June 2026

PROTECTING CRITICAL COMMUNICATIONS INFRASTRUCTURE:
EMERGING THREATS & NEEDED SOLUTIONS

Overview

The nation's communications infrastructure is a foundational component of critical infrastructure, supporting public safety, national defense, health care, transportation systems, financial markets, and daily life. Disruptions to these networks can cascade across sectors, making attacks a significant public safety and economic threat.

Attacks on communications networks have escalated in recent years with more than 18,000 incidents nationwide, affecting over 11.8 million customers. This theft and vandalism are driven in part by scrap metal resale incentives, limited oversight of secondary metals transactions, and legal gaps that leave communications assets insufficiently protected. These crimes jeopardize essential services and impose substantial repair and operational costs across the economy.

Addressing this threat will require stronger scrap-metal oversight, clearer critical infrastructure protections, enhanced penalties, and deeper coordination among providers, law enforcement, municipalities, and policymakers.

Scope & Scale of the Problem

Provider-reported data show a rapidly growing problem, increasing in both frequency and impact, and underscoring the urgency of action.

Reports from communications providers show a sharp rise in incidents over the past year, affecting millions of customers nationwide. California and Texas account for more than half of all reported incidents.

Communications networks are being targeted by thieves based on the mistaken belief that they contain copper; while some remaining legacy infrastructure does, most modern infrastructure is fiber-based. This means the stolen material has little resale value while the resulting outage and repair costs can be substantial.

Drivers Behind the Rise

The surge in attacks is not random. It is being driven by a combination of economic incentives, lack of prosecution and enforcement, and regulatory gaps.

Economic incentives tied to copper

Copper prices[1] have climbed significantly, increasing theft across multiple industries including utilities, transportation, and communications. High demand and strong resale value, make copper theft attractive to criminal networks.

Weak oversight in the scrap metal market

In some states, thefts are enabled by the ease of selling stolen material to

2025 Data Collected from Communications Providers **Shows an Alarming Rise in Incidents.**

18,327
INCIDENTS NATIONWIDE

1,527
AVERAGE INCIDENTS PER MONTH

50
AVERAGE INCIDENTS PER DAY

59%
INCREASE SINCE 2024

11.8 M
CUSTOMERS AFFECTED

1 Chart of historical daily COMEX copper prices back to 1971 https://www.macrotrends.net/1476/copper-prices-historical-chart-data

2025 Economic Impact of Communications Outages

SOCIETAL COSTS

$294M–$1.47B

Far exceeding the value of stolen materials

LARGEST LOSSES

California	Texas
$252.6M	**$97.4M**

RIPPLE EFFECTS

Each incident disrupts not only direct users, but also businesses, emergency responders, health care providers, schools, government agencies, and others who depend on communicating with them.

scrap metal dealers with limited documentation or accountability requirements. Without stronger transaction rules, ID verification, reporting requirements and enforcement mechanisms, the market continues to fuel these crimes.

Legal gaps

Penalties for destruction of networks are often too low to deter repeat offenses. In some states, penalties do not reflect the downstream consequences of disabling emergency communications, business connectivity, health care access, and public sector operations

Public Safety, Economic, and Consumer Impacts

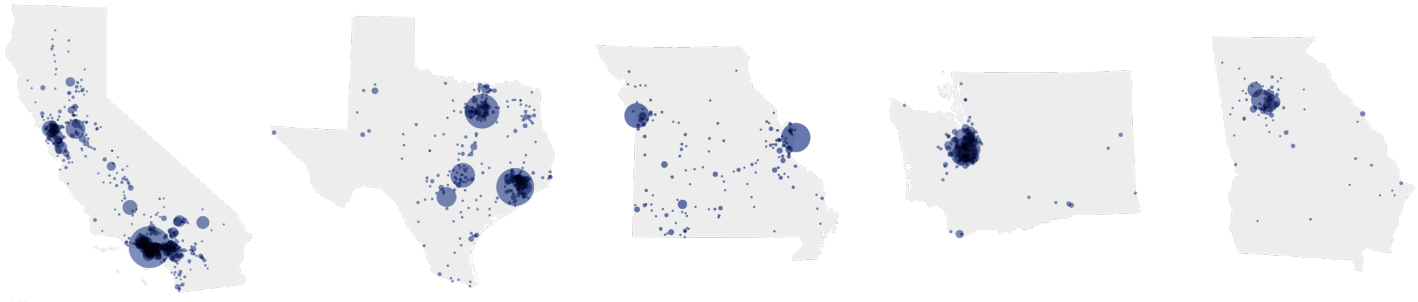
The surge in theft and attacks has consequences that extend far beyond physical damage to networks. These incidents directly affect families, businesses, and communities that rely on uninterrupted connectivity for safety, work, health care, and daily life. In today's always-connected economy, broadband and wireless service disruptions are not merely inconveniences — they can create immediate and widespread harm.

Public Safety Risks

Network outages caused by theft and vandalism can disable:

- 911 systems
- Police, fire, and EMS communications
- Hospital networks, telemedicine, and medical device connectivity
- Airport operations and flight systems
- Federal government buildings and military bases

Vandalism Incidents: Top 5 State Heatmap and 5 Hardest-Hit Areas, 2025



CALIFORNIA	
Los Angeles	1131
Stockton	236
Richmond	173
Riverside	165
Northridge	142

TEXAS	
Houston	532
Dallas	441
Austin	218
San Antonio	141
Baytown	92

MISSOURI	
St. Louis	361
Kansas City	261
Springfield	33
Independence	23
Imperial	19

WASHINGTON	
Kent	106
Seattle	65
Auburn	55
Tacoma	54
Renton	37

GEORGIA	
Atlanta	179
Marietta	91
Lithonia	76
Panola	73
Stockbridge	33

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

These disruptions can delay emergency response times and jeopardize life-critical services. Even short duration outages can have serious consequences when they affect emergency calls, public safety coordination, medical care, or government operations.

Economic Impact

The economic ripple effects of these attacks extend well beyond infrastructure repair costs. Communications outages can:

- Delay or halt business operations
- Disrupt remote work and virtual learning
- Interrupt financial transactions and payment systems
- Reduce productivity and customer access

Over time, theft and vandalism increase costs associated with repairs, prevention, and network hardening, and strain local resources.

Recent findings underscore the scale of these losses: outages caused by infrastructure theft or vandalism impose societal costs far exceeding the value of stolen materials and disproportionately affect certain states and communities.

Current Responses

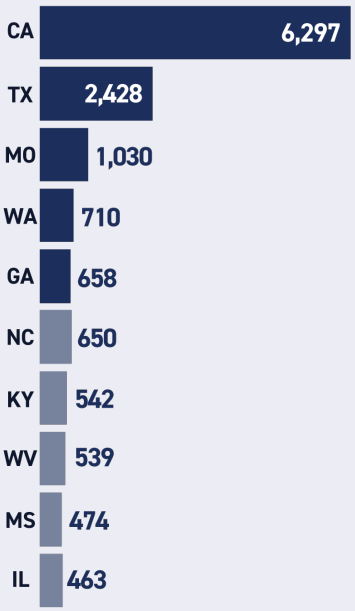
Recognizing the severity of the threat, stakeholders across industry and government have begun implementing a range of measures to protect critical communications infrastructure.

Industry Actions

Providers are investing heavily in prevention, including:

2025 Top 10 States by Number of Incidents

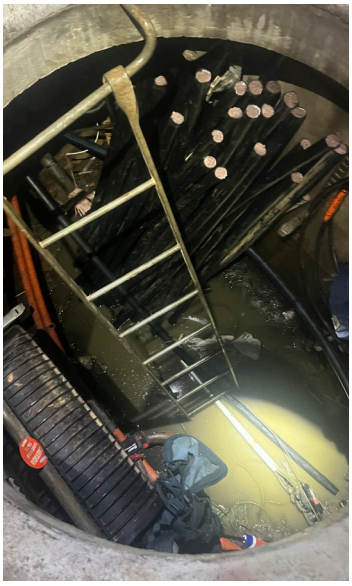
Via Reports from Large and Small ISPs Across the Country

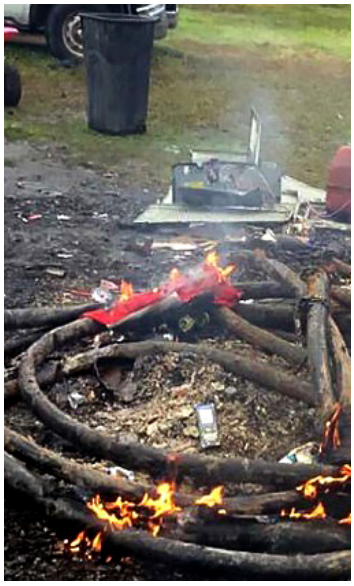


Source: Survey of large and small ISPs across the country reporting incidents.

- Enhanced physical security (surveillance, alarms, tracking devices)
- Coordination with local law enforcement
- Public education campaigns and community reporting programs
- Participating in rewards programs for information leading to arrest and prosecution
- Infrastructure redesign (downsizing cables, encasing risers, rerouting networks)
- Verification protocols for contractors and facility access

These measures are designed to reduce theft opportunities, improve detection, support investigations, encourage prosecution, and speed restoration.





State & Local Actions

State and local governments are increasingly recognizing communications theft and vandalism as a public safety and critical infrastructure threat. Thus far in 2026, over 23 states have introduced legislation, and 13 states have passed new laws enhancing scrap metal regulations and strengthening protections for critical communications infrastructure. These measures generally focus on three core areas:

- Expanding on critical infrastructure definitions to clearly include communications networks.
- Increasing penalties for intentional damage to communications networks.
- Strengthening scrap metal transaction requirements, including seller identification, transaction records, and documentation of restricted materials.

Recent state activity also reflects a growing push to treat intentional damage to communications facilities as a felony offense. In 2026, Colorado, Connecticut, Oregon, and Virginia adopted felony-level protections, continuing a broader wave of state action from 2025 and prior years.

States are also pursuing stronger scrap metal oversight to reduce the resale incentives that help fuel these crimes. Common policy approaches include requiring metal recyclers to register or obtain certification; mandating rapid transaction reporting into statewide electronic databases; requiring sellers to provide identification, contact information, vehicle details, photographs, and ownership attestations; limiting high-risk purchases, such as copper telecom wire; restricting cash payments; allowing law enforcement to inspect records and scrap yards; and establishing penalties or no-buy lists for repeat offenders.

Several states have already advanced scrap metal reform efforts in 2026, including Kentucky, Colorado, Indiana, Missouri, and Oregon. Municipalities have also formed task forces, increased coordination with law enforcement, and worked more closely with providers to identify theft patterns, support investigations, and improve rapid response.

Federal Actions

H.R. 2784, the Stopping the Theft and Destruction of Broadband Act of 2025, seeks to:

- Amend federal law to explicitly criminalize willful or malicious damage to privately owned critical communications infrastructure, closing a gap that leaves non-government networks unprotected.

Policy Priorities and Next Steps

Effective long-term mitigation will depend on a combination of strengthened laws, improved oversight, deeper collaboration across sectors, and enhanced penalties.

Policymakers should focus on five priority areas:

- **Strengthening scrap metal regulation** — including banning cash purchases for restricted metals, requiring ID and transaction records, mandating photographs of sellers and materials, and reporting purchases to law enforcement.
- **Continuing to harmonize state laws** where gaps remain to ensure communications infrastructure is clearly defined and covered under critical infrastructure protections.
- **Improving coordination** across industry, law enforcement, municipalities, and policymakers to increase prevention, enforcement, and rapid response.
- **Prioritizing law enforcement and prosecution** – ensuring theft cases are investigated, repeat offenders are pursued, and prosecutors have the tools and resources needed to hold offenders accountable.
- **Enhancing penalties** to reflect the significant public safety risks involved.

Incidents involving critical communications infrastructure have generated widespread media attention across the United States.

Learn more at protectcci.org

ncta THE INTERNET & TELEVISION ASSOCIATION ctia USTELECOM THE BROADBAND ASSOCIATION NTCA THE RURAL BROADBAND ASSOCIATION WIA Wireless Infrastructure Association ACA CONNECTS