Hidden Threat, Real Consequences: A National Security Case for Protecting Critical Communications Infrastructure from Vandalism

4th National Summit on Protecting Critical Communications Infrastructure

Philadelphia, PA

FCC Commissioner Olivia Britt Trusty

June 4, 2026

Good morning and thank you for that introduction, and thank you to our hosts, as well as industry colleagues, law enforcement partners, and policymakers who are here with us today. Your presence at this Summit reflects the kind of cross-sector collaboration we need to confront what has become a growing and deeply concerning challenge: infrastructure vandalism.

Last fall, I spoke at another summit on this issue, and I wish I could say the problem has stabilized in that time. But the reality is the opposite. In fact, the threat has grown. It has become more frequent, more sophisticated, and more coordinated. And it is why this conversation is more urgent than ever.

Infrastructure vandalism is both a property crime and a national security vulnerability. When a network goes down in America, it is never just an inconvenience. It is a grandmother in rural Texas who cannot reach her doctor. It is a small business owner in Pennsylvania watching a day's worth of transactions disappear into a dead screen. It is a dispatcher at a 911 center or public safety answering point staring at a console that is not responding. It is a child who cannot complete homework for days or perhaps weeks. It is a farmer who cannot access the price data needed to quickly navigate commodity markets. And, it is millions of other Americans who have experienced power disruptions, delayed public transportation, first responders out of reach, and more. It is, in the fullest sense of the word, a disruption to American life.

In an op-ed I wrote last October, I described infrastructure vandalism as a hidden crime. Hidden because it often happens out of sight. But its consequences are anything but invisible. Millions of Americans have already felt its impact – when their internet goes down, when their phones go silent, and when access to emergency services is disrupted. Today, we're seeing an escalation of infrastructure vandalism in the form of more frequent attacks, more sophisticated methods, and increasingly more coordinated efforts among copper thieves and other vandals.

Perhaps even more concerning is that we are entering a new reality, one where physical attacks on infrastructure are being combined with digital intelligence. It is bad enough when bad actors cut cables. But when these nefarious actors leverage technological tools to study networks and identify vulnerabilities, they are able to optimize their impact with far-reaching consequences in the form of lost service, 911 access, economic activity, public safety, and national resilience.

So today I will discuss the scope of this problem, the real numbers, the real consequences, and who is most vulnerable. I will also highlight a new and troubling dimension: the role that artificial intelligence is beginning to play as a force multiplier to these threats. And I will discuss what we need to do, not incrementally, but comprehensively, to mount a response that is equal to the threat.

First, the scope of the problem: recent industry data shows a clear surge in attacks on communications infrastructure across the country. These incidents are not isolated. They are a part of a growing pattern. Between June 2024 and June 2025, there were nearly 16,000 reported incidents of theft and vandalism targeting communications infrastructure across the United States. In the same period, outages from these attacks disrupted service for almost 10 million customers. Think about that. Nearly ten million Americans cut off not because of a natural disaster or system failure but because someone deliberately targeted an infrastructure component, facility, or installation.

More unsettling is that the pace of these attacks is also accelerating. In the first half of 2025, there were 9,770 incidents, nearly double the number from the previous six months. And the economic costs are just as staggering. A study released last fall found that outages from infrastructure attacks created societal costs, such as lost productivity, network downtime, and emergency risks, that far exceeded the value of the stolen materials themselves, totaling between $38 million and $188 million in just the second half of 2024 alone. And, given that not every incident is reported and not every cost is easy to quantify, I'm certain those numbers are much higher.

Notwithstanding these statistics, we have heard some say that copper theft is just petty crime. It is a few harmless individuals with wire cutters looking for a quick payday at the scrap yard. I understand why that public perception is there. But I want to challenge that framing,

because it fundamentally undersells the economic and national security consequences of these illicit activities.

Copper theft is real and happening at scale. But what we are witnessing more and more is something of a different kind, not just opportunistic thieves, but organized, coordinated actors who are targeting fiber routes, cell towers, and backup power systems with a level of planning and sophistication that looks less like petty theft and more like a deliberate disruption. Copper theft, in this framing, is the gateway. The onramp to something much more serious.

These attacks have hit federal buildings, disrupted operations at military installations, taken out hospital communications, and entire 911 dispatch centers as well as municipal emergency networks. NCTA data shows that more than half of copper theft incidents, approximately 53%, are concentrated in California and Texas. But let's not read that as a regional problem. Indeed, this is a nationwide crisis that impacts every state and every American in some form.

There are however some Americans who are more exposed to these threats than others, and in that sense there is a geography to this vulnerability that we cannot ignore. Rural America is on the frontlines of infrastructure vandalism in ways that compound and complicate everything else I've described so far. And, here's why: too much of rural America still runs on legacy copper networks. These are networks that were built for a different era, reliable in their time, essential to the communities they served, but are now outdated and difficult to defend.

Copper is worth money. That is why it gets stolen. But beyond its commodity value, copper infrastructure has specific vulnerabilities that make it an attractive target: it is easier to steal than fiber, it is harder to monitor remotely, and in rural areas, it is often spread across vast distances with minimal physical security. Recovery times are longer because technicians have to travel further, replacement parts may not be immediately available, and there are fewer redundant pathways to reroute service while repairs are being made. The result is that when a rural community's communications infrastructure is attacked, the outage tends to be longer, the impact tends to be deeper, and the recovery tends to be slower.

What does it actually mean when an entire rural community loses connectivity? It means that families who depend on telehealth for routine and emergency medical care are suddenly cut off from their providers and could experience a potential health crisis.

It means that small businesses, the farms, the feed stores, the independent retailers, and contractors, cannot process payments, cannot communicate with customers, and cannot access the online platforms that are now fundamental to commerce even in the most rural settings.

It also means that 911 does not work. And in communities where emergency response times are already measured in tens of minutes rather than minutes, the degradation of emergency communications is a matter of life and death.

And, it means that children in rural schools, students who may already be navigating significant connectivity challenges, lose access to the digital learning tools that have become central to modern education.

The bottom line is that the threat to rural copper networks exposes how outdated infrastructure is a security liability. In many rural communities, yesterday's networks are being targeted by today's threats. And today's threats are growing more sophisticated and more organized. The communities that were last to get connected with next-generation networks may now become the most vulnerable to being disconnected. And they have the fewest resources to respond when that happens. If we allow rural communities to remain on aging, vulnerable infrastructure while the threat environment evolves around them, those communities are at risk of being left behind. And, we shouldn't accept a future where geography determines resilience. Every community, no matter how rural or remote deserves the same commitment to reliable, secure, and modern infrastructure.

Before turning to potential solutions, it's worth highlighting the role of artificial intelligence in infrastructure vandalism. At first glance, when thinking about AI and the security of communications networks, attention tends to be on cyberattacks, deepfakes and disinformation, supply chain vulnerabilities, and more. And, rightly so. But there is a physical dimension to threats facilitated by the misuse of AI that is directly relevant to everything we are discussing today.

Let me walk you through how I see the misuse of AI beginning to intersect with infrastructure vandalism.

First: targeting optimization. AI tools can analyze publicly available data, including satellite imagery, infrastructure maps, FCC filings, and utility records, to identify high-value network nodes, map redundant versus non-redundant routes, and pinpoint locations where a single attack could cause maximum disruption. What once required significant expertise and insider knowledge can now be approximated by a sufficiently motivated actor with access to AI tools that are increasingly cheap and widely available.

Second: operational scaling. Coordinating attacks across multiple sites, across multiple regions, simultaneously, can be a barrier to unsophisticated actors who cannot manage that kind of operational complexity. AI however lowers that threshold for those willing to misuse it. It can assist with logistics, timing, and coordination in ways that make simultaneous multi-site attacks more feasible.

Third: evasion. Modern networks have detection systems. Law enforcement looks for patterns. AI can be misused to analyze those patterns and help bad actors avoid them, varying timing, locations, and methods in ways that make detection and attribution more difficult to assess.

Fourth, and perhaps most concerning: the dark web ecosystem. The combination of AI tools and dark web marketplaces is lowering the barrier to entry for would-be attackers. You no longer need to be a sophisticated operative to access the tools, the knowledge, and the network that makes a coordinated infrastructure attack possible.

Looking further ahead, the threat landscape gets even more complex. AI-assisted reconnaissance of telecommunications networks could enable automated vulnerability mapping, allowing threat actors to identify weaknesses faster than we can patch them. And, we are beginning to see the early contours of what security professionals call “blended attacks,” operations that combine a cyber intrusion with a simultaneous physical disruption, each amplifying the impact of the other.

To be clear, we are not seeing widespread, confirmed misuse of AI in domestic infrastructure vandalism cases, yet, but the trajectory and potential for harm is clear, and the

capability is developing faster than our defenses. The time to address this is before it becomes an established pattern, not after.

So with all of that said – the scope of the problem, the vulnerability of rural America, and the misuse of AI – what should we do about infrastructure vandalism? The first and most important structural answer is that we need to accelerate the transition away from legacy copper to next-generation networks — fiber, advanced wireless, satellite services, and more resilient architectures that are built for the threat environment of today and tomorrow, not the technology environment of fifty years ago.

As I previously mentioned, fiber is fundamentally harder to steal in the way copper is stolen. It has no commodity value at the scrap yard. You cannot walk into a recycling center and exchange fiber optic cable for cash. That alone removes the primary economic incentive that drives so much of the theft we are experiencing.

Fiber networks are also more amenable to remote monitoring. Modern fiber infrastructure can be equipped with sensors that detect physical tampering in near-real-time, enabling faster response and better detection of attacks before they cause extended outages.

Fiber supports greater redundancy. When a node is attacked, next-generation networks are better designed to reroute traffic, maintain service continuity, and recover faster.

And critically, for everything we've discussed about AI: next-generation networks are the platforms on which AI-driven defense systems can actually run. Predictive analytics for threat detection, automated anomaly identification, and rapid response coordination. These capabilities require modern network infrastructure. You cannot run the defenses of the future on the infrastructure of the past.

The FCC has not been standing still on these issues either. In March 2025, under Chairman Carr's leadership the FCC adopted new orders to cut red tape and streamline the copper retirement process – a process that has delayed network upgrades by years. Then in July 2025, the Commission proposed to reduce regulatory barriers that prevent much-needed investment in next-generation broadband networks and to speed the transition to modern, all-IP networks. That culminated in a March 2026 Report and Order that ultimately allows carriers to move from aging copper to fiber without costly and unnecessary bureaucratic friction. These

regulatory changes could help free up tens of billions of dollars annually in private capital that providers currently spend maintaining aging networks.

On pole attachments, the unglamorous but critical bottleneck for fiber deployment, the Commission has acted as well. In July 2025, the FCC issued a new pole attachment order that codified new access timelines for large pole attachment applications, established advance notice requirements, and required utilities to accept bulk applications without arbitrary limitations, changes designed specifically to accelerate broadband deployment in rural and underserved areas. And in September 2025, the FCC launched new proceedings to identify and address unnecessary state and local barriers to wireless and wireline infrastructure, clarify permitting rules, and encourage faster upgrades to 5G and fiber networks.

These proceedings are the operational levers that determine whether next-generation networks reach the communities most vulnerable to infrastructure attacks.

The security of our nation depends on getting this right. Modern communications networks are strategic infrastructure. They are as foundational to American competitiveness and defense readiness as highways, ports, and energy grids. When we frame the transition to next-generation networks solely as a consumer benefit or a business opportunity, we are undervaluing what is at stake. This is about American resilience. American security. American leadership in the technologies that will define the next era of global competition.

Modernizing infrastructure is the long game. But we also need to be fighting the battles in front of us right now. And that requires a coordinated national response that brings together stronger deterrence, better intelligence, smarter technology deployment, and sustained investment.

Stronger deterrence starts with the law. Progress is being made. In 2025, 23 states considered new protections for communications infrastructure, and 13 enacted laws, which strengthened felony penalties for theft and vandalism. Today, 28 states classify these crimes as felonies. That is real progress. But 28 states also means that 22 states have not made that same classification. That patchwork creates opportunities for bad actors to operate in jurisdictions where the consequences are minimal.

At the federal level, H.R. 2784 — the Stopping the Theft and Destruction of Broadband Act — would close a key gap by extending federal criminal protections to privately owned communications networks. Currently, the federal framework protects government systems far more robustly than private networks. That distinction is difficult to justify given the critical role private networks play in national security, emergency communications, and economic activity. I encourage Congress to act on this legislation as quickly as possible.

We also need to look at scrap metal market accountability. If there is no easy place to convert stolen copper into cash, the economic incentive for theft diminishes significantly. Stricter documentation requirements, waiting periods, and transaction monitoring at scrap dealers are policies that a number of states have begun implementing and can meaningfully disrupt the pipeline that makes copper theft profitable.

Public-private sector collaboration is also essential. The industry has already stepped up in important ways. The STRIKE initiative, co-led by SCTE and NCTA, is bringing providers and policymakers together to treat these attacks as the national security priority they are. Real-time information sharing among providers, between industry and law enforcement, and different levels of government is one of the most powerful tools we have. When one provider sees a pattern, a new attack method, a new geographic clustering, that intelligence should be getting to every other provider and to law enforcement without delay.

Joint task forces, bringing together federal agencies, state and local law enforcement, and industry security teams, are also proving effective in cities. For example, cities like Louisville have seen results from targeted enforcement partnerships that led to arrests and recovery of stolen materials. That model should be scaled and replicated.

And then there is AI for defense. Today, I spoke earlier about how AI can be a force multiplier for threats. But the same capabilities that make AI potentially dangerous in the wrong hands make it enormously powerful as a defensive tool.

Predictive analytics can help us identify patterns of targeting before they become attacks, flagging geographic clusters, timing patterns, and methods that suggest coordinated activity. Network monitoring powered by machine learning can detect anomalies in real-time, enabling

faster intervention. Automated response systems can reroute traffic, isolate compromised nodes, and initiate restoration protocols with a speed that human operators simply cannot match.

The future of infrastructure defense is intelligent, adaptive systems that can stay ahead of evolving threats. But, building those systems requires the modern network infrastructure I discussed earlier as well. AI-powered defense requires a next-generation network to run. These two imperatives are inseparable.

Finally, investment in resilience, particularly in rural areas, must be a sustained priority. This means building redundancy into rural networks so that a single attack does not take an entire community offline. It means hardening copper infrastructure not being upgraded to fiber with physical security measures, remote monitoring, and tamper-detection systems. It means ensuring that restoration resources are positioned so that when an outage does occur, recovery is measured in hours rather than days.

This is not cheap. But the cost of inaction is higher, measured not just in dollars, but in the very real human consequences of leaving vulnerable communities without the connectivity they depend upon.

Let me close with this.

I have been in telecommunications policy long enough to know that the temptation, when confronted with a problem this complex, is to frame it primarily as a technical challenge, something to be managed through engineering, regulation, or industry best practice. And those things matter enormously.

But infrastructure vandalism, at the scale and sophistication we are now seeing, has become a strategic and national security challenge. It is a challenge that goes to the heart of whether American communities, particularly the most vulnerable ones, can count on the connectivity that is now essential to modern life.

When we allow attacks on our communications infrastructure to go inadequately deterred, investigated, and prosecuted, we are sending the wrong message. We are telling bad actors, whatever their motivation, that the cost of disrupting American connectivity is low. We need to change that calculus.

We need to reframe this issue at every level of government and in every public conversation. Copper theft is an attack on American infrastructure. Fiber vandalism is a potential national security incident. The organized disruption of communications networks, increasingly enabled by AI tools that lower the barriers to entry, is both a local law enforcement problem and should be a federal priority.

And we need to act with the urgency that framing demands.

To my colleagues in Congress: the legislative tools are within reach. H.R. 2784 is sitting in Congress. The regulatory levers to accelerate network modernization are available. The interagency coordination mechanisms exist, they need to be activated and sustained. Let's use them.

To our partners in industry: the work you are doing through STRIKE and other collaborative initiatives is exactly right. The intelligence-sharing frameworks, the joint security operations, the investment in network monitoring, this is how we close the gap between the threat environment and our defenses. Keep going. And push us, your regulators and your government partners, to move as fast as you are.

To law enforcement: this room understands that infrastructure vandalism investigations are resource-intensive and often difficult. You deserve better tools, better data, and better coordination with the federal government and the private sector. That is a commitment I am making here today, to be an advocate within the Commission and within the broader policy conversation for the resources and frameworks that allow you to do this work effectively.

To everyone in this room: the issue of rural connectivity and rural vulnerability deserves to be at the center of this conversation, not at the margins. The communities most exposed to these threats are often the ones with the least political visibility and the fewest resources to advocate for themselves. And so, we have a responsibility to design our policies, our investments, and our enforcement priorities with them in mind.

The United States has a genuine opportunity here, not just to respond to a threat, but to lead. To demonstrate that a modern democracy can protect its critical infrastructure, transition to next-generation networks, harness AI for defense rather than disruption, and ensure that the benefits of connectivity reach every community, not just those that are easiest to serve.

That is my vision. And I believe, looking around this room, that the will to do it is here. Let's make sure the action follows. Thank you.