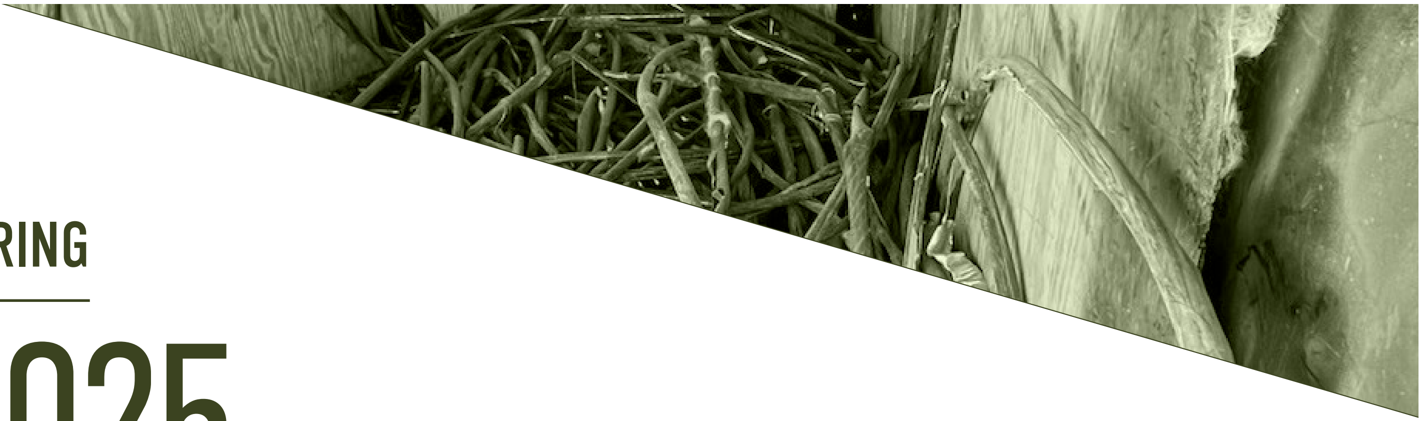


SPRING

2025

PROTECTING THE NATION'S CRITICAL COMMUNICATIONS INFRASTRUCTURE FROM THEFT & VANDALISM

Originally published November 2024

ncta THE INTERNET & TELEVISION ASSOCIATION

ctia

USTELECOM THE BROADBAND ASSOCIATION

NTCA THE RURAL BROADBAND ASSOCIATION

WIA Wireless Infrastructure Association

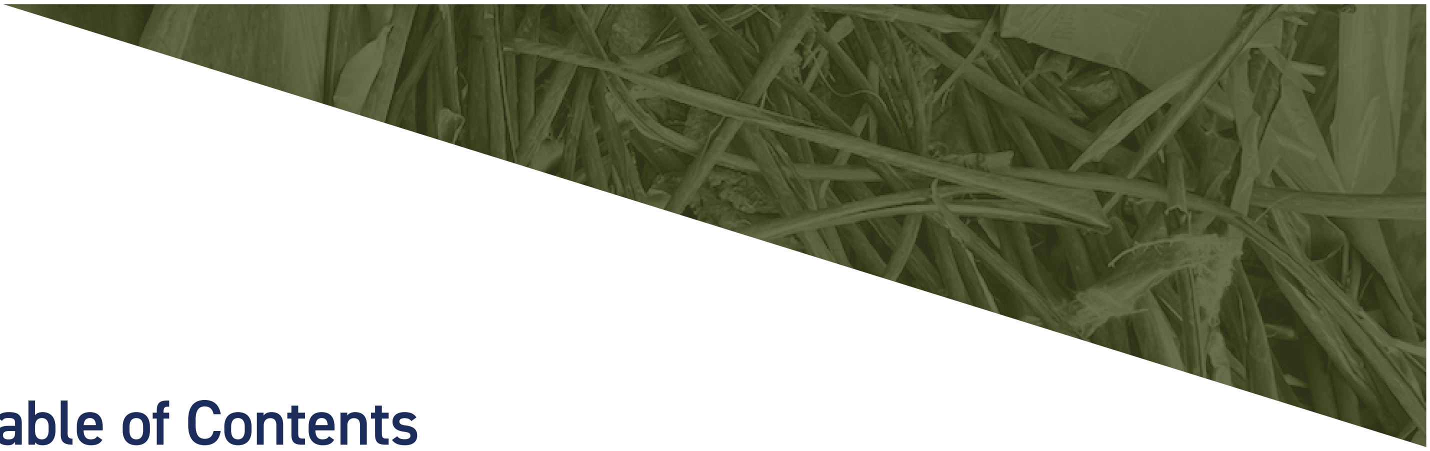
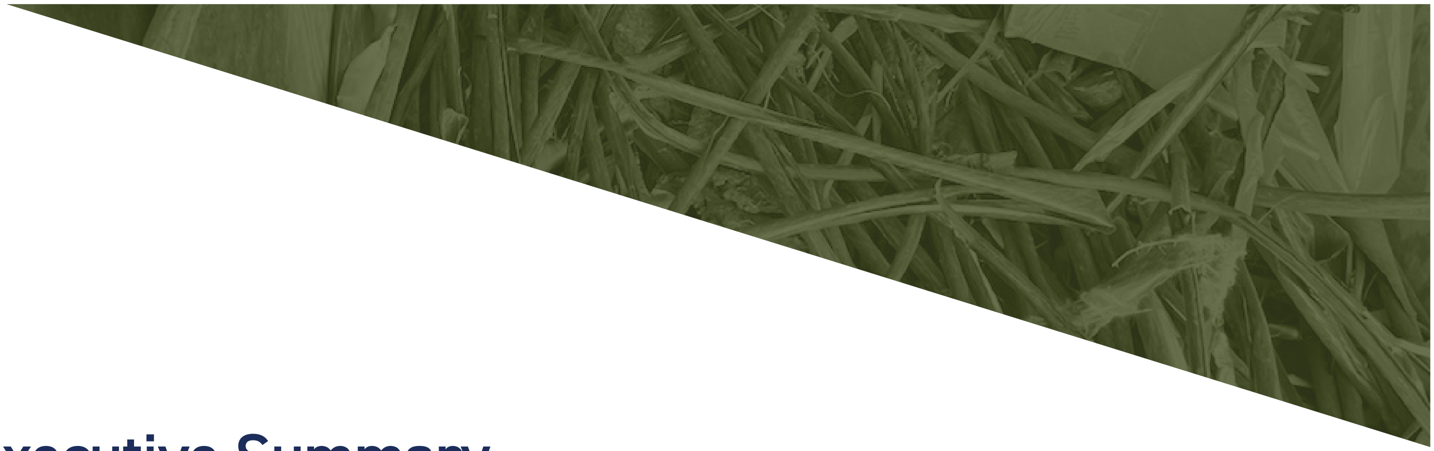


Table of Contents



Executive Summary

The U.S. communications infrastructure plays a critical role in the nation's security, economy, operation of government, and in the daily lives of most Americans. Vital sectors of society and the nation's economy, such as public safety, health care, energy, transportation, finance, information technology, and education increasingly rely on communications infrastructure. To protect economic and public safety interests, regulators, legislators, law enforcement, municipalities, and communications providers must work together to address this growing threat.

The rising market value of copper, which is used in many communications facilities, has provided bad actors with an economic incentive to target multiple industries' infrastructure (e.g., public utilities, transportation, etc.) nationwide through criminal acts of theft and vandalism. The bad actors then sell this metal and other stolen communications equipment. Critical communications infrastructure alone has experienced more than 5,700 intentional incidents of theft and vandalism between June to December 2024. In the indiscriminate search for copper, even modern communications facilities, such as fiber-optic transmission lines and wireless communications towers that have no copper, have been sabotaged.

These incidents of theft and vandalism have become increasingly common and create unnecessary service disruptions that threaten and harm American citizens, consumers and businesses. The resulting damage and resources necessary to repair the affected networks harmed by criminal conduct imposes millions of dollars of direct and indirect costs on communications network providers, consumers and the economy.

This paper seeks to increase awareness of this growing problem by highlighting:

- The greater need for collaboration among the communications industry, the scrap metal industry, state and local jurisdictions, law enforcement and law makers;
- The central and problematic role of demand side copper sale transactions;
- The proactive efforts by communications network providers to protect their assets, as well as recent best practices initiated by state and local governments to help stem the tide of this growing problem;
- Law enforcement's critical role in recognizing, investigating and prosecuting incidents of intentional theft and damage; and
- The need to examine and update existing state statutes to ensure laws are in place or strengthened to penalize the intentional theft or vandalism of critical infrastructure, cover all aspects of communications networks, make financial transactions between thieves and the recycling industry more difficult, and ensure enhanced penalties are enforced to deter future bad acts.

National Communications Infrastructure Is Essential

The U.S. government has determined that the communications sector is an integral component of the nation's economy, underlying the operations of all businesses, public safety organizations, and government.[1] It classifies communications infrastructure as a key part of the nation's critical infrastructure that comprise "the physical and virtual assets and systems so vital to the Nation that their incapacity or destruction would have a debilitating impact on national security, national economic security, or national public health or safety."[2]

Today, the nation's communications infrastructure powers modern society, providing essential connectivity for a broad range of activities and critical functions. The broadband and wireless communications networks that providers have invested trillions of dollars into over the last two decades underpin almost everything we do, and have a deep impact on a broad range of industries including but not limited to health care, global finance, energy, transportation, and many others.

Communications networks play a prominent role in:

- **Public Safety and Emergency Response:** During emergencies, communications networks are critical for public safety and coordinating emergency response efforts. They provide vital connections for coordinating emergency services, directing resources, and operating critical public alert systems[3] including 911 systems. Communications networks also play an invaluable role for law enforcement by helping to ensure prompt emergency response times, especially in rural or sprawled communities.
- **National Security:** Secure communications are fundamental to national security and related government operations. They provide a foundation for secure communications that are essential for national defense, government operations, and public safety.[4]
- **Economic Stability and Growth:** Reliable connectivity is essential for businesses to operate efficiently, enabling a broad range of opportunities from supporting artificial intelligence to e-commerce to remote work.[5] It also supports innovation and entrepreneurship, driving economic growth.
- **Interconnection of Critical Sectors:** Communications networks are the backbone that connects critical sectors of our economy, such as energy, transportation, and financial services. Disruptions in these networks can then have cascading effects on other essential services.
- **Advancing Health Care:** Telemedicine and health information systems rely on robust communications

[1] Communications Sector | Cybersecurity and Infrastructure Security Agency CISA

[2] National Security Memorandum on Critical Infrastructure Security and Resilience, The White House, April 30, 2024.

[3] Communications Sector | Cybersecurity and Infrastructure Security Agency CISA

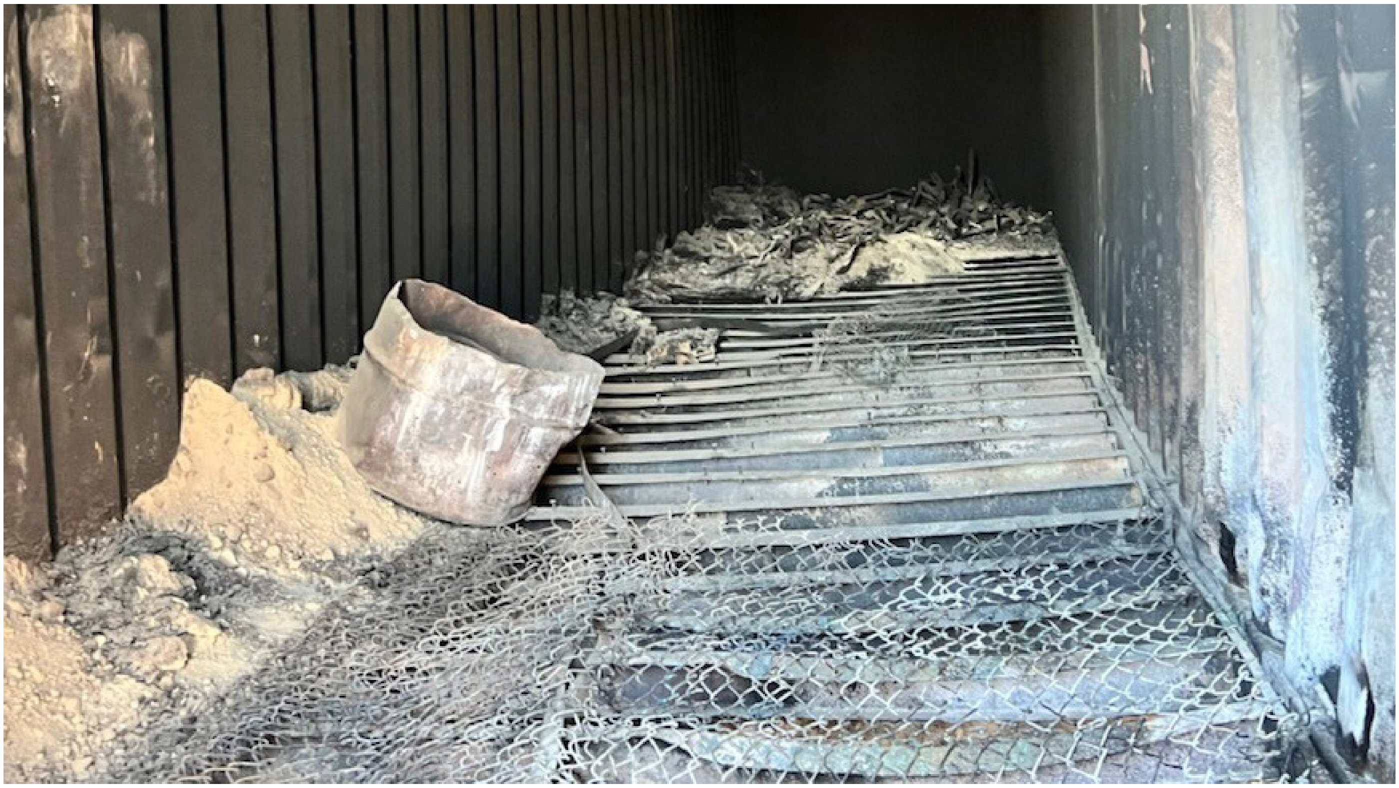
[4] The Importance of Telecommunications and Telecommunications Research | Renewing U.S. Telecommunications Research | The National Academies Press

[5] Why Infrastructure Matters: Rotten Roads, Bum Economy | Brookings

networks for efficient management and sharing of patient records, improving quality of care and amplifying public health communication. These technologies improve access to, and the quality of, care while also enhancing public health initiatives.

- **Education:** The COVID-19 pandemic highlighted the importance of internet connectivity for remote learning. Access to online resources and digital collaboration tools is crucial for students and educators. Communications networks make access to these resources, including e-learning platforms and digital libraries, which enable remote learning, support research, and facilitate collaboration amongst students, teachers, and educational institutions.
- **Financial Sector:** Communications networks enable real-time access to market data and seamless execution of financial transactions, market operations, and client transactions, by facilitating secure and reliable communications between institutions, clients, and internal operational systems.
- **Civic Engagement:** The internet enables citizens to stay informed about public services, participate in community events, and engage in the democratic process. It fosters informed civic activities by providing access to information on public services and community events, and supports digital participation to make it easier to engage in the democratic process.

All of these beneficial aspects of communications are threatened when vital portions of our critical infrastructure are dismantled by vandalism and theft.



Thieves installed a shipping container underground which was then used to burn sheathing off wires.

Threats Impact Other Critical Infrastructure

Communications networks are not the only critical infrastructure sectors facing significant threats from theft and vandalism.

Energy Infrastructure: Incidents of vandalism and theft targeting electrical substations and distribution systems are also increasing.[6] These acts can disrupt power supply, leading to outages and highlighting the vulnerability of the energy grid.[7] In April 2023, the North American Electric Reliability Corp. filed a report at the Federal Energy Regulatory Commission noting that physical security incidents resulting in a measurable grid outage as of the end of 2022 had increased 71% since 2021 and 20% since 2020.[8]

Transportation Systems: Vandalism and theft can damage transportation infrastructure, such as the communications systems that support our railways, bridges,[9] airports,[10] ports, and highways, as well as electric vehicle charging stations. These disruptions cause delays and safety hazards.[11]

Public Utilities: Water and sewage systems, street lights, traffic signals, and other public infrastructure are also at risk. Vandalism can lead to contamination or service interruptions, affecting public health and safety.

What Is Driving the Upsurge in Theft and Vandalism of Critical Infrastructure?

Global demand for copper is a major driving force for these crimes, with the metal's price soaring in recent years.[12] However, this is not a new problem. In 2008, the FBI released a report detailing the threat that copper theft posed to the country's infrastructure, noting that the price of copper had jumped over 500% in the preceding eight years.[13] The U.S. Department of Energy's 2023 Critical Materials Assessment report projects that demand for copper, a key material for energy technologies, will continue to grow significantly faster than supply, likely driving prices even higher.[14]

Today, bad actors typically target communications lines in search of copper. They steal encased copper cables and cut them into short lengths before burning them to remove the sheathing to reveal the raw

[6] https://www.electric.coop/vandalism-at-co-ops-knocks-out-power-destroys-equipment

[7] Human-Driven Physical Threats to Energy Infrastructure | National Conference of State Legislatures

[8] https://www.spglobal.com/marketintelligence/en/news-insights/latest-news-headlines/experts-eye-ways-to-mitigate-physical-assaults-on-us-power-grid-76888917

[9] https://www.latimes.com/california/story/2024-06-13/sixth-street-bridge-no-lights-copper-wire-theft

[10] Deliberately cut wires near SMF cause internet outage, some flights delayed - CBS Sacramento (cbsnews.com)

[11] Amid rising threats to critical infrastructure, CISA developing 'physical security' goals | Federal News Network

[12] In 2020, the average price for copper was approximately $2.80 per pound (Copper Prices - 45 Year Historical Chart | MacroTrends), as of October 2024, the price of copper is approximately $4.55 per pound, which represents nearly a 62.5% increase over the past four years.

[13] Precious Metal: Copper Theft Threatens U.S. Infrastructure | Federal Bureau of Investigation

[14] Critical Materials Assessments 2023 | U.S. Department of Energy

Stolen network equipment that has been recovered, but likely not reusable.

copper inside. That copper is then typically sold to scrap metal dealers, some of whom, in periods of high demand, are willing to accept the valuable commodity purportedly without knowing its origin.

Increasing vandalism has also impacted the fiber-optic networks that are now common in many broadband and wireless networks. While these high-bandwidth communications and data lines consist of glass optical fibers typically encased by plastic sheaths and do not contain copper, fiber components are often mistaken for the copper wires in telephone networks.

Theft does not stop at overhead wires; underground vaults and equipment boxes are also common targets, as are wireless network towers. Critical components, like bus bars and waveguides, are frequently targeted in wireless network towers due to the high-quality copper they contain.

In the search for copper, other critical infrastructure including utility poles, electric grids, EV charging stations, industrial property, construction sites, and water lines, suffer collateral damage and have also become targets themselves. Threats to communications infrastructure are not limited to acts of thieves in search of copper. These networks are also subject to incidents of vandalism committed by actors who intentionally attack communications infrastructure motivated by ideology or other criminal or national security intent.

Recent examples of such attempted theft and vandalism include:

- In Garland, TX, police responded to a group of thieves blocking traffic at 6 p.m. to steal copper wire and load it into a U-Haul. Police had to pursue the suspects, resulting in a short chase in the middle of rush hour, adding further risk to public safety. Police found $10,000 worth of copper had been stolen in this single hit.[15]
- In Los Angeles, CA, a surge in copper wire thefts led to extended outages, affecting everything from emergency services to daily business operations. Local authorities are struggling to curb the trend as the cost of repairs to replace the copper wire is already estimated to exceed half a million dollars.[16]
- In Philadelphia, PA, a person searching for copper cut a fiber-optic line during the 2023 Super Bowl, knocked out internet and television for tens of thousands of consumers hours before the Philadelphia Eagles were about to take the field. Finding only "worthless" fiber, the thief left empty-handed, leaving crews to splice the line back together and restore service mere minutes before kick-off.
- In Sacramento, CA, in April 2024, an intentional fiber cut at the Sacramento International Airport caused an internet outage that resulted in major flight delays for passengers.[17]
- In Austin, TX, in June 2024, an intentional fiber cut disrupted cell phone service at Austin-Bergstrom International airport and prevented passengers from making calls, using their cell network or pulling up mobile boarding passes.[18]
- In Denver, CO, during 2022, a sophisticated syndicate of copper thieves targeted a wireless carrier's small cell sites, stealing copper and causing significant damage. This resulted in $800,000 in damages to the carrier from June 2022 to February 2023, risked network security and operations, and negatively impacted residents of the affected neighborhoods. The wireless carrier provided information to the Police Department that led to the apprehension of a suspected ringleader, resulting in a dramatic reduction of the number of incidents and a significant decrease in damages to the sites.
- A Northern California and North Texas recycler and some of its employees were arrested after police executed search warrants on their business and home and recovered 1,000 pounds of stolen copper cable, hundreds of catalytic converters, cash, and drugs.
- In Fort Worth, TX, a technician and contractor walking a job site witnessed copper cable theft. The suspect pointed an AR-15-style assault rifle at them and was later arrested.
- Based on collaboration with AT&T's Global Security and Investigations team, MS Recycler alerted AT&T to a person who sold 250 pounds of burnt communication copper and planned to bring another 500 pounds the next day. The sheriff's office searched the premises and identified an additional aerial copper cable. The sheriff's office also linked the subject to numerous other thefts. Charges are pending, the estimated value is $25,000.

[15] Copper Thieves in North Texas and Across the U.S. Blamed for Disrupting Utilities | Dallas Observer

[16] L.A. is being 'stripped for parts.' Here's what the City Council wants to do about it | Los Angeles Times

[17] Deliberately cut wires near SMF cause internet outage, some flights delayed - CBS Sacramento (cbsnews.com)

[18] Network disruption stops AT&T, T-Mobile customers from making calls at Austin airport, KXAN News, March 18, 2024.

- A Texas consumer told a suspect to stop stealing copper critical infrastructure cable. The suspect fired a shot at the consumer, but the consumer was not injured.
- In Amador County, CA, in April and May 2023, cuts to fiber optic cables caused outages to 911 Emergency Services. Dispatchers were cut off from most of the 911 calls that were made due to the cable cuts. Three suspects were subsequently arrested.

In Bremerton, WA, in April 2024, Lumen had a copper cut that took down the airport at Bremerton. The cut also disrupted services at the local prison, Mission Creek Correctional, which created a significant security issue. This was just one of 69 cases of line cutting since the first of this year in Washington state. These thefts cost the company $500,000 just this year.

Altogether, thieves cause significant damage, leading to a troubling rise in internet and other communications network outages. While no particular geographic region is safe from these disruptions, the risk is especially high in rural and dense urban residential areas where wires mounted on utility poles and rooftop mounted communications equipment are tempting targets.

Critical Communications Networks Are High-Risk Targets Requiring Coordinated Action

While vandalism and theft on communications networks are not new problems, the frequency of these incidents has steadily risen at a time when daily life increasingly requires reliable connectivity. Communications networks provide connectivity for health care devices, health care providers, emergency response networks, public communications systems such as 911, municipal services, and other operations without which communities would be paralyzed in an emergency. The disruption caused by these malicious acts impacts the public's ability to access communications services, causing tangible harm, and making it imperative to prioritize vandalism and theft targeting these networks as a significant threat. More resources must be allocated and new policies implemented to protect this critical infrastructure. Industry, law enforcement, and policymakers need to work together to find impactful solutions.

A survey of large and small communications companies across the country found that, between June and December 2024, there were 5,770 reported incidents of intentional theft and/or vandalism targeting communications infrastructure—averaging 824 per month, or 27 incidents per day nationwide. Ten states accounted for 93% of the reported theft and vandalism incidents over this period, with California and Texas alone accounting for 51% of these incidents. The incidents collectively affected more than 1.5 million customers and cost communications providers millions of dollars in repair costs.[19]

[19] The data referenced in the preceding paragraph and the chart on the following page is limited to reported incidents from service providers participating in this report; the actual number of incidents damaging communications networks nationwide is unknown and likely higher than 5,770. Moreover, internal tracking of incident data varies by service provider, though many are now working to harmonize internal tracking to ensure better accounting of customer impact. Additionally, impact to business customers — including health care, finance, public safety, and commercial activity — is more difficult to quantify. The 5,770 customer impact statistic provides value in that it offers a general and limited measure of activity across states, but should not be considered a full accounting of activity.

Figure 1. Theft and Vandalism Incidents, June–December 2024

5,770
INCIDENTS NATIONWIDE

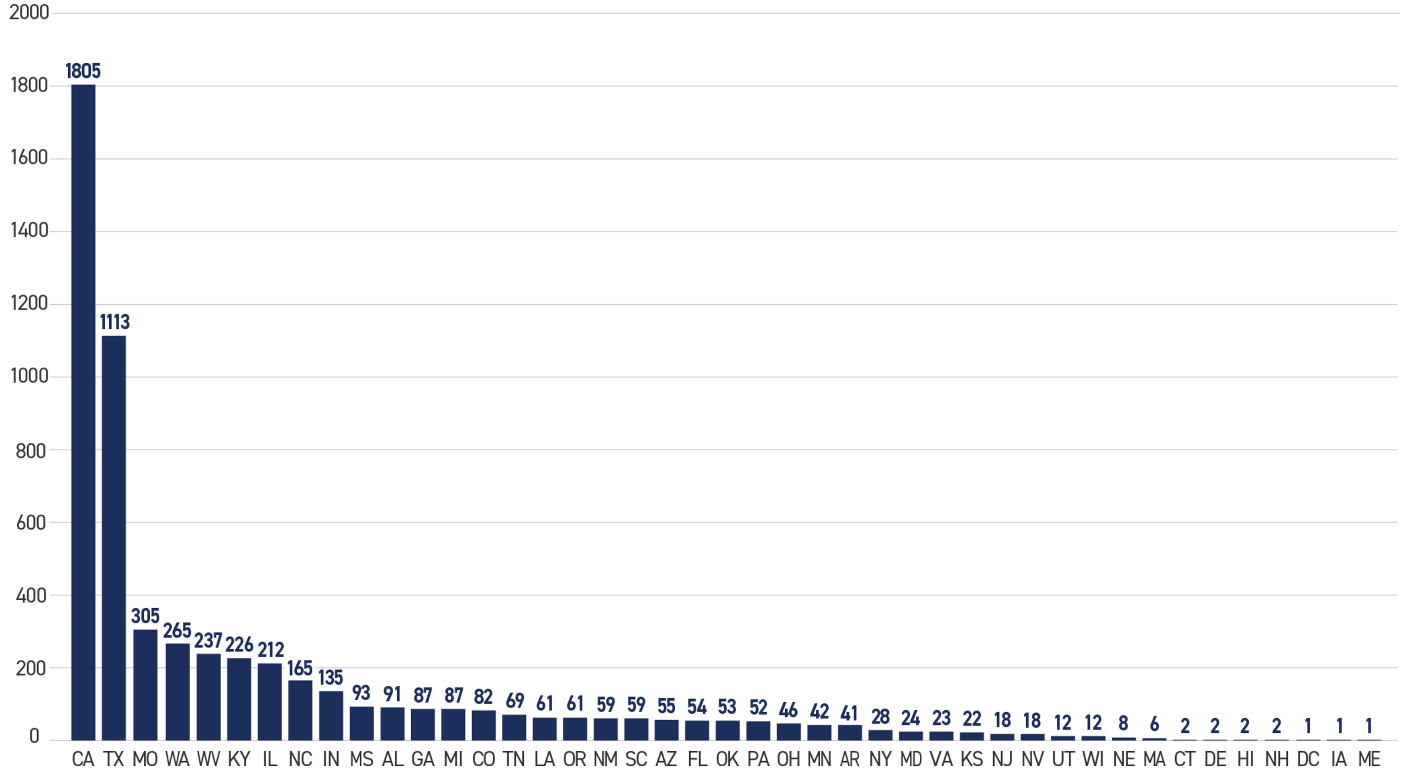
824
AVERAGE INCIDENTS PER MONTH

27
INCIDENTS PER DAY

1.5 M+
CUSTOMERS AFFECTED

Source: Survey of large and small ISPs across the country reporting incidents.

Figure 2. Incidents by State, June–December 2024



Threats to Communications Infrastructure Present Public Safety Risks

The disabling of critical communications networks due to vandalism and theft has a significant impact on essential public services like emergency response, health care, energy grids, and public transportation and can lead to broader societal costs and potential risks to public safety. A coordinated attack on a network can also have cascading effects, affecting law enforcement activity and jeopardizing local emergency systems.

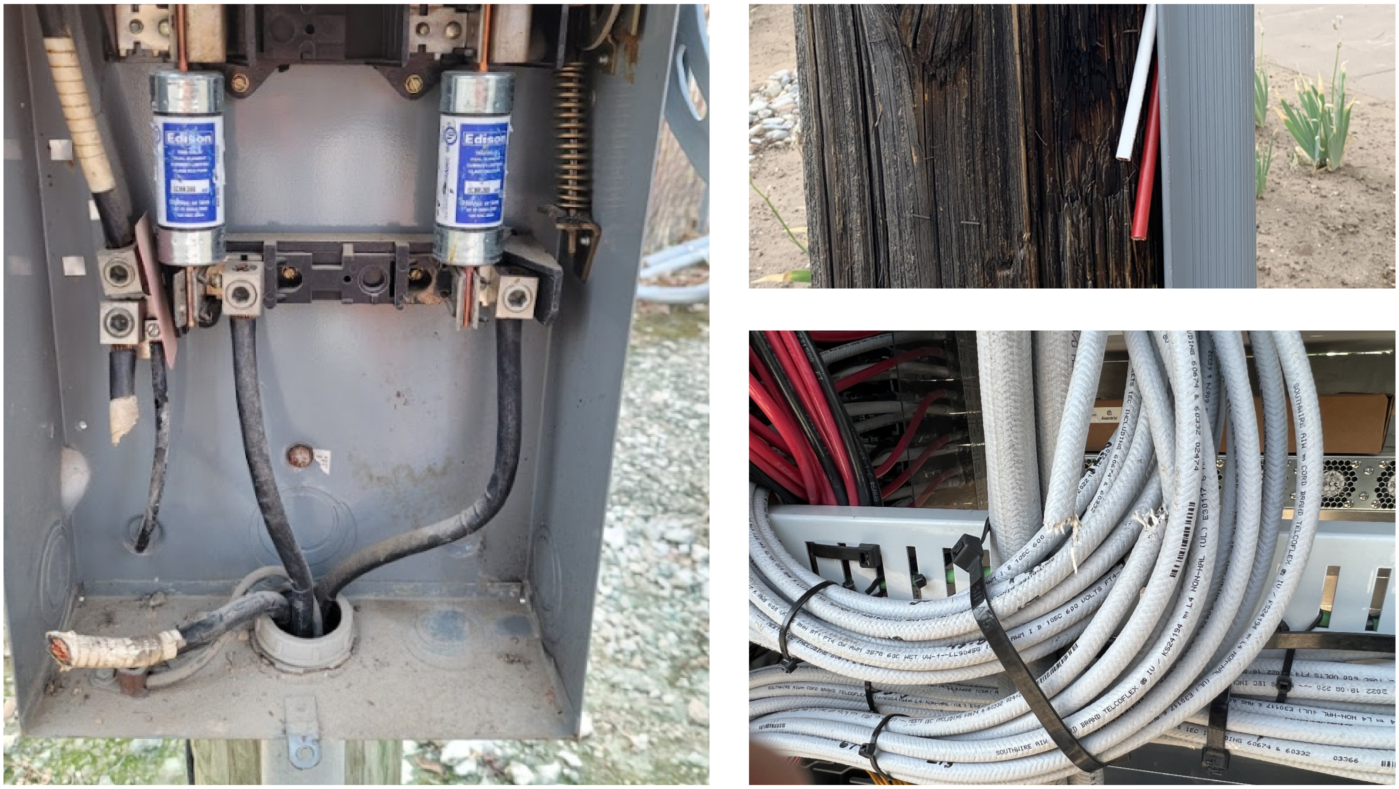
- Disruption of 911 systems and law enforcement communications can delay emergency response times, especially in rural or sprawled communities.
- Health care services heavily depend on broadband networks for patient care, access to medical records, medical devices, and telemedicine services.

Other critical services rely on electrical or other wiring that may be subject to theft or vandalism. For example, in April 2008, five tornado warning sirens in Jackson, Mississippi, did not sound because thieves had stripped the sirens of copper, an essential component to the equipment's ability to deliver the sirens.

Simply put, this type of theft has become a public safety issue for our nation.

Theft and Vandalism of Communications Infrastructure Have a Negative Economic Impact

Communications outages resulting from theft and vandalism have downstream effects that are equally problematic, costing businesses that rely upon reliable communications networks millions of dollars in economic damages. These events create delays in business operations that lead to lost productivity and revenue. Companies that rely on broadband and phone services, for instance, may face delays in transactions, customer service issues, and operational inefficiencies.



Left: Successful cuts and theft of wire in equipment cabinet. Top right: Cuts to wires on utility pole in conduit. Bottom right: Cuts to wires on utility pole in cabinet.

The cost of repairing and replacing stolen or damaged private communications infrastructure can be substantial. This includes not only the physical materials but also the labor and time required to restore services. While some incidents may lead to communications infrastructure damages of perhaps only $5,000 to $10,000, the biggest risk is that any single incident can lead to a disruption of emergency 911, law enforcement or other critical communications services, where the losses may be measured in hundreds of thousands of dollars or even loss of life.

Repairing damaged public utilities also results in millions of dollars in costs, with the expenses passed onto local jurisdictions, taxpayers or utility ratepayers. Unlike public utilities, however, communications providers that operate in a competitive marketplace cannot recover their costs from the regulated rate base; instead, they must bear the costs associated with restoration and repair of damage to their communications infrastructure. And in a competitive market, such costs may ultimately be borne by consumers.

To prevent future incidents, service providers may also need to invest in enhanced security measures, such as surveillance systems, security personnel, and advanced technology to protect their infrastructure, further increasing the costs of operating their networks and driving up costs for consumers.

How to Combat the Problem

Addressing the serious and growing problem of theft and vandalism targeting critical infrastructure requires coordination among a wide array of stakeholders, including the scrap metal industry, the communications industry, states and municipalities, law enforcement, and policymakers.

Need for Scrap Metal Industry Solutions

Any comprehensive solution must go beyond simply protecting communications infrastructure by addressing the demand side of copper transactions. For example, in 2014, the last time metal theft reached critical mass, the Institute of Scrap Recycling Industries launched StopMetalsTheft.org, a website that designed to educate and involve stakeholders, law enforcement, prosecutors, and the industry in curbing metal theft.

Ethical and transparent practices by scrap metal dealers are integral to preventing bad actors from vandalizing and stealing copper lines. When certain dealers fail to uphold these practices, it further complicates the ability to trace and recover stolen copper. It is critical to ensure that scrap metal dealers who prefer raw copper are aware the material they are purchasing is often stolen.

Proactive Measures Used by Communications Providers

Communications providers have implemented a broad array of solutions to try to address the problem of theft and vandalism, including:

- Directly engaging with state and local elected officials, County Supervisors, City Councils, Chambers of Commerce, City Managers, and Local District Attorneys to ensure the affected jurisdictions, public and other involved individuals are aware of the prevalence and consequences of cable thefts and how they can work with communications providers to effectively respond to theft.

- Enhancing relationships with law enforcement to facilitate quick alarm response and arrests.
- Working with utility coalitions on theft and vandalism issues.
- Offering monetary rewards for information leading to the arrest and conviction of individuals involved in copper theft and/or vandalism.
- Engaging in educational outreach and awareness with the recycling industry.
- Working with state legislatures to strengthen and enhance their state statutes related to metal theft.
- Increasing security measures, such as investing in enhanced site security measures, like surveillance systems, security personnel, and advanced technology (e.g., Ensurity trackers & AirTags) to protect their infrastructure.
- Working with landlords to improve building security and verify credentials before granting access to rooftop facilities.
- Managing their infrastructure to address the problem, whether by using metal pipes and casings at risers, downsizing cable and pairs, or facility service re-routing and trimming of trees from copper.
- Improving processes to better identify cable markings, preserve evidence of vandalism, and verify the legitimacy of contractors and employees.

State and Municipal Government Actions

State and local jurisdictions have also been adopting laws and implementing practices to help stem the tide of theft and vandalism against communications infrastructure. As of April 2025, 20 states are considering legislation aimed at addressing the problem—for example:

- **Alabama:** The state requires that if a party claims ownership of metal property in a recycler's possession and the recycler contests, the other party may bring legal action.
- **California:** The Los Angeles Police Department and Bureau of Street Lighting in 2024 formed a Copper Wire Task Force to address the issue of copper theft and vandalism which has resulted in eighty-two arrests and 2,000 pounds of recovered materials.[20]
- **Idaho:** Some cities have required sellers present ID to recyclers to combat the laundering of stolen metals.
- **Kentucky:** In March 2025, Governor Beshear signed into law legislation that includes equipment or communications lines used in the delivery of cable television, telephony or broadband service as critical infrastructure, and imposes enhanced felony penalties on bad actors that damage, possess or tamper with this key infrastructure.[21]
- **Michigan:** An individual that has been convicted of a crime involving theft, conversion, or sale of scrap

[20] 'Significant Victory': More Than 80 Arrested in Copper Wire Theft Crackdown | LATimes

[21] https://apps.legislature.ky.gov/record/25rs/sb64.html

metal may not enter a purchase transaction.

- **Minnesota:** The state requires licenses to sell scrap metal to dealers, similar to how the state requires licenses to sell catalytic converters to recyclers.[22]
- **Mississippi:** The state has made it unlawful to sell or for a dealer to purchase any copper telecommunications wire in any form or any metal property identified as belonging to a telecom company.
- **Missouri:** State law identifies communications networks and facilities as critical infrastructure and includes enhanced penalties for damage of communications networks.
- **North Carolina:** The state requires that a seller provide the physical address where they obtained the property, the date when the seller obtained the property and the license plate number, make, model, and color of the delivery vehicle.
- **Texas:** The Cities of Dallas and Fort Worth have both enacted local laws requiring scrap metal dealers to collect seller information prior to purchase. The Fort Worth Police Department's Metal Task Force and the Dallas Police Department have both dedicated resources to the investigation of metal-theft driven offenses.
- **West Virginia:** In 2024, the Kanawha County Sheriff's Office (SO) working in conjunction with the WV State Police, Charleston Police Department, Putnam County SO and Boone County SO targeted and investigated two recycling centers which resulted in multiple arrests and a significant decrease in cable theft activity.

Role of Law Enforcement

Left: Thief makes off on bike with severed wire and splicing box. Right: Truckload of stolen wires.

[22] Metal Thieves Are Stripping America's Cities | New York Times

- **Recognizing and prosecuting crimes:** Law enforcement plays a crucial role in recognizing, investigating, and prosecuting these crimes. With more focused attention and resources, law enforcement can have a positive impact on securing communications networks.
- **Tracking and patrols:** Assistance from all levels of law enforcement is needed to better track stolen materials, increase patrols in vulnerable areas, enhance data collection, and enhance tools for prosecuting offenders.
- **Assertive prosecution:** Local prosecutors should assertively prosecute these crimes to protect consumers and individuals who rely on communications infrastructure, recognizing that communication outages affect banks, hospitals, law enforcement, remote workers, and many such entities who can be seriously harmed by even short outages, especially in instances when multiple providers are attacked simultaneously.

Role of State Legislatures

The patchwork of fixes described above highlights the need for a more comprehensive solution, and more attention and involvement from state policymakers and regulators.

States take a variety of approaches, with some already making it a felony to damage critical infrastructure, which includes communications networks, while others have criminal statutes specifically addressing damage to communications infrastructure. Several states – such as Florida, North Carolina, South Carolina, and Tennessee – already properly classify those crimes as felonies and already correctly categorize communications networks as critical infrastructure. Kentucky became the first in the 2025 legislative session to pass a law that improves definitions and increases penalties.

However, many other states have no criminal statute specifically addressing damage to critical or communications infrastructure. Even in those states with existing criminal statutes with appropriate penalties, several states' critical infrastructure laws apply only when the subject property or equipment is enclosed (e.g., by a fence or other barrier), as in Alabama, Kansas, Louisiana, Montana, and Texas. Several other states' criminal laws apply only to a limited set of infrastructure that does not include communications networks, including Alabama, Louisiana, and Texas.

Regarding scrap metal, a similar patchwork applies: some states have a robust process for policing the sale and purchase of scrap metal, with appropriate penalties for violations of this process, while other states have weak or insufficient laws. States should examine their current laws and update them as needed. Core principles of any metal recycling regime should include at least:

- Required licensing
- Detailed recordkeeping of all transactions
- Access to sales database
- Prohibition of purchase of burnt copper
- Special certification for copper sales

- Legal holds on purchases of copper
- Penalties including license suspension
- Eliminate liability limitations

Role of the Federal Government

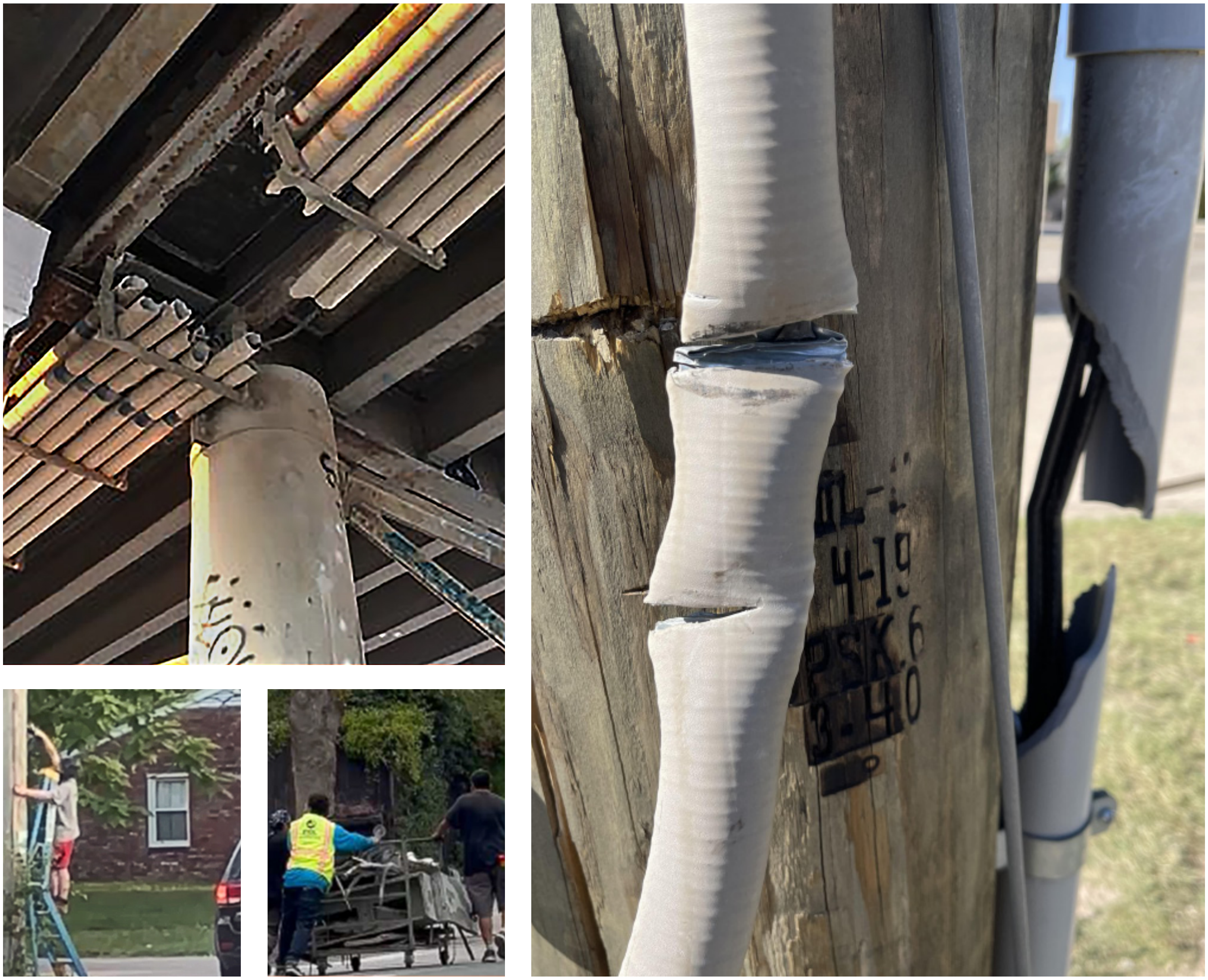
Concurrently with state legislative efforts, we encourage lawmakers to consider whether these acts of theft and vandalism should also be criminalized at the federal level. For example, federal law already criminalizes the willful or malicious destruction of federal government-operated and controlled communications networks (See 18 USC § 1362). This statute could be a model for federal action, or policymakers may consider alternative approaches that align with updated state laws. In any event, criminalizing this behavior would put communications networks on par with the destruction of other critical infrastructure, like energy facilities and transportation systems. (See 18 USC § 1366 and 18 USC § 1992, respectively).

Left: Vandalism of wire conduit on utility pole. Top right: Underground wire vault broken into and vandalized. Bottom right: Trailer full of stolen wires.

Conclusion

The rise in copper wire theft and vandalism raises serious concerns about the vulnerability of America's critical infrastructure. To protect economic and public safety interests, regulators, legislators, law enforcement, municipalities, and communications providers must work together to address this growing threat.

As past incidents have shown, vandals and thieves can target critical infrastructure and cause significant damage. With proper coordination and enhanced criminal penalties, however, partnerships across industry and government can develop effective strategies to safeguard critical communications infrastructure against vandalism, theft, and attacks and secure their communities.



Top Left: Severed wire conduits located beneath a bridge. Bottom Left: Individuals in the process of extracting and fleeing with stolen communication wires. Right: Vandalized wire conduit on a utility pole.

Addendum

Originally published November 2024 | Revised April 2025

This second edition of "Protecting the Nation's Critical Communications Infrastructure from Theft & Vandalism" includes updates throughout, incorporating responses from a second survey of large and small communications companies nationwide, covering incidents from June to December 2024. It also reflects recent state actions and introduces new tables detailing damage by type of vandalism and by location.

Reference Charts

A survey of large and small communications companies across the country for incidents from June to December 2024 reveals there were 5,770 reported incidents of intentional acts of theft and/or vandalism of communications infrastructure nationwide, averaging 824 per month or 27 incidents per day. Ten states accounted for 79% of the reported theft and vandalism incidents over this period, with California and Texas alone accounting for 51% of these incidents. The incidents collectively affected more than 1.5 million customers and cost communications providers millions of dollars in repair costs.

The data referenced in the preceding paragraph and the chart below is limited to reported incidents from service providers participating in this report; the actual number of incidents damaging communications networks nationwide is unknown and likely higher than 5,770. Moreover, internal tracking of incident data varies by service provider, though many are now working to harmonize internal tracking to ensure better accounting of customer impact. Additionally, impact to business customers — including health care, finance, public safety, and commercial activity — is more difficult to quantify. The 5,770 customer impact statistic provides value in that it offers a general and limited measure of activity across states, but should not be considered a full accounting of activity.

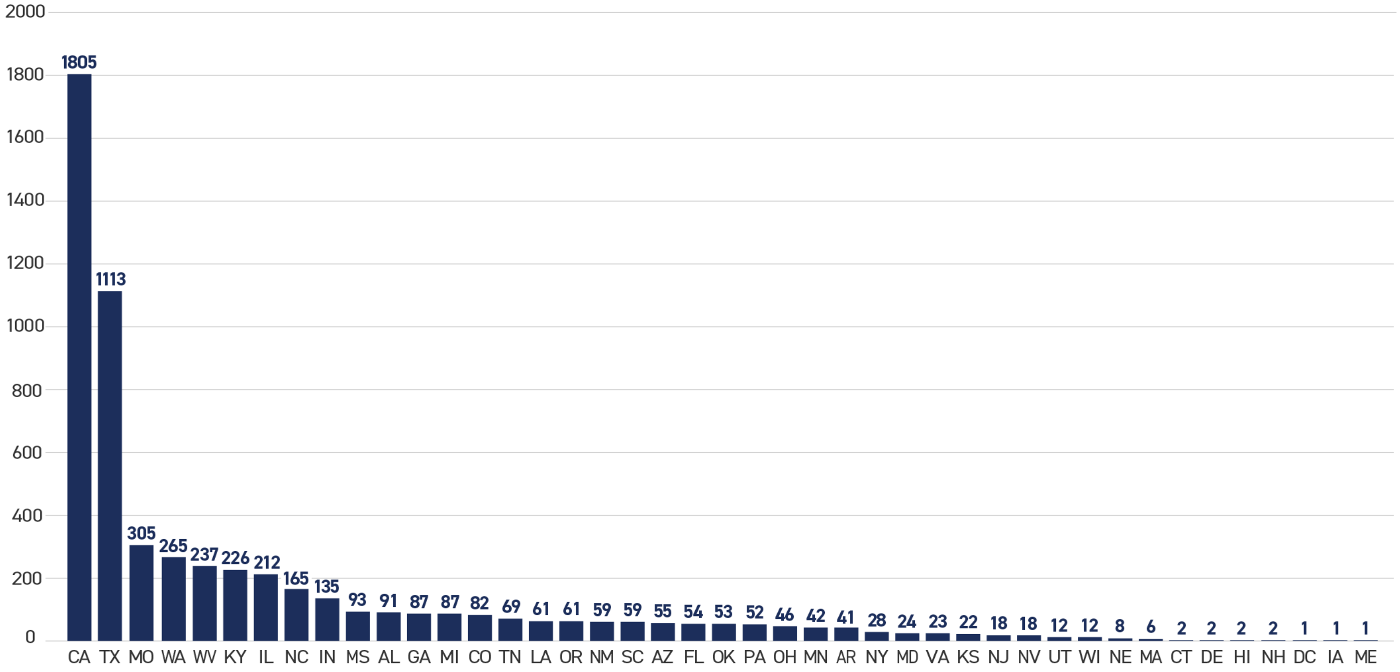
Figure 1. Theft and Vandalism Incidents, June–December 2024

5,770	**824**	**27**	**1.5 M+**
INCIDENTS NATIONWIDE	AVERAGE INCIDENTS PER MONTH	INCIDENTS PER DAY	CUSTOMERS AFFECTED

Source: Survey of large and small ISPs across the country reporting incidents.

Note: This chart has been included on page 8 of the main report.

Figure 2. Incidents by State, June–December 2024



Note: This chart has been included on page 8 of the main report.

Figure 3. Incidents by Damage Location, June–December 2024

The table below describes the location of vandalized infrastructure. This infrastructure covers millions of miles connecting critical infrastructure, essential services, businesses, and customers in a resilient manner across the country. The table shows the reported locations where criminals vandalize U.S. telecommunications critical infrastructure.

DAMAGE LOCATION	# OF INCIDENTS
Aerial/Aerial Cables	1486
Facility	107
Buried	96
Ground/Above Ground Pedestal	128
Other*	114
Underground (Vault, Cables, Pedestal)	99
Poles	37
Above Ground Doghouse	18
Unknown	29

* "Other" includes damage locations reported in fewer than 3 incidents or uncategorized entries.

Figure 4. Types of Vandalism Damage, June–December 2024*

This table describes the types of vandalism committed by criminals over the seven month period in 2024. The most common vandalism was to cabling hung on utility poles along with cabling that transcends down the pole to a ground based vaults or cabinets before it travels to customer homes. The table shows the types of vandalism that causes outages to other critical infrastructure entities, essential services, businesses and customers.

DAMAGE TYPE	# OF INCIDENTS
Cuts into Copper & Fiber	1915
Aerial Damage	1300
Other**	647
Ground Copper Damage	567
Unknown	452
Copper & Cable Theft	251
Copper Buss Bar	240
Power Cable/Rectifiers	114
Fiber Cable	90
Copper, Pedestal	50
Power Cables	44
Gun Shot	50
Batteries	30
Arson	21
Company Property	18
Engineering Equipment	17
Fire	12
Acts Against Corporation - Vandalism/Sabotage	18
Hybrid & Grounding Cables	25
Grounding Equipment	6
Accidental Damage	5
Vehicle	5

* While each incident varies in scope and severity, data from this period indicate that on average, approximately 2,000 customers were affected per outage caused by vandalism or theft, with an average outage duration of 138 hours.

** "Other" includes damage types reported in fewer than 3 incidents or uncategorized entries.