



FALL

2025

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

Originally published November 2024.
Updated April 2025 and October 2025.





Table of Contents

Executive Summary	1
National Communications Infrastructure is Essential	3
Threats Impact More Than Communications Infrastructure	4
What's Driving the Upsurge in Theft and Vandalism?	5
Protecting High-Risk Communications Networks Requires Coordinated Action	7
Threats to Communications Infrastructure Present Public Safety Risks	9
The Economic Impact of Theft and Vandalism on Communications Infrastructure	10
How to Combat the Problem	10
Conclusion	16
Addendum	16



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 — including public safety, health care, energy, transportation, finance, information technology, and education — increasingly rely on communications infrastructure. When the fiber optics providing communications services to critical institutions like airports, hospitals, and fire and police stations is cut, this can affect and jeopardize the safety of millions of people. 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 has created powerful economic incentives to target multiple industries' infrastructure (e.g., public utilities, transportation, etc.) nationwide through criminal acts of theft and vandalism. As previously reported in April 2025, from June to December 2024, more than **5,770** incidents of intentional theft or sabotage targeting communications networks were reported. The updated paper reveals that in the following six months, January to June 2025, reported incidents surged to **9,770** — nearly doubling the prior period. Over a full year, this totals more than **15,540** incidents, underscoring the scale and accelerating pace of the threat. Even modern fiber optic networks and wireless communications towers and equipment, which contain no copper, have been sabotaged in indiscriminate searches for scrap material.

These crimes disrupt essential services, impose millions of dollars in repair costs, and endanger public safety by threatening emergency communications, hospitals, airports, military installations, and other public safety institutions. Fiber cuts and related acts can paralyze critical operations, creating cascading disruptions that may affect millions of citizens simultaneously.

A critical driver of this activity is the ease with which stolen materials and equipment can be sold to scrap metal dealers and resellers, often with limited oversight or accountability. Addressing the demand side of this illicit market is as important as securing the networks themselves. Stronger regulation, tighter transaction requirements, and enhanced enforcement at the state and local levels are urgently needed to reduce the incentive for theft.

In response, communications providers, state governments, law enforcement, and federal lawmakers have taken important steps. States such as Kentucky, Texas, and Minnesota have strengthened critical infrastructure protections and expanded felony classifications for theft and vandalism. Municipal initiatives in Los Angeles and Louisville have led to arrests and recovery of stolen materials. At the federal level, H.R. 2784 — The Stopping the Theft and Destruction of Broadband Act of 2025 — has been introduced to close statutory gaps and criminalize attacks on privately owned communications networks nationwide.

While acknowledging these efforts and the progress achieved in increasing awareness of this growing problem, this paper highlights:

- The scale of theft and vandalism incidents and their economic and safety consequences;
- The greater need for collaboration among the communications industry, the scrap metal industry, state and local jurisdictions, law enforcement and lawmakers;
- The critical role of scrap metal dealers and resellers in enabling these crimes, and the urgent need for stricter oversight and regulation;
- 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;
- The need to examine and update existing state statutes to ensure laws are in place or strengthened to penalize intentional theft or vandalism of critical infrastructure, cover all aspects of communications networks, and ensure enhanced penalties are enforced to deter future bad acts.



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

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 systems³ 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 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.

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](#)

- **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.

Threats Impact More Than Communications Infrastructure

When vandals and thieves target communications infrastructure, they disrupt much more than networks. Other critical infrastructure sectors face similar risks:

- **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.

These attacks show that communications vandalism and theft is part of a broader trend threatening multiple critical infrastructure sectors.

6 [Vandalism at Co-ops Knocks Out Power, Destroys Equipment | National Rural Electric Cooperative Association \(NRECA\)](#)

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

8 [Experts eye ways to mitigate physical assaults on US power grid | S&P Global](#)

9 [Copper thieves leave 6th Street Bridge — the ‘Ribbon of Light’ — completely in the dark | Los Angeles Times](#)

10 [Deliberately cut wires near SMF cause internet outage, some flights delayed | CBS Sacramento](#)

11 [Amid rising threats to critical infrastructure, CISA developing ‘physical security’ goals | Federal News Network](#)



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

What's Driving the Upsurge in Theft and Vandalism?


Soaring global demand for copper fuels these crimes.¹² 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 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.

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](#)



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:

- **Garland, TX:** Police responded to 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
- **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
- **Philadelphia, PA:** During the 2023 Super Bowl, a person searching for copper cut a fiber-optic line, knocking 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.
- **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
- **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
- **Northern California and North Texas:** A 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.

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.](#)

- **Bremerton, WA:** In April 2024, a copper cut shut down the local airport and disrupted Mission Creek Correctional, creating a major security risk. It was one of 69 line-cutting incidents in the state this year, costing Lumen over \$500,000.
- **Parkland, WA:** In April 2025, thieves were caught on video stealing \$55,000 worth of copper wire and cables, using a forklift stolen from the same company. The company has requested to remain anonymous for safety reasons.¹⁹
- **Los Angeles, CA area:** In June 2025, thirteen cable lines were cut, disrupting service for more than 50,000 people. Critical services were affected, including a U.S. military base, 911 and emergency dispatch, public safety agencies, financial institutions, courts, hospitals, and schools.²⁰
- **Oregon and Washington:** Companies have been facing a huge uptick in copper wire theft, with the number of theft and vandalism incidents doubling in 2025 compared to 2024.²¹
- **Jefferson County, MO:** Wire theft impacted hospitals, schools, and 911 services across the county. A local investigation led to felony charges against two individuals stealing wires in their search for copper.²²

Protecting High-Risk Communications Networks Requires Coordinated Action

While vandalism and theft on communications networks are not new problems, their frequency has steadily risen as 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.

Between January and June 2025, communications companies across the country reported 9,770 incidents of intentional theft and/or vandalism targeting their infrastructure—an average of 1,297 per month, or 43 incidents each day nationwide. Just ten states accounted for 80% of these attacks, with California and Texas alone accounting for over half (53%). Together, these incidents disrupted service for over 9.5 million

19 [Thieves Steal \\$55k Worth Of Copper Wire, Cables From Pierce County Company, King5.](#)

20 [Internet outage was 'domestic terrorism,' Spectrum says KTLA5](#)

21 [Companies try to combat copper wire theft as incidents spike in Oregon, Washington KGW8](#)

22 [Wire thefts lead to felony charges in Jefferson Co., Fox2now](#)

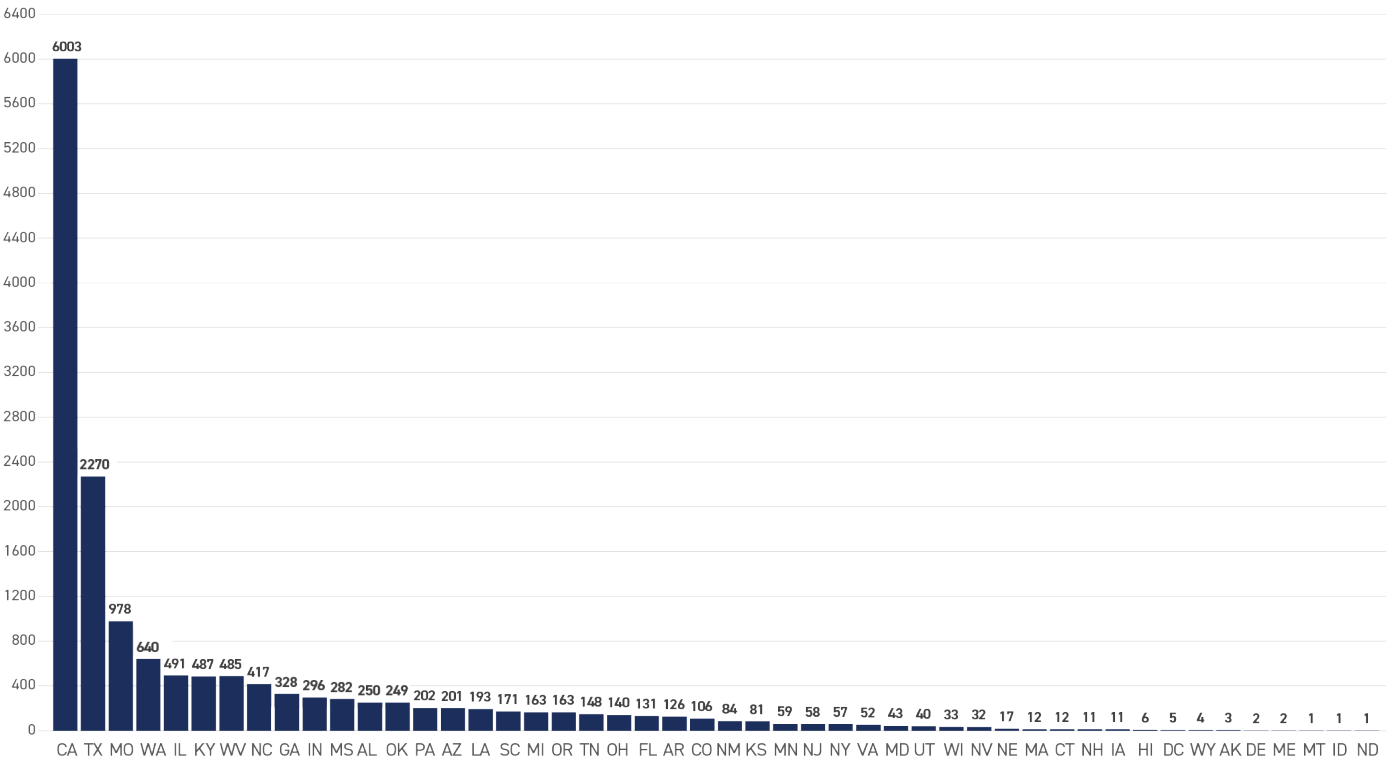
customers and forced providers to spend millions on repairs.²³ This concentration of activity highlights where coordinated action—by law enforcement, legislators and industry—can have the greatest impact in reducing future incidents.

Figure 1. Theft and Vandalism Incidents, June 2024–June 2025



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

Figure 2. Incidents by State, June 2024–June 2025



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

23 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 15,540. 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 9.5+ million 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.

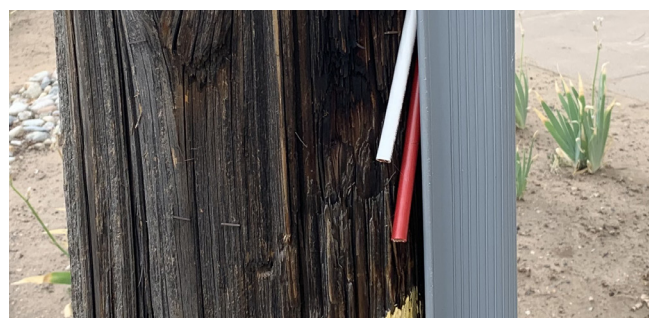
Threats to Communications Infrastructure Present Public Safety Risks

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. When fiber is cut, the consequences extend far beyond inconvenience: hospitals can lose access to life-saving telemedicine and patient data, airports can face widespread delays and cancellations affecting millions of travelers, military installations can experience compromised communications and police, fire, and 911 systems can be disabled when citizens most urgently need them. 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.



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 Economic Impact of Theft and Vandalism on Communications Infrastructure

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.

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, recognizing that protecting critical infrastructure requires not only physical safeguards but also engagement with communities, law enforcement, and policymakers. These proactive measures include:

- 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.
- Hosting educational and liaison events across the country with local law enforcement, prosecutors, government agencies, and utility partners to strengthen collaboration, share best practices and enhance coordinated responses to theft and vandalism.
- Enhancing relationships with law enforcement to facilitate quick response, investigations, and arrests.
- Creating and broadcasting PSAs with local prosecutors and law enforcement to educate about the dangers and consequences communications infrastructure attacks.
- 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, accompanied by outreach campaigns to raise public awareness and encourage reporting of suspicious activity.
- 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.
- Collaborating with landlords to improve building security and verify credentials before granting access to rooftop facilities.
- Managing infrastructure to mitigate theft risks, including using metal pipes and casings at risers, downsizing cable and pairs, or facility service re-routing and trimming of trees from copper.
- Improving internal processes to better identify cable markings, preserve evidence of vandalism, and verify the legitimacy of contractors and employees.

Through this combination of partnerships, public education, deterrence incentives, and technical safeguards, communications providers are working to protect networks, strengthen deterrence and build broader community support in combating these crimes.

State and Municipal Government Actions

State and local jurisdictions have continued to adopt laws and implement practices aimed at stemming the tide of theft and vandalism against communications infrastructure. These actions, which complement broader legislative efforts at both the state and federal levels, reflect a growing recognition of the scope and severity of the problem. In 2025, 23 states considered legislation, and 13 of those enacted new laws strengthening critical infrastructure protections, while several municipalities have partnered with law enforcement to launch dedicated task forces. The following examples highlight recent measures and illustrate the varied approaches taken to address this issue at the state and local level:

- **Alabama:** If a party claims ownership of metal property in a recycler's possession and the recycler contests, the other party may bring legal action. In 2025, the state passed a law to expand the definition of critical infrastructure and removed a fencing requirement to impose penalties.
- **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. Additionally, in 2025, the California legislature passed a law prohibiting the unauthorized purchase and processing of communications equipment by scrap metal recyclers. The bill has not been signed by the Governor as of the publication of this report.
- **Idaho:** Some cities have required sellers present ID to recyclers to combat the laundering of stolen metals.
- **Indiana:** In 2025, the definition of critical infrastructure was amended to expressly include communications facilities such as cell towers, wires, and equipment.
- **Kentucky:** In March 2025, Governor Beshear signed legislation classifying equipment or communications lines used in the delivery of cable TV, telephony, or broadband service as critical infrastructure, with enhanced felony penalties for damage, possession, or tampering.
- **Louisiana:** In 2025, the definition of critical infrastructure was expanded to include communications network equipment, with new penalties for theft.



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

- **Michigan:** Individuals convicted of crimes involving theft, conversion, or sale of scrap metal may not enter purchase transactions.
- **Minnesota:** Requires licenses to sell scrap metal to dealers, similar to licenses required to sell catalytic converters to recyclers. In 2025, the law penalizing damage to telephone lines was expanded to cover cable and broadband lines, with enhanced penalties.
- **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:** Communications networks and facilities are classified as critical infrastructure, with enhanced penalties for damage.
- **North Carolina:** Sellers must provide the physical address where they obtained the property, the date obtained, and the license plate number, make, model, and color of the delivery vehicle.
- **Texas:** The Cities of Dallas and Fort Worth enacted local laws requiring scrap metal dealers to collect seller information before purchase. The Fort Worth Police Department's Metal Task Force and the Dallas Police Department both dedicated resources to investigating metal-theft-driven offenses. In 2025, the definition of critical infrastructure was expanded to include communications networks and equipment, with enhanced penalties for theft of equipment or components containing brass or copper.
- **West Virginia:** In 2024, the Kanawha County Sheriff's Office, working with the WV State Police, Charleston Police Department, Putnam County SO, and Boone County SO, targeted and investigated two recycling centers, resulting in multiple arrests and a significant decrease in cable theft activity.

Role of Law Enforcement

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

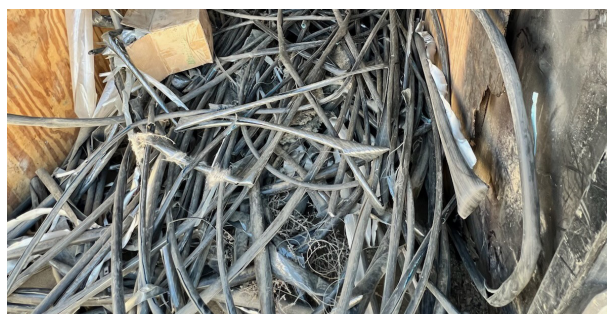
Current state laws on theft and vandalism against telecommunications infrastructure are inconsistent. To be effective, more comprehensive solutions are needed. State legislatures have an opportunity to have a substantial impact through reforming damage statutes to include critical telecommunications infrastructure

as well as imposing additional rules on the scrap metal dealing and secondary metals recycling processes, which often serve as conduits for stolen materials.

In 2025, as mentioned above, 23 states introduced bills to close gaps in protection, and 13 of those enacted new laws that strengthen critical infrastructure protections. These include removing outdated “fenced-in” enclosure requirements, explicitly covering communications networks, and expanding felony classifications for damage. Despite this progress, many states still do not require strict oversight of transactions involving scrap or restricted metals. To substantially reduce the risk of theft and illicit profit, state legislation should include specific regulatory requirements for scrap metal commerce.

States (such as Florida and Texas) and certain municipalities (such as Louisville, KY) have adopted strong regulations that illustrate this model. These regulations include, but are not limited to, the following key elements: licensing or registration of secondary metal recyclers and dealers; retention of digital copies of the seller’s photo ID; photos of the seller at the time of sale; photo evidence of the property being sold (including vehicle and license plate where applicable); detailed transaction descriptions; prohibitions on cash transactions for restricted metals with payment by check, and prompt electronic reporting of such purchases to law enforcement with comprehensive identifying information. These provisions help raise the barrier for bad actors to move stolen equipment through scrap dealers and help reduce the economic incentive that continues to drive attacks on critical communications infrastructure.

While 2025 saw important progress, state legislatures should continue to build on this momentum by crafting legislation that ensures protections for telecommunications as a part of incorporates these scrap metal regulatory measures. Such measures work in tandem with stronger damage statutes to protect communications infrastructure more effectively.

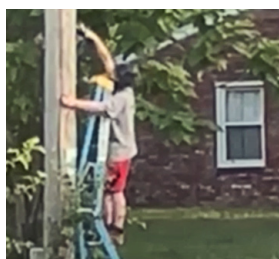


Left: Vandalism of wire conduit on utility pole. Top right: Underground wire vault broken into and vandalized. Bottom right: Trailer full of stolen wires.

Role of the Federal Government

Federal lawmakers are also beginning to recognize that this problem must be addressed at the national level. In April 2025, H.R. 2784, the Stopping the Theft and Destruction of Broadband Act of 2025, was introduced in Congress by Rep. Laurel Lee (R-Florida) and Rep. Marc Veasey (D-Texas). This proposal would amend Title 18, Section 1362 of the U.S. Code so that willful or malicious acts against private communications networks—not just systems controlled or operated by the government—are explicitly criminalized at the federal level.

While existing statutes reach government-targeted attacks, a gap remains in protecting the vast array of privately owned networks that form the backbone of virtually every modern service on which we rely—from emergency response and healthcare to transportation, finance, energy, and beyond. By extending Title 18's provisions to apply to all critical infrastructure, H.R. 2784 seeks to close this loophole and ensure that all perpetrators face the full weight of the law.



Top Left: Severed wire conduits located beneath a bridge. Bottom Left: Individuals in the process of extracting and fleeing with stolen communication wires. Right: Compromised door protecting network infrastructure.



Conclusion

The sharp rise in theft and vandalism—over 15,540 reported incidents in the past year—demonstrates the urgent vulnerability of America's critical infrastructure. These acts not only impose millions in economic damages but also jeopardize public safety by disrupting 911 systems, hospitals, airports, and other essential services.

A critical driver of these crimes is the ease with which stolen materials and equipment can be sold to scrap metal dealers and resellers with little oversight. Without stronger regulation of these transactions—through requirements such as photo identification, transaction reporting, and prohibitions on cash purchases—the economic incentive for theft will remain high and progress on other fronts will be undermined.

Encouragingly, important steps have been taken. Communications providers have strengthened site security and deepened collaboration with law enforcement. More than a dozen states have enacted stronger laws, both expanding felony classifications for theft and imposing tighter rules on scrap metal transactions. At the federal level, H.R. 2784—the Stopping the Theft and Destruction of Broadband Act of 2025—seeks to close gaps in criminal protections for privately owned communications networks.

To build on this momentum, regulators, legislators, law enforcement, municipalities, and providers act in unison. Comprehensive solutions must focus not only on securing communications infrastructure but also on addressing the demand side of the illicit market. By enforcing stronger oversight of scrap metal dealers and resellers alongside tougher penalties for vandalism and theft, the nation can reduce incentives for these crimes, protect critical communications networks, and safeguard the economic and public safety interests of all Americans.

Addendum

Mapping Incident Hotspots Across the Most Impacted States

The following analysis shows the five states with the highest reported activity—California, Texas, Missouri, Washington, and Illinois—revealing where these crimes are most concentrated. These state-level heatmaps and tables depict the top 25 affected cities in these five states.

(continued on the next page)

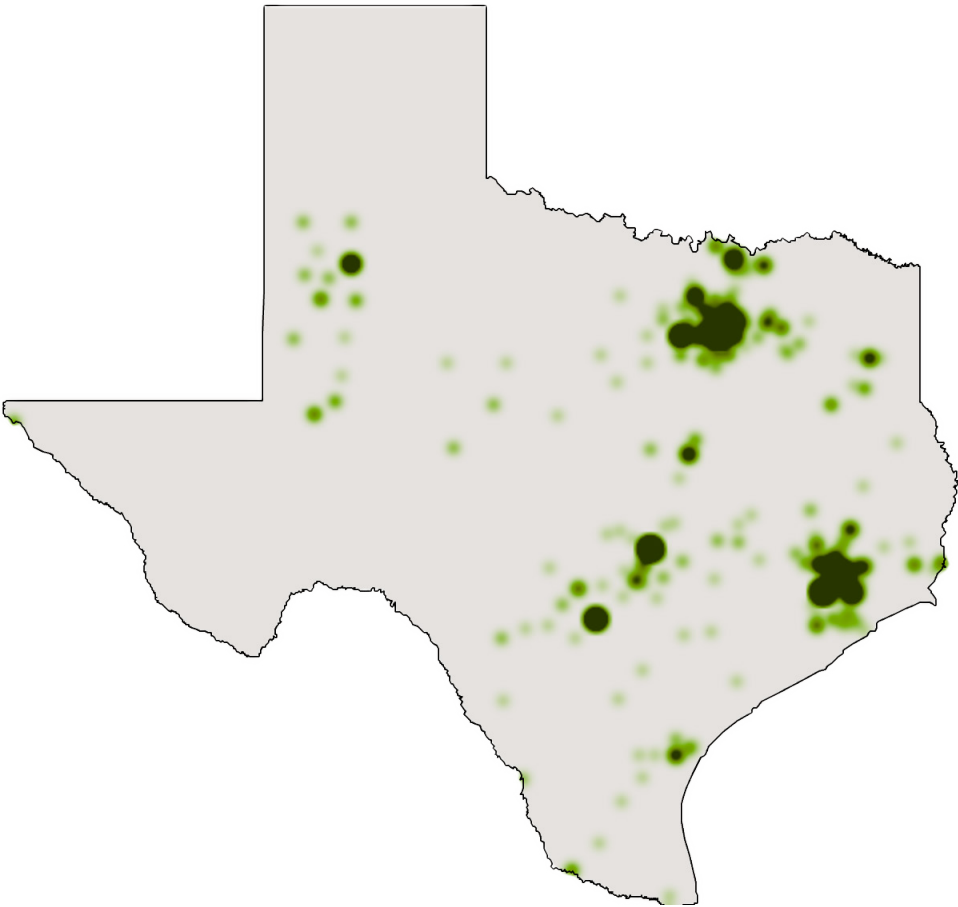
Figure 3. California Vandalism Incidents: State Heatmap and 25 Hardest-Hit Cities, June 2024–June 2025



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

CITY	COUNT
Los Angeles	991
Stockton	255
Richmond	225
Sepulveda	153
Riverside	150
San Jose	106
Northridge	94
Barstow	90
Reseda	89
Huntington Park	87
Van Nuys	80
Norwalk	74
Bakersfield	71
South Gate	71
El Sobrante	71
North Hollywood	68
Victorville	67
Fresno	66
Jurupa Valley	64
Oroville	64
Hayward	62
San Bernardino	60
Compton	60
Gardena	59
Granada Hills	59

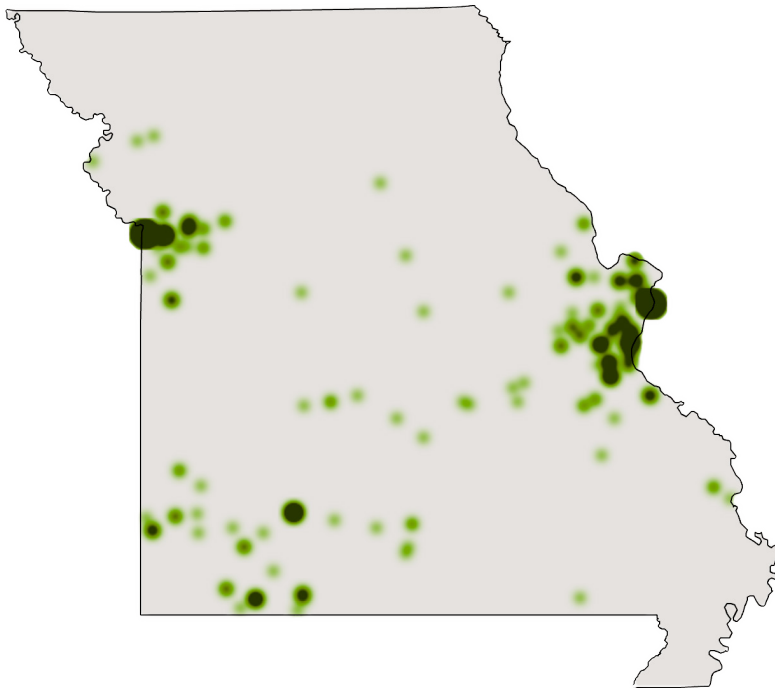
Figure 4. Texas Vandalism Incidents: State Heatmap and 25 Hardest-Hit Cities, June 2024–June 2025



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

CITY	COUNT
Dallas	438
Houston	244
Austin	194
San Antonio	91
Fort Worth	78
Garland	74
Baytown	51
Irving	42
Crosby	36
Humble	34
Sherman	32
Huffman	32
Lubbock	30
Kingwood	28
Plano	26
Denton	22
Mesquite	21
Spring	17
Lorena	14
Arlington	11
Rowlett	10
Dayton	10
Corpus Christi	10
Longview	10
Carrollton	9

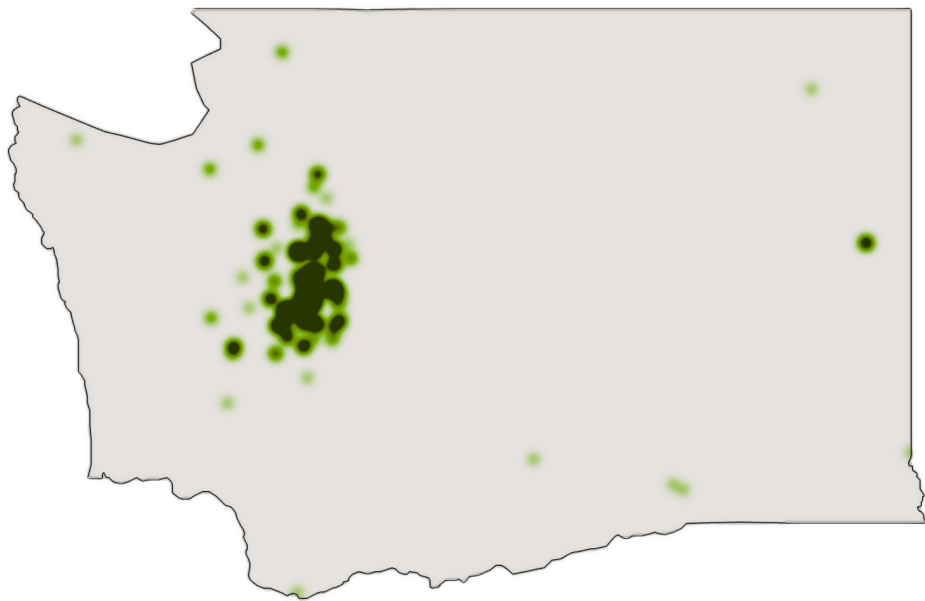
Figure 5. Missouri Vandalism Incidents: State Heatmap and 25 Hardest-Hit Cities, June 2024–June 2025



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

CITY	COUNT
St. Louis	326
Kansas City	267
Independence	28
Springfield	20
Imperial	15
Cedar Hill	11
De Soto	11
Hillsboro	9
Shell Knob	9
Arnold	7
Buckner	6
High Ridge	5
St Charles	5
Florissant	5
Fenton	5
Joplin	5
Wentzville	5
Barnhart	5
Bloomsdale	5
Portage Des Sioux	4
Harrisonville	4
Sibley	4
Branson	4
Carthage	3
St. Clair	3

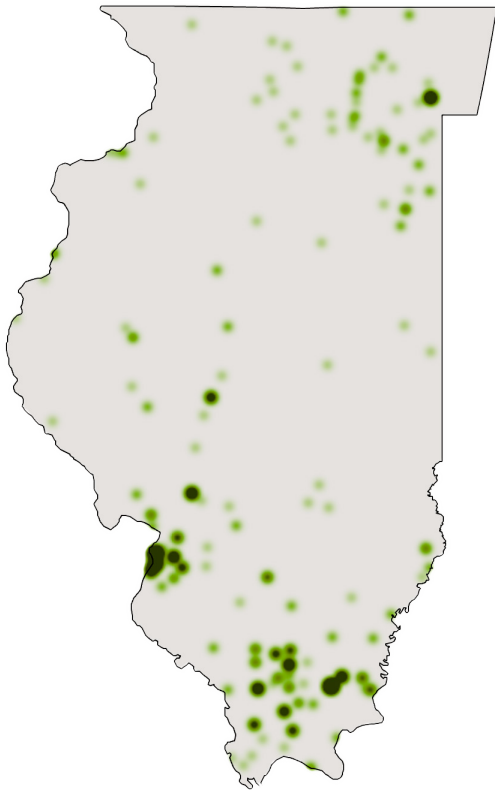
Figure 6. Washington Vandalism Incidents: State Heatmap and 25 Hardest-Hit Cities, June 2024–June 2025



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

City	COUNT
Kent	109
Tacoma	48
Auburn	39
Renton	35
Seattle	30
Maple Valley	25
Bellevue	18
Woodinville	17
Federal Way	16
Lakewood	12
Bonney Lake	11
Sammamish	11
Redmond	10
Sumner	9
Issaquah	9
Puyallup	8
Graham	8
Seatac	8
Olympia	7
Enumclaw	7
Spokane	7
Gig Harbor	7
Poulsbo	6
Lynnwood	6
Spanaway	6

Figure 7. Illinois Vandalism Incidents: State Heatmap and 25 Hardest-Hit Cities, June 2024–June 2025



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

City	COUNT
Harrisburg	47
Granite City	42
East St. Louis	24
Chicago	19
Gillespie	15
Carbondale	14
West Frankfort	14
Eldorado	13
Collinsville	13
Goreville	10
Springfield	9
Cahokia	9
Anna	7
Vienna	7
O'Fallon	7
Christopher	7
Benton	6
Edwardsville	6
Centralia	5
Ridgway	5
Shawneetown	5
Sauget	4
Herrin	4
Elkville	4
Du Quoin	4

