, R. (2022). Another Telco Supply-Chain Shortage: Cable Ships. Light Reading. Retrieved from: https://www.lightreading.com/digital-transformation/another-telco-supply-chain-shortage-cable-ships
[15] Stankiewicz, K. (2022). Intel CEO Now Expects Chip Shortage to Last Into 2024. CNBC. Retrieved from: https://www.cnbc.com/2022/04/29/semiconductor-shortage-intel-ceo-says-chip-crunch-to-last-into-2024.html#:~:text=Intel's%20Pat%20Gelsinger%20now%20expects,for%20its%20fiscal%20second%20quarter. Nhjukiuo809b.
[16] Baumgartner, J. (2021). Supply Chain Constraints Cut Into AT&T's Fiber Buildout Plan. Light Reading. Retrieved from: https://www.lightreading.com/optical-networking/supply-chain-constraints-cut-into-at-t-s-fiber-buildout-plan.
[17] Baumgartner, J. (2022). CommScope Struggles with Supply and Demand for Set-Tops and Gateways. Light Reading. Retrieved from: https://www.lightreading.com/cable-technology/commscope-struggles-with-supply-and-demand-for-set-tops-and-gateways.
[18] Ziser, K. (2021). Juniper Nets $1.2 Billion for Q2 Despite Supply Chain Struggles. Light Reading. Retrieved from: https://www.lightreading.com/cloud/juniper-nets-1-2-billion-for-q2-despite-supply-chain-struggles.
[19] TXO (2023). Navigating the Supply Chain Chaos. White Paper. Retrieved from: https://media.txo.com/wp-content/uploads/2023/04/25230053/Navigating-the-supply-chain-chaos.pdf.
[20] Threats to Undersea Cable Communications (2017). Private-Public Analytic Exchange Program.
[21] Science News Explores (2023). Scientists Say: Fiber Optic Cable. Retrieved from: https://www.snexplores.org/article/scientists-say-fiber-optic-cable-definition-pronunciation#:~:text=Fiber%20optic%20cables%20were%20first,2.5%20billion%20miles)%20of%20cable.
[22] Garner, G. G., T. Hermans, R. E. Kopp, A. B. A. Slangen, T. L. Edwards, A. Levermann, S. Nowikci, M. D. Palmer, C. Smith, B. Fox-Kemper, H. T. Hewitt, C. Xiao, G. Aðalgeirsdóttir, S. S. Drijfhout, T. L. Edwards, N. R. Golledge, M. Hemer, G. Krinner, A. Mix, D. Notz, S. Nowicki, I. S. Nurhati, L. Ruiz, J-B. Sallée, Y. Yu, L. Hua, T. Palmer, B. Pearson, (2021). IPCC AR6 Sea Level Projections. Version 20210809. Retrieved from: https://doi.org/10.5281/zenodo.5914709

[23] Carew, S. (2012). Hurricane Sandy Disrupts Northeast U.S. Telecom Networks. Reuters. Retrieved from https://www.reuters.com/article/technology/hurricane-sandy-disrupts-northeast-us-telecom-networks-idUSBRE89T0YU/.
[24] Rizzato, F. (2018). 4G Networks Were the Most Affected By Sulawesi Earthquake. Open Signal. Retrieved from: https://www.opensignal.com/2018/11/22/4g-networks-were-the-most-affected-by-sulawesi-earthquake.
[25] Mena, B. (2020). California Wildfires Can Bring Internet Outages, Some Want Networks To Be Tougher. San Francisco Chronicle. Retrieved from: https://www.sfchronicle.com/business/article/California-wildfires-can-bring-internet-outages-15610411.php
[26] Bergen, M. (2022). Google, Oracle Data Centers Knocked Offline By London Heat. Bloomberg. Retrieved from: https://www.bloomberg.com/news/articles/2022-07-19/google-oracle-data-centers-knocked-offline-by-london-heat.