S. HRG. 119–319

SIGNAL UNDER SIEGE: DEFENDING AMERICA'S COMMUNICATIONS NETWORKS

HEARING

BEFORE THE

SUBCOMMITTEE ON TELECOMMUNICATIONS
AND MEDIA

OF THE

COMMITTEE ON COMMERCE,
SCIENCE, AND TRANSPORTATION
UNITED STATES SENATE

ONE HUNDRED NINETEENTH CONGRESS

FIRST SESSION

DECEMBER 2, 2025

Printed for the use of the Committee on Commerce, Science, and Transportation

Available online: http://www.govinfo.gov

U.S. GOVERNMENT PUBLISHING OFFICE
62–989 PDF WASHINGTON : 2026

SENATE COMMITTEE ON COMMERCE, SCIENCE, AND TRANSPORTATION

ONE HUNDRED NINETEENTH CONGRESS

FIRST SESSION

TED CRUZ, Texas, *Chairman*

JOHN THUNE, South Dakota
ROGER WICKER, Mississippi
DEB FISCHER, Nebraska
JERRY MORAN, Kansas
DAN SULLIVAN, Alaska
MARSHA BLACKBURN, Tennessee
TODD YOUNG, Indiana
TED BUDD, North Carolina
ERIC SCHMITT, Missouri
JOHN CURTIS, Utah
BERNIE MORENO, Ohio
TIM SHEEHY, Montana
SHELLEY MOORE CAPITO, West Virginia
CYNTHIA LUMMIS, Wyoming

MARIA CANTWELL, Washington, *Ranking*
AMY KLOBUCHAR, Minnesota
BRIAN SCHATZ, Hawaii
EDWARD MARKEY, Massachusetts
GARY PETERS, Michigan
TAMMY BALDWIN, Wisconsin
TAMMY DUCKWORTH, Illinois
JACKY ROSEN, Nevada
BEN RAY LUJÁN, New Mexico
JOHN HICKENLOOPER, Colorado
JOHN FETTERMAN, Pennsylvania
ANDY KIM, New Jersey
LISA BLUNT ROCHESTER, *Delaware*

Brad Grantz, *Republican Staff Director*
Nicole Christus, *Republican Deputy Staff Director*
Lila Harper Helms, *Staff Director*
Melissa Porter, *Deputy Staff Director*

SUBCOMMITTEE ON TELECOMMUNICATIONS AND MEDIA

DEB FISCHER, Nebraska, *Chair*
JOHN THUNE, South Dakota
ROGER WICKER, Mississippi
JERRY MORAN, Kansas
DAN SULLIVAN, Alaska
MARSHA BLACKBURN, Tennessee
TODD YOUNG, Indiana
TED BUDD, North Carolina
ERIC SCHMITT, Missouri
JOHN CURTIS, Utah
BERNIE MORENO, Ohio
TIM SHEEHY, Montana
SHELLEY MOORE CAPITO, West Virginia
CYNTHIA LUMMIS, Wyoming

BEN RAY LUJÁN, New Mexico, *Ranking*
AMY KLOBUCHAR, Minnesota
BRIAN SCHATZ, Hawaii
EDWARD MARKEY, Massachusetts
GARY PETERS, Michigan
TAMMY BALDWIN, Wisconsin
TAMMY DUCKWORTH, Illinois
JACKY ROSEN, Nevada
JOHN HICKENLOOPER, Colorado
JOHN FETTERMAN, Pennsylvania
ANDY KIM, New Jersey
LISA BLUNT ROCHESTER, *Delaware*

CONTENTS

WITNESSES

APPENDIX

SIGNAL UNDER SIEGE: DEFENDING AMERICA'S COMMUNICATIONS NETWORKS

TUESDAY, DECEMBER 2, 2025

U.S. SENATE,
SUBCOMMITTEE ON TELECOMMUNICATIONS AND MEDIA,
COMMITTEE ON COMMERCE, SCIENCE, AND TRANSPORTATION,
Washington, DC.

The Subcommittee met, pursuant to notice, at 10 a.m., in room SR–253, Russell Senate Office Building, Hon. Ted Cruz, Chairman of the Committee, presiding.

Present: Senators Fischer, Cruz, Sullivan, Blackburn, Young, Schmitt, Moore Capito, Luján, Cantwell, Peters, Rosen, Hickenlooper, and Blunt Rochester.

OPENING STATEMENT OF HON. DEB FISCHER, U.S. SENATOR FROM NEBRASKA

Senator FISCHER. Good morning. The hearing will come to order. I want to thank our witnesses for being here with us today.

Today's hearing comes at an important moment. Our nation's communication networks are facing rapidly evolving threats, ranging from fraud and espionage to sabotage. In a few minutes we will examine and consider how government and industry can work together to strengthen our network's security.

The United States intelligence community assesses that the People's Republic of China is the most active and persistent cyber threat to United States institutions. Last year, the hacking group, Salt Typhoon, backed by the PRC, infiltrated U.S. telecom providers. We need a unified cyber defense strategy now more than ever. Threat actors are deploying advanced technology at scale to try to undermine our networks at every juncture. These attacks are increasingly supercharged by artificial intelligence, as well.

While private industry continues to innovate, collaborate, and defend against these threats, the risk environment is growing more complex. Congress must coordinate with industry and ensure robust Federal response. Supply chain security remains a critical part of this conversation. The PRC-linked companies such as Huawei continue to pose significant risks to allied communication infrastructure. Congress created the Rip & Replace program to remove this vulnerable equipment from portions of American networks, and the FCC continues to identify high-risk vendors.

This Committee has also advanced my bill to increase transparency around foreign-owned communication licensees. Earlier this Congress, I introduced the FACT Act, which requires the Federal Communications Commission to publicly identify companies that hold FCC licenses that are owned by adversarial governments. I am proud it passed the Senate in October, and I look forward to seeing it become law.

As we grow more connected, we feel the impacts of network insecurity, globally, nationally, and locally. Just last month, Kearney Public Schools in Kearney, Nebraska, experienced a major cyberattack that disrupted phone and computer systems. We also witnessed a series of 911 system outages across Nebraska, with multiple failures caused by a lack of network diversity and redundancy.

As global conflict increases, networks that span international borders are also prime geopolitical targets for bad actors, seeking to create economic and political instability. Undersea cables carry more than 95 percent of international Internet traffic, including sensitive financial and governmental data. Recent physical cuts to those cables, both accidental and intentional, have caused disruptions worldwide, knocking millions of people and businesses offline, including major cloud services.

And as we look to space, satellite constellations are rapidly expanding. With over 10,000 active satellites in orbit, most operated by United States companies, these systems support at-home connectivity, national security functions, and critical infrastructure. We must ensure foreign adversaries do not infiltrate these systems for espionage or other nefarious purposes.

Across all these domains, threat actors are growing more aggressive and persistent. Today's hearing allows us to deepen our understanding of these threats and ensure our networks remain secure. There is no single solution to the network security challenges ahead. However, I hope today that we will shed light on different approaches that this Committee can champion. I look forward to the discussion.

Senator Luján, you are recognized for your opening remarks.

STATEMENT OF HON. BEN RAY LUJÁN, U.S. SENATOR FROM NEW MEXICO

Senator LUJÁN. Thank you, and first off I want to recognize and thank Chair Fischer for her leadership in calling this hearing today on a critical issue facing us all across America. I want to thank our witnesses, as well, for being here.

I think every member on this Committee can agree that there is nothing more important than keeping our communities and our country safe. That is why the security of our communications networks is vital. The networks are the foundation of our daily lives. They carry our phone calls, texts, Internet traffic, health information, emergency services, and so much more. It is also our responsibility to ensure that foreign actors like China cannot infiltrate our infrastructure or steal Americans' data.

There is clear evidence that foreign adversaries, including nation-state actors, are escalating their efforts to infiltrate and compromise our networks. The Salt Typhoon hacks from last year exposed fundamental weaknesses in our telecom infrastructure. That attack breached major carriers, such as Verizon, AT&T, and T-Mobile, and compromised millions of individuals' information. This attack also likely represents the largest telecommunications hack in our Nation's history.

About a year ago, we examined this very topic, in this very committee room. Yet a year later, our communications networks are no more secure. And we can see that it is not just the major carriers. I am also concerned that our schools, hospitals, libraries, police departments, and emergency responders are all exposed and do not have the resources to defend themselves against foreign adversaries.

I am also extremely concerned that the Federal Communications Commission rushed to dismantle efforts taken under the last administration to verify the security of America's networks. The FCC stripped these protections away, replacing them with voluntary pledges and handshakes with companies whose networks have already proven themselves to be vulnerable to data breaches. To put it plainly, these companies are basically leaving their front doors unlocked after a data break-in, and the FCC has decided to take their word when they promise they have installed deadbolts and security cameras. It is all deeply troubling.

By removing enforceable standards, the FCC is weakening our national security at a time when our communications and digital landscapes are growing like never before.

There is still a lot we do not know about the damage done by the Salt Typhoon hacks. In fact, President Trump fired the Board that was investigating the attack. But what we do know is that rolling back protections and requirements to harden our networks is putting us on a dangerous path, and it will not prevent or mitigate attacks like this in the future. There will be more attacks. That is certain.

This should not be a partisan issue. This is a matter of national security. We are fortunate to have an expert panel with us today who will speak to the vulnerabilities in our communications system and how we can address them to protect our constituents. I look forward to productive conversation today, and again, thank you all for being here.

Thank you, Madam Chair.

Senator FISCHER. Thank you, Senator Luján. I am very fortunate to have my friend as the Ranking Member on this Committee, and I thank you for your comments and look forward to important work that we can do together.

I would like to introduce our witnesses now today. Our first witness is Robert Mayer, Senior Vice President of Cybersecurity and Innovation at USTelecom. In this role, Mr. Mayer leads the association's efforts on cyber and national security.

Our second witness is Daniel Gizinski, President of Comtech's Satellite and Space Communications Segment. In his capacity, Mr. Gizinski leads efforts to advance Comtech's strategy and growth as the company focuses on next-generation satellite solutions.

Our third witness is Jamil Jaffer, Founder and Executive Director of the National Security Institute. He also serves as an Assistant Professor of Law and Director of the National Security Law and Policy Program at the Antonin Scalia Law School at George Mason University.

And our final witness is Debra Jordan, former Chief of the Public Safety and Homeland Security Bureau at the Federal Communications Commission.

Mr. Mayer, you are recognized to give your opening statement.

STATEMENT OF ROBERT MAYER, SENIOR VICE PRESIDENT OF CYBERSECURITY AND INNOVATION, USTELECOM—THE BROADBAND ASSOCIATION

Mr. MAYER. Thank you. Chair Fischer, Ranking Member Luján, and members of the Subcommittee, thank you for the opportunity to appear before you today. I am Robert Mayer, Senior Vice President of Cybersecurity and Innovation at USTelecom—The Broadband Association. I also serve as the Chair of the Communications Sector Coordinating Council at the Department of Homeland Security.

This Subcommittee knows the economic, national security, and social value of our Nation's communications infrastructure and what we bring to communities around the Nation. And while we invest billions in protecting our networks and our customers, nations including China, Russia, and Iran leverage their capabilities to infiltrate our infrastructure in pursuit of geopolitical and economic gains.

Defending against such attacks requires a whole-of-government coordination and deep and enduring trust between the private sector and the government when sharing information. It also requires, when appropriate, our government to push back on our adversaries by imposing costs through diplomatic, economic, cyber, and military means, that mirror the scale and sophistication of our adversaries. Congress can help to advance this mission by pursuing several core principles and action steps.

First, the public-private partnership model should be preserved and strengthened. It is flexible, evolves with the threat, supports actionable remediation, and it encourage early and candid reporting.

Second, cybersecurity frameworks must be flexible and adaptive. While there may be a natural impulse to mandate a detailed cybersecurity checklist, such requirements lag behind adversaries who change their techniques faster than any rules can be written. And furthermore, they shift attention away from managing real risks to managing paperwork, while our adversaries have already moved on.

The goal is not less oversight. It is oversight and measures whether our Nation's defenses are managing risks, adapting to new intelligence, or shoring up our collective defense. Those are the outcomes that strengthen national security, cybersecurity the most.

Third, under national Cyber Director Sean Cairncross's leadership, the forthcoming National Cybersecurity Strategy is expected to strengthen consequence-based responses and deepen public-private coordination, an approach we strongly support. Congress must reinforce that direction by restoring durable information sharing authorities and pass a long-term reauthorization of the CISA 2015 framework.

At the same time, Congress and Federal agencies should prioritize maximizing existing funding mechanisms. For example, BEAD non-deployment funds and related Federal or State initiatives should be strategically leveraged to strengthen the capabilities of local and regional providers, including the retirement of vulnerable end-of-life equipment and support for cyber workforce development, ensuring that smaller providers have sustained access to trained personnel who can effectively manage the evolving threat environment.

Congress and the Administration must also accelerate efforts to speed up deployment of more secure and resilient fiber broadband networks through much-needed broadband permitting reform legislation as well as supporting efforts to retire and reform network modernization rules.

Finally, cybersecurity requires a whole-of-society approach with shared responsibility that must be borne at all levels across the private and public sectors. USTelecom and our members and the sector writ large remain committed to working shoulder-to-shoulder with our government partners and Congress to outpace our adversaries and to protect the infrastructure that Americans rely upon every day.

Thank you for the opportunity to testify, and I look forward to your questions.

[The prepared statement of Mr. Mayer follows:]

PREPARED STATEMENT OF ROBERT MAYER, SENIOR VICE PRESIDENT, CYBERSECURITY AND INNOVATION, USTELECOM—THE BROADBAND ASSOCIATION

The Threat Landscape

Chair Fischer, Ranking Member Luján, and Members of the Subcommittee:

Thank you for the opportunity to testify. I am Robert Mayer, Senior Vice President of Cybersecurity and Innovation at USTelecom—The Broadband Association whose members include the full scope of our Nation's communications providers—including national, regional and local companies and cooperatives. I also serve as Chair of the Communications Sector Coordinating Council which represents broadcast, cable, satellite wireless, and wireline industries. The mission of said council is to ensure that communications networks and systems are secure, resilient, and rapidly restored after a natural or man-made disaster.

Cybersecurity has become one of the most persistent and complex national security challenges our country faces. That challenge spans the Nation's entire critical infrastructure landscape. Energy systems, financial networks, transportation systems, cloud environments, public sector networks, and communications providers all contend with sophisticated, state-backed and state-funded adversaries—such as China, Russia, and Iran. These actors have positioned themselves to conduct long-running campaigns designed not just to disrupt, but to stealthily infiltrate multiple sectors of U.S. infrastructure.

These threats are not hypothetical. In recent years, state-sponsored actors have attempted to infiltrate or actually infiltrated: U.S. energy grids, water utilities, ports, and telecommunications infrastructure. Not only are these attacks more overt, more sustained, and more aggressive than we have seen before, but the attack surface has also gotten a lot broader. Instead of just denying service to a single website or releasing ransomware at a single location, these actors are looking to preposition deep into network infrastructure, and they are looking at the entire ecosystem of cybersecurity, sometimes using third-party vendors and other more distant access points to get at critical infrastructure.

Beyond incidents visible to the public lies the quiet, steady probing by these state-sponsored adversaries who use automation, machine learning, and tailored tradecraft to identify and exploit vulnerabilities, test defensive reactions, and constantly adapt their tactics, techniques and procedures. They do this across critical infrastructure as a whole.

In a landscape like this, cybersecurity cannot be treated as a static checklist or a one-time investment. It has to be a continuous mission: understanding how adversaries are changing, how technologies are evolving, and where the most serious risks are emerging. It requires close and continuous coordination between those who operate critical systems and those in government who see the broader pattern of foreign activity. Private industry is a critical stakeholder in this environment, but we cannot do it alone.

Our national response must remain anchored in a clear understanding of responsibility: the culpability for these attacks lies with the nation-states that conduct them, not the industries and organizations that are aggressively working to defend against them. Importantly, under the leadership of National Cyber Director Sean Cairncross, we expect the updated U.S. National Cybersecurity Strategy will underscore this point—emphasizing a more proactive, consequence-based approach tied to real-world threats. As an industry, we stand ready to work closely with the White House and Congress, aligning our capabilities with the strategy's expected call for strengthened public-private partnerships and shared defense efforts.

What We Are Doing

Over the past two decades, the communications sector and the Federal government have built a partnership model that has grown more mature and more operational over time. In our sector, that collaboration is organized through the Communications Sector Coordinating Council (CSCC), which includes 57 companies of different sizes, technologies, and regional footprints. The CSCC works closely with the Government Coordinating Council, which brings together DHS, CISA, the FCC, DOJ, the Department of War, NSA, and other agencies. Together, these bodies provide the basic architecture for joint planning, risk assessment, and information sharing. Providers participate in regular operational briefings, including classified briefings on a biweekly cadence, with CISA, law enforcement, as well as military and intelligence agencies. In these settings, industry and government experts discuss constantly evolving threats and mitigation strategies.

In addition to these recurring engagements, communications providers participate in a broader ecosystem of public-private collaboration. That includes the Joint Cyber Defense Collaborative, which brings industry and government together on joint planning and response; the Communications Information Sharing and Analysis Center, which supports operational information sharing among providers; the Network Security Information Exchange and the National Security Telecommunications Advisory Committee, which provides technical and strategic perspectives; and the Enduring Security Framework led by NSA and CISA, which focuses on the intersection of national security and commercial technology. Each of these forums plays a different role, but together they create a fabric of collaboration that has proven its value repeatedly.

Cybersecurity programs are continuously evolving. Our members meet—and very often exceed—cybersecurity requirements as conditions for authorization to provide services, bid on government contracts, and participate in government programs, as well as to ensure customer trust in the competitive global marketplace.

Not every network is the same. A large nationwide carrier, a regional operator, and a local rural provider have unique network architectures. But across the sector, you see the same themes: more rigorous identity and access management; stronger protections around administrative interfaces; increased segmentation of networks so that an issue in one area does not automatically spread to others; more systematic logging and analysis of activity; implementation of zero trust architecture; and a steady push to close known vulnerabilities faster.

Recent campaigns attributed to sophisticated state-sponsored actors have pushed these efforts further. Providers have shortened patching timelines, reexamined remote-access configurations, expanded threat-hunting programs that look for subtle indicators of compromise, tightened vendor-security requirements, and invested in new analytic capabilities that help distinguish normal from abnormal behavior in large volumes of data. Many are also planning ahead for future classes of risk, including the eventual need for quantum-resistant cryptography to protect the most sensitive communications.

Industry collaboration has deepened as well. Providers, through CISO-level coordination among major North American carriers, are standing up the Communications Cybersecurity Information Sharing and Analysis Center (C2 ISAC), a next-generation platform for real-time threat sharing and joint analysis. At USTelecom, we also have created various coordinating and information-sharing platforms such as the International Communications CISO Council (ICCC), and the Council to Secure the Digital Economy (CSDE), bringing together high-level U.S. and international executives to foster sharing best practices, information, and insights. These initiatives reflect a simple reality: no single company sees everything, and timely peer-to-peer sharing of high-quality information makes every participant more resilient.

All of this work takes place while communications providers continue to deliver reliable service at national scale, all while expanding both the infrastructure that will enable AI to promote American economic competitiveness, scientific and engineering discovery, and cyber defenses themselves, as well as the broadband access that brings education, healthcare, and economic opportunity to more Americans.

Call to Action

Congress can help advance our sector's mission. The goal should be to reinforce what is working in our national cybersecurity posture and to avoid unintentionally weakening it.

Foremost, our existing *public–private partnership model should be preserved and strengthened.* The existing ecosystem—Sector Coordinating Councils, Government Coordinating Councils, information-sharing organizations, and joint planning bodies—gives us a way to bring together operational experience and national-level intelligence. It has the flexibility to evolve as threats evolve. It encourages frank discussion and early reporting. Those are not easy things to recreate once lost.

From the perspective of communications providers, several additional principles stand out. First, Congress can make a tangible difference by *strengthening information-sharing authorities.* The CISA 2015 framework establishes clear guidance and protections that enable companies to report threats quickly and safely. The current short-term extension is helpful, but Congress must pass a long-term reauthorization to maintain trust, improve early voluntary reporting, and better align industry capabilities with Federal intelligence and response efforts. Restoring those authorities would reinforce trust and encourage the early voluntary reporting that is so important to effective defense.

As part of this information sharing, *interagency collaboration needs to be enhanced.* We continue to see challenges in collaboration between Federal agencies, which at times has placed the industry in the position of helping coordinate between multiple agencies. Congress can play an important role in driving more effective and sustained interagency collaboration.

Any, *cybersecurity frameworks need to be flexible and adaptive.* While there may be a natural impulse to impose a detailed cybersecurity checklist, when requirements are fixed in place they create two primary problems; they lag behind adversaries who change their techniques faster than any rule can be written, and they shift attention from managing real risk to managing paperwork, which means a provider can be fully compliant yet still exposed. Cybersecurity regulations end up hardwiring yesterday's best practices into law while the adversary moves on.

In a sector as diverse as communications, technical prescriptions are especially problematic for regional and smaller carriers that differ widely in resources, size, topology, and technology. Forcing all of them into a single mold will redirect limited resources away from high value security investments.

Most importantly, overly prescriptive mandates can have a chilling effect on the very collaboration that has proven essential. When every deviation from a mandated standard carries potential regulatory consequences, organizations become more cautious about what they share and who they share it with. Early and validated reporting of threats is what allows a pattern to be recognized and properly addressed. We should be encouraging companies to share information quickly and avoid liabilities that make them hesitant to do so.

Second, we must *future-proof our Nation's cybersecurity investments* by ensuring American leadership in AI, quantum, and other emerging technologies. The boundaries between cybersecurity and AI innovation are becoming increasingly indistinguishable as AI becomes both a critical tool for defending networks and a powerful capability in the hands of adversaries. Strengthening our position in AI is therefore inseparable from strengthening our cyber posture, which makes it all the more essential to accelerate the infrastructure that AI depends on.

In parallel with these efforts, Congress can help providers deploy more modern and secure networks by retiring outdated copper infrastructure regulation and streamlining AI infrastructure and broadband permitting processes. Our members stand ready to deploy modern networks, but permitting obstacles at the federal, state, and local level result in costly delays. Congress should speed up National Environmental Policy Act (NEPA) and National Historic Preservation Act (NHPA) approvals for AI infrastructure and broadband permits.

Third, policy should ensure that *local and regional providers are not left behind.* While large carriers may have extensive internal cybersecurity resources dedicated to engagement with federal partners, smaller providers do not always have that opportunity. Existing funding mechanisms—such as BEAD non-deployment funds and related Federal or state initiatives—should therefore be strategically leveraged to strengthen local and regional providers' capabilities, including the retirement of vulnerable end-of-life equipment. These programs can also play a critical role in supporting cyber workforce development, ensuring that smaller providers have sustained access to trained personnel who can effectively manage evolving threats.

Communications providers are committed to doing their part. We are investing significantly in our own defenses, engaging actively in public–private partnerships, and recognizing that the threat environment is only growing more complex. Cybersecurity is a shared responsibility, and the most effective path forward is one that combines operational expertise, national-level intelligence, and policy frameworks that support collaboration rather than rigidity.

Senator FISCHER. Thank you, Mr. Mayer. Mr. Gizinski, you are now recognized for your opening statement.

STATEMENT OF DANIEL GIZINSKI, PRESIDENT OF SATELLITE AND SPACE COMMUNICATIONS SEGMENT, COMTECH

Mr. GIZINSKI. Chair Fischer, Ranking Member Luján, members of the Subcommittee, I appreciate the opportunity to speak before you today.

America's communications infrastructure is under increasing pressure from foreign adversaries who are using advanced techniques to infiltrate, disrupt, and exploit our networks. Satellite communications are a critical part of that infrastructure. Satellites have long served a quiet but critical role in supporting global communications, and over the past few years we have seen a tremendous pace of innovation, including the emergence of build-out of large-scale, non-geostationary orbit constellations, such as SpaceX's Starlink, Amazon's Leo constellation, and many others.

We have also seen the emergence of the directed device market, connecting smartphones and other small devices directly to satellites, with companies like Apple, AST SpaceMobile, and Lynk Global.

One of the unique benefits of satellites is the global reach, which also increases the attack surface of those systems. Many of the satellites providing coverage to the United States expose network traffic far outside of our borders.

Yet we have seen that cybersecurity practices in the sector have not kept pace. A recent study by researchers at the University of California, San Diego, and the University of Maryland showed the ability to intercept sensitive traffic across a number of satellites. Other published studies explore some of the risks satellites are exposed to across their space segment, user segment, and ground segment, each with unique considerations and complexities.

In the case of the space segment, components are typically not accessible following launch, which limits the ability to field certain updates. While there are certain fixes available for certain use cases, what I refer to as commonsense cyber hygiene, things like enabling encryption either on the satellite modem or inline, serve as a low-cost and simple step and something that we recommend to our customers. We note that many of the existing satellite security compliance frameworks that are in place today also recommend this, but despite that we still see many networks operated without this key protection step in place.

Strong cyber posture can be built effectively with a framework that brings together both government and industry to share threat intelligence, align incentives, and respond quickly to emerging risks. Protection requirements should be aligned with risk, understanding that not all data requires the same treatment. Our adversaries are looking forward in their approach to developing attacks, and our defense posture should reflect that.

First, we most promote information sharing, both amongst government and within industry. Establishing a broad forum that allows for free and open information sharing has strong industry support including from the Satellite Industry Association, who represents a number of domestic satellite industry members.

Second, we should consider how to move beyond rigid, compliance-only frameworks toward incentive-based models. Static checklists and controls are inherently rearward-facing, whereas a balanced model would allow for industry to be rewarded for a forward-looking security posture, offering incentive for those that invest in proactive security measures or contribute meaningfully toward collaborative threat mitigations that benefit the sector at large. This cultural shift will be key to promoting innovation and security that keeps pace with the rate of commercial innovation.

Third, cybersecurity must be designed in from the foundation. This means building subcomponents to be secure by design, and including the supply chain and threat sharing and mitigation planning. It also means ensuring that security frameworks extend to hardware and software vendors with close attention paid to the source of these critical subcomponents.

Satellite connectivity supports a wide range of critical daily services, and is playing a central role in helping expand connectivity access to underserved communities. It is also a key enabler of defense and emergency response operations and continuing to drive innovation across many other industries. The cyber threats that this sector faces are real, and they are evolving quickly. If we want to ensure the long-term resilience and security of this sector, we need to give it the attention it deserves.

[The prepared statement of Mr. Gizinski follows:]

PREPARED STATEMENT OF DANIEL GIZINSKI, PRESIDENT, SATELLITE AND SPACE SEGMENT, COMTECH TELECOMMUNICATIONS

Chairman Fischer, Ranking Member Luján, and Members of the Subcommittee,

Thank you for the opportunity to speak with you today. My name is Daniel Gizinski, and I serve as President of the Satellite and Space Communications (S&S) Segment at Comtech. Today, Comtech delivers resilient, high-performance satellite ground systems and secure communications technologies that enable real-time connectivity for government, defense, and commercial missions—most of which are designed, manufactured, and supported in the US. I appreciate the opportunity to contribute to this important discussion.

As this Subcommittee has recognized, America's communications infrastructure is under increasing pressure from foreign adversaries who are using advanced technologies to infiltrate, disrupt, and exploit our networks. Satellite communications are a critical part of that infrastructure. They enable everything from global military operations to emergency response and commercial connectivity. And yet, they have historically received less attention than terrestrial networks when considering cybersecurity and our national defense posture.

Since their inception, satellites have played a foundational role in global communications. Geostationary satellites (GEO) have long provided backhaul for remote cellular towers, broadcast services, and critical infrastructure links. For areas underserved by fiber or terrestrial wireless networks—remote, rural, mountainous regions, or even maritime environments—satellite links have often been the only feasible way to transport traffic.

The industry has seen tremendous innovation over the past five years, including the emergence and build-out of large-scale non-geostationary orbit (NGSO) constellations, including SpaceX's Starlink, Amazon's Leo constellation (formerly Project Kuiper), SES's O3b mPOWER network, and Eutelsat OneWeb, among many others. These systems deliver high-speed, low-latency connectivity to users around the world, including in rural and underserved areas where traditional infrastructure doesn't reach and enable new capabilities in maritime, aviation, defense, and enterprise markets.

At the same time, we're seeing the emergence of the direct-to-device market—connecting smartphones and other small devices directly to satellite with companies like Apple, AST SpaceMobile, and Lynk Global. This has the potential to transform emergency response, expand mobile coverage globally, and provide critical connectivity services in underserved locations or areas impacted by natural disasters.

What makes this moment especially important is the pace of change. Unlike traditional geostationary satellites, which typically have an operational lifecycle of 15 to 20 years, low-earth orbit (or LEO) constellations are built on much shorter technology cycles, typically 5 to 7 years. That means the industry is evolving quickly, with new capabilities and risks emerging constantly. Our regulatory and security frameworks need to keep up.

At the same time, the threat landscape is becoming more complex. Satellite networks naturally present a broader attack surface than terrestrial systems—many of the satellites providing coverage to the United States expose network traffic outside of our borders.

Yet many of the cybersecurity practices in the sector haven't kept pace. A recent study by researchers at the University of California, San Diego, and the University of Maryland[1], showed that a significant number of geostationary satellite signals are still being transmitted without encryption. Using an $800 off-the-shelf receiver and a rooftop dish, the researchers were able to intercept sensitive data from commercial airlines, cellular networks, critical infrastructure, and even military and law enforcement communications.

This wasn't a sophisticated cyberattack. It was a clear example of how basic security practices like encryption are still not universally applied, even when called for by existing security frameworks.

Additional research has revealed vulnerabilities in commercial satellite modems, including insecure firmware update paths, exposed web interfaces, and outdated protocols. In a number of instances, encryption was disabled by default.[2] A number of other attack methods have been demonstrated against a variety of satellite systems.[3] One of the potential reasons this has not been more readily explored is there is little reward to attract low-level cyber criminals to satellite systems—in contrast, there is substantial interest to nation-state actors. Our security posture must recognize the level of sophisticated threat actors these systems face.

Five main threat actors and advanced persistent threat (APT) groups have targeted satellite communications technology, with others having conducted attacks as well (Flashpoint, 2024). These attacks include exploiting legacy protocols, insecure firmware, and unpatched systems to gain access to sensitive data and disrupt operations.

We strongly encourage a thoughtful approach to securing these critical systems. Satellite communications provide a lifeline for both defense and commercial users. Today, satellites enable global command and control, real-time intelligence sharing, logistics coordination, and resilient communications in denied or degraded environments. Enterprises rely on satellite networks for everything from maritime and aviation connectivity to oil and gas operations, disaster response, and financial transactions. A successful cyberattack on a commercial satellite link or gateway could disrupt services across continents, compromise customer data, or even impact national economies. At the same time, many of these systems are highly complex, expensive, and take a significant amount of time to deploy, which may limit the pace at which new defensive capabilities can be reasonably fielded. Satellite systems are exposed to risks across their space segment, user segment, link segment, and ground segment—each with unique considerations and complexities.[4]

In the case of the space segment—components are typically not accessible following launch, which limits the ability to field certain updates. There are simple fixes available for certain use cases—what I refer to as common-sense cyber hygiene. Enabling encryption, either on the satellite modem or in-line, is a low cost and simple step, and one we recommend to our customers—as do many of the exist-

[1] *Don't Look Up: There Are Sensitive Internal Links in the Clear on GEO Satellites*

[2] *A Comprehensive Analysis of Security Vulnerabilities and Attacks in Satellite Modems*

[3] *PowerPoint Presentation*

[4] *Recommendations to Space System Operators for Improving Cybersecurity*

ing satellite security compliance frameworks.[5] Despite many frameworks calling for encryption on satellite links, we still see networks operated without this protection step in place.

Rigid, rules-based frameworks often rely on static checklists and controls that have been written and developed in response to past incidents, rather than in anticipation of future threats. Flexible frameworks that promote collaboration between industry and Government, encourage thoughtful risk-based decision-making, and enable flexibility will be key to developing a culture of innovation around cybersecurity. This cultural shift will be key to promoting innovation in security that keeps pace with commercial innovation.

Strong cyber posture can be built effectively with a framework that brings together government and industry to share threat intelligence, aligns incentives, and responds quickly to emerging risks. Protection requirements should be aligned with risk, understanding that not all data requires the same treatment. Our adversaries are looking forward in their approach to developing attacks, and our defense posture should reflect that.

First, information sharing at the speed of relevance is critical, and a point that has broad support across the industry. The Satellite Industry Association (SIA) is a US-based trade association that provides representation of leading domestic satellite operators, service providers, manufacturers, and more.[6] SIA has long emphasized that cybersecurity is central to the satellite industry's mission of providing secure, reliable, and resilient connectivity. SIA also highlights the importance of voluntary information sharing. Sector participants often face common threats, and they must be free to collaborate among themselves and with government to identify and respond to attacks, share mitigations, and learn from past experiences. Information sharing benefits should be secure, confidential, and free from fear of liability or regulatory consequences. This principle is essential to building trust and strengthening the entire ecosystem. Ensuring that this collaboration includes both industry and government perspectives is critical in an era where sophisticated attacks are common.

Second, I believe we should consider how to move beyond compliance-only frameworks and begin incorporating incentive-based models into our cybersecurity posture. Today, much of the focus is on penalties for breaches or non-compliance. But there's also an opportunity to reward forward-looking behavior and encourage industry to bring innovative approaches forward. Organizations that invest in proactive security measures, adopt modern encryption standards, or participate in collaborative threat-sharing initiatives could benefit from things like tax credits, grants, or streamlined certification processes. Cybersecurity tends to operate as a cost-center in most organizations, and an incentive program would help industry thoughtfully allocate both effort and talent. These are ideas worth exploring as part of a balanced and practical approach to security.

Third, we need to recognize that cybersecurity can't be an afterthought. It has to be built in from the start, across all layers of a system. That means designing subcomponents with security in mind: secure boot, memory-safe programming languages, authenticated firmware updates, and architectural decisions that prioritize security alongside performance and cost[7]. This means extending threat sharing beyond service providers to many levels of the supply chain, ensuring that all layers of the tech stack are designed with security in mind. Supply chain security remains a critical component, and ensuring that appropriate attention is paid to both the origin of hardware and software is key[8].

There's also a growing gap between the people writing cybersecurity policy and the people building the systems. We're seeing more professionals enter the field who understand the security rules but may not fully understand the full architecture, product technology, ecosystem, and/or the potential threat landscape. We need to make sure cybersecurity expertise is integrated into system design from the beginning, not added on later.

With the exponential growth and technology trajectories of this sector and satellite connectivity becoming increasingly interwoven into the daily fabric of our lives and our Nation's security, it's clear that satellite communications must be treated as a priority within our national communications infrastructure. Satellite connectivity currently supports a wide range of critical daily services, it is playing

[5] *Security and Privacy Controls for Information Systems and Organizations Introduction to Cybersecurity for Commercial Satellite Operations*

[6] *About Satellite Industry Association (SIA)—Washington, DC*

[7] *Cybersecurity in the Space Domain: Why It's Time to Stop Leaving the Front Door Unlocked—Comtech Telecommunications Corp.*

[8] *Comtech-WP-Ground-Station-Cyber-Threats-and-Product-Design-Techniques-for-Defense.pdf*

a central role in helping expand connectivity access to underserved communities, it is a key enabler of defense and emergency response operations, and satellite connectivity is continuing to drive innovation across industries. The cyber threats this sector faces are real, and they are evolving quickly. If we want to ensure the long-term resilience and security of this sector, we need to give it the attention it deserves and be willing to rethink how we approach oversight, collaboration, and innovation.

I appreciate the opportunity to appear before you today on behalf of the satellite industry and I am happy to answer any questions.

Senator FISCHER. Thank you, Mr. Gizinski. Mr. Jaffer, you are recognized for your opening statement.

STATEMENT OF JAMIL N. JAFFER, FOUNDER AND EXECUTIVE DIRECTOR, NATIONAL SECURITY INSTITUTE, ANTONIN SCALIA LAW SCHOOL, GEORGE MASON UNIVERSITY

Mr. JAFFER. Chairman Fischer, Ranking Member Luján, and members of the Subcommittee, thank you for taking the time and for having me here to testify today.

The unfortunate fact is that we are at war in the cyber domain today. It is low-level war. Our adversaries are coming after us day in and day out. The attacks on our system and our communications infrastructure are constant. China, for one, has engaged in a wide-scale effort to penetrate every aspect of America's telecommunications infrastructure, from wire line to wireless, from undersea cables to our satellite infrastructure. They are in a constant effort to come after us.

Russia is similar. Since 2019, Russia has had the capability to conduct disruptive and destructive attacks, according to the Director of National Intelligence. China has now begun deploying that capability, as well, primarily overseas, but also here in the United States.

This is an important point. It is important because at this time in our Nation's history we must remember that President Xi has told his armed forces to be prepared to invade Taiwan by 2027. If, in fact, President Xi makes good on that effort, and if the United States decides to push back, we may very well be in a shooting war with China in the very near future. That shooting war will not only be in that domain, it will typically be in the cyber domain, as well. China will engage in efforts to not only surveil American systems but to go after them aggressively. And if they have put in place these disruptive and destructive capabilities that we have seen since Volt Typhoon was in place, they will use those capabilities to our detriment.

It is not just China and Russia, though. Iran and North Korea, as well, have begun building up their cyber capabilities and are becoming serious and capable actors. And unlike China and Russia, it is much harder to deter nations like Iran and North Korea.

Of course, in the cyber domain, there are a lot of people who believe that deterrence is not successful or not possible. But the reality is that we do not practice deterrence in the cyber domain to defend our communications infrastructure. The reality is that our adversaries do not know where our red lines are. They do not know what we would do if those red lines were crossed. And to the extent that we do enforce our red lines on occasion in the cyber or telecommunications domain, we do not do it in a way that other adversaries can see. As a result, the deterrent effect is limited.

If we are going to successfully prevent China and Russia and Iran and North Korea from taking action against our telecommunications infrastructure, we must make it clear to them, at a governmental level, that we will view an attack on our communications infrastructure as an attack on our Nation and respond accordingly.

Beyond that there are big debates about what we should do about hacks like Salt Typhoon, where the Chinese government was successfully able to infiltrate and deeply penetrate our telecommunications infrastructure. On one hand you have the prior FCC action seeking to effectively and aggressively regulate our telecommunications infrastructure. On the other hand, you have a voluntary approach adopted by the current FCC Chairman. And in the middle you have a question about what the government should have done about Salt Typhoon.

We have now learned that the government actually identified the Salt Typhoon attackers before they came after our telecommunications infrastructure. We also knew that for years China had been targeting our telecommunications infrastructure and have not successfully gotten as deep as they expected. In many ways, this is like what happened before 9/11. We knew the attack was coming. We knew it was being planned. We did not know where. We even identified operatives in Kuala Lumpur. We just did not know they were coming to the United States. The same was true of the Salt Typhoon. We knew they were coming after our infrastructure. They were in our networks. We had seen them. We did not realize what they were doing to our telecommunications industry. And the question is, why didn't the government take more aggressive efforts to protect its own information, its own infrastructure and our Nation's infrastructure, and why today is the government's position that we should aggressively regulate rather than partnering to effectively achieve success?

These are difficult questions, but the truth is if we do not answer those questions today, in the relative peace of the current moment, even in the low-level war that we are in, we will face significant and effective attacks on our infrastructure by our adversaries, if and when that day comes to pass.

We cannot allow that day to come to pass, and that is why, in this moment, it makes sense to find ways to partner, going forward. The first and most effective thing Congress can do is to reauthorize the Cyber Information Sharing Act that was passed in 2015, and was recently reauthorized for a brief period as part of the government reopening effort.

But that law can be strengthened. There are those in the Senate who actually reduce the effectiveness of those laws and would limit their scope. The right thing to do here actually is to expand their scope, provide more liability and regulatory protection, and provide incentives to our industry to do better and be more effective. If we can partner more effectively and really build truly on a public and private partnership, that is how to be most successful in defending our communications and our technology infrastructure at this important time in our Nation's history.

Thank you for your time, and I appreciate the opportunity, and I look forward to your questions.

[The prepared statement of Mr. Jaffer follows:]

Prepared Statement of Jamil N. Jaffer[1] on Signal Under Siege: Defending America's Communications Networks[2]

I. Introduction

Chairman Fischer, Ranking Member Luján, and Members of the Subcommittee: thank you for inviting me here today to discuss the threats facing America's communication networks and how we might best defend this critical part of our Nation's infrastructure.

This hearing comes at a particularly important time in our Nation's history, as we see a series of major technological revolutions underway, with artificial intelligence capabilities being brought to bear across a broad range of industries and within our government and that our allies as well, the near-dawn of the quantum computing era, the potential availability of photonics for computing, and expanding access to extremely fast and reliable communications capabilities that permit the transmission of increasingly massive amounts of data around the globe at the speed of light.

At the same time, we also see the very core infrastructure that these new and novel capabilities depend upon being held at risk, under significant threat, by our adversaries, in particular, by nations like China, Russia, Iran, and North Korea and their proxies. The threats posed by these nation-states and those that they support and allow to operate, include efforts to steal our technology at huge scale, to limit our ability to design, manufacture, and deploy the massive computing infrastructure necessary to sustain and grow these revolutionary capabilities, to prevent us from accessing and using data necessary to train and employ the mathematical models and algorithms that undergird AI and other cutting-edge technologies, to threaten our ability to consistently supply the power needed to drive these technologies, and, perhaps most importantly for today's hearing, to hold at risk the very telecommunications network infrastructure and systems that our people, our companies, and our government rely upon to provide access to these capabilities and to transmit the data around the globe.

Indeed, in recent months and years, we've seen the threat landscape created by nation-state actors and their proxies, expand significantly. Just in the last month, we've learned that Chinese nation-state actors utilized Anthropic's Claude Code capabilities and infrastructure earlier this fall to launch semi-autonomous hacks against nearly three dozen global governments and private sector organizations.[3] And long prior this effort, we've learned about other major threats targeting the both America's cyber and telecommunications infrastructure as well as that of our allies, including actual hacks and capabilities being put in place for destructive at-

[1] Jamil N. Jaffer currently serves as Founder & Executive Director of the National Security Institute and the NSI Cyber & Tech Center and as an Assistant Professor of Law and Director of the National Security Law & Policy Program and the Cyber, Intelligence, and National Security LL.M. Program at the Antonin Scalia Law School at George Mason University. Mr. Jaffer is also a Venture Partner at Paladin Capital Group, a leading global multi-stage investor that identifies, supports and invests in innovative companies that develop promising, early-stage technologies to address the critical cyber and advanced technological needs of both commercial and government customers. Mr. Jaffer serves on a variety of public and private boards of directors and advisory boards, including as a member of the Virginia Governor's Task Force on Artificial Intelligence. Among other things, Mr. Jaffer previously served as Chief Counsel & Senior Advisor to the Senate Foreign Relations Committee, Senior Counsel to the House Intelligence Committee, Associate Counsel to President George W. Bush in the White House, and Counsel to the Assistant Attorney General for National Security in the U.S. Department of Justice, as well as a member of the Cyber Safety Review Board at the Department of Homeland Security. Mr. Jaffer is testifying before this Subcommittee in his personal and individual capacity and is not testifying on behalf of any organization or entity, including but not limited to any current or former employer or public or private entity.

[2] Significant portions of this testimony have been drawn in whole or in part from prior testimony provided to the House and Senate by Mr. Jaffer, including, in particular, from Mr. Jaffer's testimony provided to the United States House of Representatives Committee on Energy & Commerce's Subcommittee on Communications & Technology in April 2025. Citations to and quotations marks from such testimony have been omitted, including the significant portions of Mr. Jaffer's prior testimony which have been excerpted verbatim herein.

[3] *See* Anthropic, *Disrupting the First Reported AI-Orchestrated Cyber Espionage Campaign* (Nov. 2025), available online at <*https://assets.anthropic.com/m/ec212e6566a0d47/original/Disrupting-the-first-reported-AI-orchestrated-cyber-espionage-campaign.pdf*>.

tacks—particularly but not exclusively, coming from China and its ruling cabal of the Chinese Communist Party (CCP).

Moreover, while credible reports from last year indicate that the Chinese government has successfully penetrated deep into American telecommunications networks, and has also sought to put in place destructive capabilities at the heart of American and allied critical infrastructure—these efforts, known as Salt Typhoon and Volt Typhoon, respectively, are part of a much larger and more troubling story. As it turns out, there is a significant effort afoot in the cyber domain, architected not just by China, but also by Russia, Iran, and North Korea, and a wide range of proxy actors operating on their behalf, to target America's communications infrastructure, and that of our allies and partners as well.

These efforts are aimed not only at collecting information and intelligence on American government officials and our Federal policies and priorities, but also at stealing our intellectual property, collecting massive amounts of data and intelligence on our citizens and, perhaps most troubling, putting in place capabilities that can be used to destructive effect when they choose to do so.

These efforts also stretch across significant parts of our Nation's critical infrastructure and are aimed—in various forms—at both the government and key industries, including our financial services, energy, telecommunications, and technology sectors, just to name a few.

While today's hearing is focused on threats to America's communications networks (and the technology that rides on top of it) and assessing what we can do to better defend those networks and systems, it is important that we understand these threats—and our response—in the context of two key issues: (1) the larger national security threat and competition from China, including its key economic and technological elements; and (2) the ongoing and increasingly robust collaboration between our adversaries in China, Russia, Iran, and North Korea.

II. The Threat Environment Facing America and Our Communications Networks

A. China

Starting with China, the current Director of National Intelligence, in her first-ever Annual Threat Assessment of the Intelligence Community provided earlier this year, has made clear that the People Republic of China (PRC) "presents the most comprehensive and robust military threat to U.S. national security . . . [with] a joint force that is capable of full-spectrum warfare" and active efforts ongoing that are "aimed at making the PLA a world-class military by 2049."[4] As a result, the DNI expects that China will seek to remain "in a position of advantage in a potential conflict with the United States . . . [while also] . . . conducting wide-ranging cyber operations against U.S. targets for both espionage and strategic advantage."[5]

At the same time, the DNI expects that "Beijing will continue to strengthen its conventional military capabilities and strategic forces, intensify competition in space, and sustain its industrial-and technology-intensive economic strategy to compete with U.S. economic power and global leadership."[6] Moreover, as we think about the most likely flashpoint with China—over Taiwan (which CCP leader Xi Jinping has told his military to be prepared to invade in 2027,[7] just over a year from now)—it is worth noting that the DNI is of the view that "[a] conflict between China and Taiwan would disrupt U.S. access to trade and semiconductor technology critical to the global economy . . . [and] [e]ven without U.S. involvement in such a conflict, there would likely be significant and costly consequences to U.S. and global economic and security interests."[8]

Speaking specifically about threats to American networks writ large, the DNI has stated unambiguously that China "remains the most active and persistent cyber

[4] *See* Office of the Director of National Intelligence, *Annual Threat Assessment of the U.S. Intelligence Community* (Mar. 2025), at 9, available online at <*https://www.dni.gov/files/ODNI/documents/assessments/ATA-2025-Unclassified-Report.pdf*>.

[5] *Id.* at 10, available online at <*https://www.dni.gov/files/ODNI/documents/assessments/ATA-2025-Unclassified-Report.pdf*>.

[6] *Id.* at 9.

[7] *See* William J. Burns, *Transcript: Trainor Award Ceremony Honoring CIA Director William J. Burns* (Feb. 9, 2023), available online at <*https://isd.georgetown.edu/2023/02/09/watch-trainor-award-ceremony-honoring-cia-director-william-j-burns/*> ("[O]ur assessment at CIA is that I wouldn't underestimate President Xi's ambitions with regard to Taiwan. . . . We know, as a matter of intelligence, that he's instructed the People's Liberation Army to be ready by 2027 to conduct a successful invasion.")

[8] *See 2025 Annual Threat Assessment, supra* n. 4 at 11.

threat to U.S. government, private-sector, and critical infrastructure networks[,]"[9] further noting that that "China has demonstrated the ability to compromise U.S. infrastructure through formidable cyber capabilities that it could employ during a conflict with the United States."[10] Indeed, the DNI's view is that, if China believes "a major conflict with Washington [is] imminent, it could consider aggressive cyber operations against U.S. critical infrastructure and military assets," with the specific aim of "deter[ring] U.S. military action by impeding U.S. decision-making, inducing societal panic, and interfering with the deployment of U.S. forces."[11]

And this is where the Volt Typhoon and Salt Typhoon efforts by China come into play. The DNI has stated that the Volt Typhoon "campaign [by China] to preposition access on critical infrastructure for attacks during crisis or conflict," and the "more recently identified compromise of U.S. telecommunications infrastructure [by China], also referred to as Salt Typhoon, demonstrates the growing breadth and depth of the PRC's capabilities to compromise U.S. infrastructure."[12]

Truth be told, none of this new when it comes to China. Since at least 2019, over half a decade ago, the U.S. Intelligence Community has been flagging that "China presents a persistent cyber espionage threat and a growing attack threat to our core military and critical infrastructure systems," and specifically warning that China "is improving its cyber attack capabilities," and noting specifically that "China has the ability to launch cyber attacks that cause localized, temporary disruptive effects on critical infrastructure—such as disruption of a natural gas pipeline for days to weeks—in the United States."[13]

This drumbeat continued into 2021, with the then-new Administration warning that "China presents a prolific and effective cyber-espionage threat, possesses substantial cyber-attack capabilities, and presents a growing influence threat[,]" and specifically noting that China both "can launch cyber attacks that, at a minimum, can cause localized, temporary disruptions to critical infrastructure within the United States[,]" and noting specifically—for the first time—that China's "cyber-espionage operations have *included compromising telecommunications firms,* providers of managed services and broadly used software, and other targets potentially rich in follow-on opportunities for intelligence collection, attack, or influence operations."[14]

This was followed, in 2022, with continued warnings of China's "almost certain[]" capability "to launch[] cyber attacks that would disrupt critical infrastructure services within the United States, including against oil and gas pipelines and rail systems," and noting once again the threat to telecommunications, software and other target rich environments.[15]

It is also worth noting that these threats in the cyber domain, including to American communications networks—both historic and ongoing—are undergirded by China's efforts to "dominat[e] global markets and strategic supply chains . . . making other nations dependent on China[,]" particularly in areas that are critical to United States technology leadership, such as critical minerals, semiconductors, and artificial intelligence.[16] For example, the current DNI has made clear that "China's dominance in the mining and processing of several critical materials is a particular threat, providing it with the ability to restrict quantities and affect global prices."[17] We also know that China seeks to "become a global [science and technology] superpower, surpass the United States, promote self-reliance, and achieve further economic, political, and military gain . . . [by] prioritiz[ing] technology sectors such as advanced power and energy, AI, biotechnology, quantum information science, and semiconductors."[18]

[9] *Id.* at 11.

[10] *Id.* at 9.

[11] *Id.* at 12.

[12] *Id.* at 11.

[13] *See* Daniel R. Coats, *Statement for the Record: Worldwide Threat Assessment of the U.S. Intelligence Community* (Jan. 29, 2019), at 5, Senate Select Committee on Intelligence, available online at *<https://www.intelligence.senate.gov/sites/default/files/documents/os-dcoats-012919.pdf>*.

[14] *See* Office of the Director of National Intelligence, *Annual Threat Assessment of the U.S. Intelligence Community* (Apr. 9, 2021), at 8, available online at *<https://www.intelligence.senate.gov/sites/default/files/documents/2021-04-09%20Final%20ATA%202021%20%20Unclassified%20Report%20-%20rev%202.pdf>* (emphasis added).

[15] *See* Office of the Director of National Intelligence, *Annual Threat Assessment of the U.S. Intelligence Community* (Feb. 7, 2022), at 8, available online at *<https://intelligence.house.gov/uploadedfiles/hhrg_117_ig00_wstate_hainesa_20220308.pdf>*.

[16] *See 2025 Annual Threat Assessment, supra* n. 4 at 12.

[17] *See id.*

[18] *Id.* at 13.

And the tie-in between these efforts and the threats to our telecommunications and cyber infrastructure is that the Chinese are actively exploiting our communications networks to juice their efforts to become a technology superpower. They are doing so in a range of ways, including engaging in intellectual property theft at industrial scale, with the DNI noting that China is directly stealing "hundreds of gigabytes of intellectual property from companies in Asia, Europe, and North America in an effort to leapfrog over technological hurdles, with as much as 80 percent of U.S. economic espionage cases as of 2021 involving PRC entities."[19] China also use its intelligence collection capabilities on U.S. networks to identify investments, recruit talent, evade sanctions, and conduct cyber operations, all of which are key parts of their effort to "accelerat[e] [China's] S&T progress through a range of licit and illicit means."[20]

And it is worth noting that China's ongoing "multifaceted, national-level strategy designed to displace the United States as the world's most influential AI power by 2030,"[21] is not simply aimed at economic gain but is also designed to support China's intelligence collection efforts and its larger plan to undermine American national security.

Indeed, the current DNI has made clear that "Chinese AI firms are already world leaders in voice and image recognition, video analytics, and mass surveillance technologies," and that the "[t]he PLA probably plans to use large language models (LLMs) to generate information deception attacks, create fake news, imitate personas, and enable attack networks."[22]

It goes without saying that these Chinese intelligence collection efforts and covert and overt messaging operations take place over the entirety of America's communications networks. One obvious example is very real threat posed by TikTok to America's national security.[23] While many Americans—and perhaps some key leaders and policymakers—view TikTok primarily as a way to watch a bunch of kid and dog videos, the fact is that TikTok's extensive collection of data on Americans and our allies, its ties to the Chinese Communist Party, and the Chinese government's influence over TikTok's algorithm, makes it a unique and serious national security threat. [24]

Indeed, when one combines the massive amount of data that TikTok collects on its users with other data stolen by Chinese government hackers, including security clearance files and the sensitive financial, health, and travel data of millions of Americans, it is clear that the Chinese government can use this data—powered by AI—to drive future sophisticated intelligence collection and disinformation campaigns targeting Americans and our allies.[25]

As if this weren't enough, it is worth noting that China also seeks to increase its already central role in the semiconductor supply chain to undermine U.S. communications networks, including our ability to build them and to secure them. The DNI has identified that the China has "made progress in producing advanced 7-nanometer (nm) semiconductor chips for . . . cellular devices using previously acquired deep ultraviolet (DUV) lithography equipment," and has noted that while they may face volume production challenges, China is also continuing to "explore applying advanced patterning techniques to DUV machines to produce semiconductor chips as small as 3nm,"[26] a claim that appears to be supported by reporting earlier this year that Chinese semiconductor company SMIC has managed to manufacture 5 nm chips using such techniques with DUV machines.[27] And, of course, the DNI rightly notes that "China [already] leads the world in legacy logic semiconductor (28nm and up) production, accounting for 39.3 percent of global capacity, and

[19] *Id.*

[20] *Id.*

[21] *Id.*

[22] *Id.*

[23] *See, e.g.,* Protecting Americans from Foreign Adversary Controlled Applications Act, Pub. L. No. 118–50, div. H, 138 Stat. 955 (2024); The White House, *Protecting Americans' Sensitive Data from Foreign Adversaries,* 86 Fed. Reg. 31423 (June 9, 2021); The White House, *Addressing the Threat Posed by TikTok,* 85 Fed. Reg. 48637–38 (Aug. 6, 2020).

[24] *See Brief of Amicus Curiae Former National Security Officials, TikTok Inc., et al., v. Merrick B. Garland,* No. 24–1113 (S. Ct.) (filed Dec. 27, 2024), available online at <*https://www.supremecourt.gov/DocketPDF/24/24-656/336098/20241227135716235_24-656%2024-657bsacFormerNational SecurityOfficials.pdf*>.

[25] *Id.* at 4–13.

[26] *See 2025 Annual Threat Assessment, supra* n. 4 at 14.

[27] *See* Ananya Gairola, *China's Chip Breakthrough Without ASML Makes Chamath Palihapitiya Take Stock Of Beijing's 'Formidable' Nature: 'America Can Win If . . .',* Benzinga (Apr. 23, 2025), available online at <*https://www.benzinga.com/tech/25/04/44970472/chinas-chip-breakthrough-without-asml-makes-chamath-palihapitiya-take-stock-of-beijings-formidable-nature-america-can-win-if*>.

is expected to add more capacity than the rest of the world combined through 2028[,]" for chips that are "vital to producing automobiles, consumer electronics, home appliances, factory automation, broadband, and many military and medical systems,"[28] including critical parts of our telecommunications networks and systems.

Indeed, China has long sought to infiltrate U.S., allied, and other global communications networks with their own equipment, both by building it on the cheap using stolen U.S. technology and then innovating on top of it, as well as by heavily subsidizing the sale of such equipment. The stories of how companies like Huawei and ZTE built their core networking capabilities and got them deployed globally are well known,[29] and multiple Congressional committees and U.S. administrations have sought to highlight the threat to our own infrastructure and that of our allies,[30] and the relative success of the U.S. domestic rip-and-replace program can serve as a model for other nations as well.[31] But the challenges continue. A recent report from the U.S.-China Economic and Security Review Commission (USCC) notes Chinese critical infrastructure investments in various strategic locations around globe, including in the Middle East, Southeast Asia, and Africa, noting, for example, that China's investment into Southeast Asia's information and communications technology sector exceeds $12 billion and is focused on areas like cloud computing, data center capacity, and core network equipment provision for national telecommunications infrastructure.[32] Taking a page from the U.S. book, the USCC notes that while today Huawei supplies 70 percent of Indonesia's network equipment, it "has offered to take over the remaining percentage with a free rip-and-replace program."[33] This approach is almost certainly being mirrored in strategic locations around the globe.

China has also targeted the undersea cables that serve as the backbone of the international communications system, which carries 95 percent of global Internet traffic and around 99 percent of transoceanic digital communications.[34] The USCC report notes that China is "increasingly engaged in undersea cable-cutting activities as a gray zone pressure tactic, and there is mounting evidence that Beijing is developing new cable-cutting technologies for potential wartime use."[35] The USCC goes on to note that "[f]or over a decade, Chinese scientists at research institutions affiliated with the PLA have actively researched strategies for severing undersea cables, acquiring numerous patents for technologies designed to cut deep-sea cables more cheaply and efficiently" and that earlier this year, the China Ship Scientific Research Center (a U.S. sanctioned entity) "unveiled a new design for an 'electric cutting device for deep-sea cables' reportedly capable of severing armored cables at depths of more than 13,000 feet."[36] Indeed, the USCC reports that "Chinese vessels have sabotaged critical undersea cables near Taiwan and in the Baltic Sea" and notes two incidents in 2025 alone, where "Chinese-owned 'shadow fleet' vessels cut cables near Taiwan while engaging in highly irregular movement patterns and disguising their identities and locations as well as a November 2024 incident where a "Chinese vessel severed two undersea cables in the Baltic Sea—one connecting Sweden and Lithuania, the other connecting Germany and Finland—after dragging its anchor for more than 100 miles," which European investigators believe was a joint Russia-China operation.[37] And this doesn't even cover the potential tapping threat posed by Chinese cable repair vessels nor the relative lack of allied repair capacity in the IndoPacific (as well as globally) noted by the USCC.[38]

Finally, when it comes to the threats posed by China to American communication networks, we cannot forget about China's efforts to compete with the United States in the space domain and, in particular, its ability to potentially take action against

[28] *See 2025 Annual Threat Assessment, supra* n. 4 at 13.

[29] *See, e.g.,* Jill C. Gallagher, *U.S. Restrictions on Huawei Technologies: National Security, Foreign Policy, and Economic Interests,* Congressional Research Service (Jan. 5, 2022), at 6–12, available online at <*https://www.congress.gov/crs_external_products/R/PDF/R47012/R47012.2.pdf*>.

[30] *Id.* at 12–39.

[31] *Id.* at 22–25.

[32] *See* U.S.-China Economic and Security Review Commission, *2025 Report to Congress* (Nov. 2025), at 233–34, available online at <*https://www.uscc.gov/sites/default/files/2025-11/2025_Annual_Report_to_Congress.pdf*>.

[33] *Id.* at 234.

[34] *See* Jill C. Gallagher, *Undersea Telecommunication Cables: Technology Overview and Issues for Congress,* Congressional Research Service (Sept. 13, 2022), available online at <*https://www.congress.gov/crs_external_products/R/PDF/R47237/R47237.2.pdf*>.

[35] *See USCC 2025 Report, supra* n. 32 at 98.

[36] *Id.*

[37] *Id.*

[38] *Id.* at 99.

the United States in that arena. While it is true that in recent decades, the long-haul telecommunications infrastructure has pivoted from satellite-based communications to undersea cables as noted above, the reality is that we are increasingly relying on space-based assets for a range of services and capabilities that are critical to our communications capabilities, including position, navigation, and timing, as well as broadband access across the globe, both for government and industry use cases. As such, China's rapidly developing capabilities in intelligence, surveillance, and reconnaissance (ISR), where the DNI finds that it has "achieved global coverage . . . in some of its . . . constellations and world-class status in all but a few space technologies[,]" as well as its Beidou constellation which competes with our GPS system, and its recent launch of a low Earth orbit (LEO) constellation for satellite Internet services,[39] are all concerning trends.

These trends, of course, are also particularly concerning when viewed in light of China's counterspace capabilities, which the DNI has made clear "will be integral to PLA military campaigns," particularly given that "China has counterspace-weapons capabilities intended to target U.S. and allied satellites."[40] Chinese capabilities to go after America's space-based communications infrastructure don't just include "ground-based counterspace capabilities, including EW systems, directed energy weapons (DEWs), and antisatellite (ASAT) missiles intended to disrupt, damage, and destroy target satellites," but also includes "orbital technology demonstrations . . . [and] on-orbit satellite inspections of other satellites," capabilities that "while not counterspace weapons tests, prove [China's] ability to operate future space-based counterspace weapons . . . [and] which probably would be representative of the tactics required for some counterspace attacks."[41]

For its part, the Federal Communication's Commission under its new chairman has sought to take action to address the threats posed by China and other threat actors. For example, the FCC recently established a Council on National Security aimed at leveraging the FCC's authorities to counter foreign adversaries, like China, with the goals of reducing the American technology and communications sectors' supply chain dependencies on such adversaries; mitigating America's vulnerabilities to cyberattacks, espionage, and surveillance; and ensuring U.S. victory in our strategic competition with China in critical technology domains like AI, space, next gen communications, and quantum computing.[42] The FCC has also taken action in a range of areas including foreign ownership, control, and influence over FCC licensees,[43] foreign controlled labs,[44] and the security of submarine cables,[45] to name just a few.

B. Russia

Turning to Russia, it is clear—and the current DNI agrees—that "Russia's current geopolitical, economic, military, and domestic political trends underscore its resilience and enduring potential threat to U.S. power, presence, and global interests[,]" and that Russian President Vladimir Putin is "prepared to pay a very high price to prevail in what he sees as a defining time in Russia's strategic competition with the United States, world history, and his personal legacy."[46] Indeed, the DNI believes that "Moscow's massive investments in its defense sector will render the Russian military a continued threat to U.S. national security," noting that Russia has "increased its defense budget to its heaviest burden level during Putin's more than two decades in power," while also "import[ing] munitions such as UAVs from Iran and artillery shells from North Korea . . . enhancing the threat its military poses."[47]

[39] *See 2025 Annual Threat Assessment, supra* n. 4 at 15.

[40] *Id.*

[41] *Id.*

[42] *See* Federal Communications Commission, *FCC Council on National Security,* available online at <*https://www.fcc.gov/fcc-council-national-security*>.

[43] *See* Federal Communications Commission, *Protecting our Communications Networks by Promoting Transparency Regarding Foreign Adversary Control,* Notice of Proposed Rulemaking (May 22, 2025), available online at <*https://docs.fcc.gov/public/attachments/FCC-25-28A1.pdf*>.

[44] *See* Federal Communications Commission, *FCC Takes Action on "Bad Labs" Apparently Controlled By China* (Sept. 25, 2025), available online at <*https://docs.fcc.gov/public/attachments/DOC-414369A1.pdf*>.

[45] *See* Federal Communications Commission, *Review of Submarine Cable Landing License Rules and Procedures to Assess Evolving National Security, Law Enforcement, Foreign Policy, and Trade Policy Risks,* Report and Order and Further Notice of Proposed Rulemaking (Aug. 7, 2025), available online at <*https://docs.fcc.gov/public/attachments/FCC-25-49A1.pdf*>.

[46] *See 2025 Annual Threat Assessment, supra* n. 4 at 16.

[47] *Id.* at 18.

Like China, Russia's "disinformation, espionage, influence operations, military intimidation, cyberattacks, and gray zone tools . . . [are also part of an effort] to try to compete below the level of armed conflict and fashion opportunities to advance Russian interests."[48] Indeed, the current DNI has made clear that Russia's cyber-enabled "influence activities . . . including [] stoking political discord in the West, sowing doubt in democratic processes and U.S. global leadership, degrading Western support for Ukraine, and amplifying preferred Russian narratives. . .will continue for the foreseeable future and will almost certainly increase in sophistication and volume."[49] And current DNI's view is that Russian "information operations efforts to influence U.S. elections are advantageous, regardless of whether they affect election outcomes, because reinforcing doubt in the integrity of the U.S. electoral system achieves one of [Russia's] core objectives."[50]

The fact, of course, is that much of these efforts, take place through Russia's cyber exploitation of American communications and technology networks and systems. Specifically, the DNI has determined that "Russia's advanced cyber capabilities, its repeated success compromising sensitive targets for intelligence collection, and its past attempts to pre-position access on U.S. critical infrastructure make it a persistent counterintelligence and cyber attack threat."[51]

Such capabilities should be a major concern for the United States because the "practical experience [Russia] has gained integrating cyber attacks and operations with wartime military action . . . [will] almost certainly amplify[] its potential to focus combined impact on U.S. targets in [a] time of conflict."[52] Indeed, the DNI assesses that Russia's "demonstrat[ion] [of] real-world disruptive capabilities during the past decade, including gaining experience in attack execution by relentlessly targeting Ukraine's networks with disruptive and destructive malware[,]"[53] provides Moscow with a "unique strength" in the cyber domain.[54]

As with China, however, these facts should not be surprising, particularly given that since at least 2019, the United States has been raising concerns about Russia's efforts to "map[] our critical infrastructure with the long-term goal of being able to cause substantial damage," and given that the then-DNI, Senator Dan Coats, specifically disclosed that Russia was actively "staging cyber attack assets to allow it to disrupt or damage U.S. civilian and military infrastructure during a crisis."[55]

This is the exact same kind of deployment of cyber capabilities that we saw Volt Typhoon put in place more recently on behalf of the Chinese government. Indeed, as one thinks about the capabilities that a nation like Russia has available to target American telecommunications systems and networks today, it is worth noting that back in 2019, the then-DNI stated that "Russia has the ability to execute cyber attacks in the United States that generate localized, temporary disruptive effects on critical infrastructure—such as disrupting an electrical distribution network for at least a few hours[.]"[56]

And these concerns only grew more troubling, particularly for our telecommunication's infrastructure, in 2021 and 2022, when the DNI specifically noted that "Russia continues to target critical infrastructure, including underwater cables and industrial control systems, in the United States and in allied and partner countries, as compromising such infrastructure improves—and in some cases can demonstrate—its ability to damage infrastructure during a crisis."[57]

Russia, like China, is also focused on American undersea cables. For at least a decade, news reports have flagged the threat that Russian ships pose to American undersea cable networks systems, both from a damage perspective as well as from an intelligence collection capability.[58] And in 2023, the Congressional Research

[48] *Id.*
[49] *Id.* at 20.
[50] *Id.*
[51] *Id.* at 19.
[52] *Id.*
[53] *Id.* at 20.
[54] *Id.* at 19.
[55] *See 2019 Worldwide Threat Assessment, supra* n. 13 at 6.
[56] *Id.*
[57] *See 2021 Annual Threat Assessment, supra* n. 14 at 9; *2022 Annual Threat Assessment, supra* n. 15 at 12.
[58] *See, e.g.,* David E. Sanger & Eric Schmitt, *Russian Ships Near Data Cables Are Too Close for U.S. Comfort,* New York Times (Oct. 26, 2015), available online at <*https://www.nytimes.com/2015/10/26/world/europe/russian-presence-near-undersea-cables-concerns-us.html*>; *see also, e.g.,* Morgan Chalfant & Olivia Beavers, *Spotlight Falls on Russian Threat to Undersea Cables,* The Hill (June 17, 2018), available online at <*https://thehill.com/policy/cybersecurity/392577-spotlight-falls-on-russian-threat-to-undersea-cables/*>; CBS News, *Concern over Russian Ships Lurking Around Vital Undersea Cables* (Mar. 30, 2018), available online at <*https://www.cbsnews.com/news/russian-ships-undersea-cables-concern-vladimir-putin-yantar-ship/*>;

Service noted that as far back in 2018, the Associated Press cited a Russian publication for the proposition that "Russia has the capability to cut cables, connect to top-secret cables, and jam underwater sensors that detect intrusions" raising significant concern for the NATO allies, among others.[59]

Like China, as well, it is worth noting Russia also has advanced "space programs threaten the Homeland, U.S. forces, and key warfighting advantages,"[60] and that "Russia continues to train its military space elements and field new antisatellite weapons to disrupt and degrade U.S. and allied space capabilities[, including by] . . . expanding its arsenal of jamming systems, DEWs, on-orbit counterspace capabilities, and ASAT missiles designed to target U.S. and allied satellites."[61]

It is also clear that "Russia has proven adaptable and resilient, in part because of the expanded backing of China, Iran, and North Korea[,]"[62] that "Russia's relationship with China has helped Moscow circumvent sanctions and export controls to continue the war effort, maintain a strong market for energy products, and promote a global counterweight to the United States, even if at the cost of greater vulnerability to Chinese influence[,]" and that Russia's "increase[ed] military cooperation with Iran and North Korea . . . continue[s] to help its war effort[.]"[63]

C. Iran

Members of this Committee are also well aware of the significant threat that Iran poses to American national security and our interests, allies, and partners globally, including our longstanding allies in the Middle East, including Israel, Jordan, Saudi Arabia, the United Arab Emirates, and Bahrain, to name a few. This threat is perhaps most clear in the Iranian regime's support of all manner of terrorist groups around the world from Hizballah to Hamas and Palestinian Islamic Jihad to the Yemeni Houthis and groups in Iraq and Syria that have directly attacked—and kidnapped and killed—Americans citizens and soldiers for years. The DNI recently made clear that Iran "will continue to directly threaten U.S. persons globally and remains committed to its decade-long effort to develop surrogate networks inside the United States . . . [including] seek[ing] to target former and current U.S. officials it believes were involved in the killing of . . . IRGC[]-Qods Force Commander Qasem Soleimani in January 2020[, having] previously [] tried to conduct lethal operations in the United States."[64]

And we well know of Iran's longstanding efforts to pursue nuclear weapons capabilities, against the interests of the United States and our allies. But it is also worth noting that Iran is also building up—and sharing with other U.S. adversaries—its conventional weapons capabilities as well. Indeed, according to the DNI, "Iranian investment in its military has been a key plank of its efforts to confront diverse threats and try to deter and defend against an attack by the United States or Israel[,]" including through its efforts to "bolster the lethality and precision of its domestically produced missile and UAV systems,"[65] and to share them with countries like Russia, which has long been using Iranian Shaheed drones in Ukraine.

But the one of the most important—and undercounted—threats posed by Iran are its efforts in the cyber domain, including its efforts to target our telecommunications networks and systems. Specifically, according to the DNI, "Iran's growing expertise and willingness to conduct aggressive cyber operations also make it a major threat to the security of U.S. and allied and partner networks and data."[66]

Indeed, the current DNI has noted that "[g]uidance from Iranian leaders has incentivized cyber actors to become more aggressive in developing capabilities to conduct cyber attacks."[67] This is particularly concerning because in 2019, the-DNI Coats told Congress that Iran was "attempting to deploy cyber attack capabilities that would enable attacks against critical infrastructure in the United States and allied countries," and that it was then "capable of causing localized, temporary disruptive effects—such as disrupting a large company's corporate networks for days

Michael Birnbaum, *Russian Submarines Are Prowling Around Vital Undersea Cables. It's Making NATO Nervous,* Washington Post (Dec. 22, 2017), available online at <*https://www.washingtonpost.com/world/europe/russian-submarines-are-prowling-around-vital-undersea-cables-its-making-nato-nervous/2017/12/22/d4c1f3da-e5d0-11e7-927a-e72eac1e73b6_story.html*>.

[59] *See* Jill C. Campbell, *Protection of Undersea Telecommunication Cables: Issues for Congress,* Congressional Research Service (Aug. 7, 2023), at 7, available online at <*https://www.congress.gov/crs_external_products/R/PDF/R47648/R47648.4.pdf*>.

[60] *See 2025 Annual Threat Assessment, supra* n. 4 at 19.

[61] *Id.* at 20.

[62] *Id.* at 16.

[63] *Id.* at 17.

[64] *Id.* at 22.

[65] *Id.*

[66] *Id.*

[67] *Id.*

to weeks—similar to its data deletion attacks against dozens of Saudi governmental and private-sector networks in late 2016 and early 2017."[68]

And we also know that "Iran often amplifies its influence operations with offensive cyber activities[,]" including efforts during the last election cycle to acquire information from the President's campaign and to "manipulate U.S. journalists into leaking [the] information illicitly acquired from the campaign."[69]

These capabilities and efforts demonstrate Iran's interest in and ability to target and use American communications systems to undermine our national security. When combined with the challenges of effectively deterring an actor like Iran, as well as the limited efforts the United States has historically taken to establish real deterrence in the cyber domain by being relatively unwilling to impose significant consequences, the potential for a strategic miscalculation increases significantly as does the threat to American communications networks.

D. North Korea

The DNI also assesses that North Korea will "continue to pursue strategic and conventional military capabilities that target the [United States], threaten U.S. and allied armed forces and citizens, and . . . undermine U.S. power and reshape the regional security environment in [North Korea's] favor."[70]

North Korea's focus, in the cyber domain, is targeting American telecommunications networks and the financial institutions that ride upon them to "fund[] its military development—allowing it to pose greater risks to the United States—and economic initiatives by stealing hundreds of millions of dollars per year in cryptocurrency."[71] However, the DNI also assesses that North Korea "may also expand its ongoing cyber espionage to fill gaps in the regime's weapons programs, potentially targeting defense industrial base companies involved in aerospace, submarine, or hypersonic glide technologies."[72]

Like with China, Russia, and Iran, much of this unsurprising because we knew back in 2019 that "North Korea poses a significant cyber threat to financial institutions [and] remains a cyber espionage threat . . . us[ing] cyber capabilities to steal from financial institutions to generate revenue[,] . . . includ[ing] attempts to steal more than $1.1 billion from financial institutions across the world [and] . . . a successful cyber heist of an estimated $81 million from the New York Federal Reserve account of Bangladesh's central bank."[73]

We also learned, interestingly, in 2019 that North Korea "retains the ability to conduct disruptive cyber attacks,"[74] a capability that we more recently learned was focused on American cyber networks. Specifically, in 2021, the DNI told Congress that that "Pyongyang probably possesses the expertise to cause temporary, limited disruptions of some critical infrastructure networks and disrupt business networks in the United States, judging from its operations during the past decade, and [further that] it may be able to conduct operations that compromise software supply chains."[75] We also learned, in 2022, that "Pyongyang is well positioned to conduct surprise cyber attacks given its stealth and history of bold action."[76]

As with Iran, given North Korea's burgeoning capacity and willingness to conduct operations in the cyber domain, and the relative challenges of using deterrence against a nation like North Korea poses, as well as the limited willingness of the United States to engage in more generally deterrence in the cyber domain, the potential for a tactical miscalculation—and the concomitant threat to American communications networks—is more significant than one might initially assume.

III. Assessing the Threats to America's Communications Infrastructure

When we look across the totality of the threats to America's communications infrastructure posed these four major nation-state threat actors—China, Russia, Iran, and North Korea—what becomes increasingly clear is that it is virtually impossible for any one private sector actor, or even any single industry in the United States alone, writ-large, to effectively combat these the scale, scope and nature of these threats.

[68] *See 2019 Worldwide Threat Assessment, supra* n. 13 at 6.
[69] *See 2025 Annual Threat Assessment, supra* n. 4 at 26.
[70] *Id.*
[71] *Id.* at 28.
[72] *Id.*
[73] *See 2019 Worldwide Threat Assessment, supra* n. 13 at 6.
[74] *Id.*
[75] *See 2021 Annual Threat Assessment, supra* n. 14 at 14; *2022 Annual Threat Assessment, supra* n. 15 at 17.
[76] *See 2022 Annual Threat Assessment, supra* n. 15 at 17.

We are faced today with a nonstop, day-in, day-out, military-grade assault on our Nation's critical infrastructure and that of our allies. This effort is being undertaken by multiple military and intelligence organizations across multiple adversary countries and is focused on the core networks, systems, and technologies that support our governments, telecommunications systems, banking networks, energy grids, and healthcare institutions, just to name a few important ones.

While this assault is not always aimed the destruction or disruption of these networks, systems, or technologies, even the intelligence collection and information operations that our adversaries are running can have massive implications for our economic and national security. They can enable mass-scale intellectual property theft—much of which is already taking place—and thereby undermine America's innovation-driven economy while bootstrapping nations like China. They can also undermine government institutions and cut out basic support for the rule of law across the globe. And they can enable future military and intelligence operations against our nations and its allies. Even more troublingly, we are seeing nation-state adversaries put in place the very capabilities that would enable them to engage in large-scale, sustained disruptions of American and allied critical infrastructure, including key telecommunications networks and systems.

The question then is what is to be done about these threats posed to our core networks, systems, and technologies. As a nation, the stark reality is we are not currently positioned to provide for a comprehensive defense of our nation—nor the very communications systems or networks that American companies help operate—and we do not appear prepared to undertake the actions needed to do so.

One need only look at the Salt Typhoon hacks aimed at our communications infrastructure—primarily for intelligence collection—to understand just how vulnerable (and underprepared) we are to deal with these adversaries. In that case, we learned—after years and years of knowing that the Chinese government and its military and intelligence institutions were focused on this effort—that China had obtained widescale access to our telecommunications networks.[77] Specifically, the FBI stated that China's "targeting of commercial telecommunications infrastructure has revealed a broad and significant cyber espionage campaign," and that Chinese-affiliated actors "have compromised networks at multiple telecommunications companies to enable the theft of customer call records data, the compromise of private communications of a limited number of individuals who are primarily involved in government or political activity, and the copying of certain information that was subject to U.S. law enforcement requests pursuant to court orders."[78]

This was an astounding event; according to the then-Chairman of the Senate Intelligence Committee, Senator Mark Warner (D–VA), it was the "worst telecom hack in our Nation's history—by far,"[79] and according the then-Vice Chair of the Committee (and now current Secretary of State and National Security Advisor) Senator Marco Rubio (R–FL) referred to the hack as "an egregious, outrageous and dangerous breach of our telecommunications systems across multiple companies[.]"[80]

And yet, after the reported convening of a White House Unified Coordination Group (UCG),[81] a lengthy (and apparently still ongoing) law enforcement investiga-

[77] *See* Chris Jaikaran, *Salt Typhoon Hacks of Telecommunications Companies and Federal Response Implications,* Congressional Research Service (Jan. 23, 2025), available online at <*https://www.congress.gov/crs_external_products/IF/PDF/IF12798/IF12798.15.pdf*> ("In early October 2024, media outlets reported that People's Republic of China (PRC) state-sponsored hackers infiltrated United States telecommunications companies (including Internet service providers). . . . [P]ublic reporting suggests that the hackers may have targeted the systems used to provide court-approved access to communication systems used for investigations by law enforcement and intelligence agencies. PRC actors may have sought access to these systems and companies to gain access to presidential candidate communications. With that access, they could potentially retrieve unencrypted communication (*e.g.,* voice calls and text messages).")

[78] *See* Federal Bureau of Investigations, *Joint Statement from FBI and CISA on the People's Republic of China Targeting of Commercial Telecommunications Infrastructure* (Nov. 14, 2024), available online at <*https://www.fbi.gov/news/press-releases/joint-statement-from-fbi-and-cisa-on-the-peoples-republic-of-china-targeting-of-commercial-telecommunications-infrastructure*>.

[79] Ellen Nakashima, *Top Senator Calls Salt Typhoon "Worst Telecom Hack in our Nation's History,"* Washington Post (Nov. 21, 2024), available online at <*https://www.washingtonpost.com/national-security/2024/11/21/salt-typhoon-china-hack-telecom/*>.

[80] Patrick Maguire, *Sen. Marco Rubio Says Chinese Hacking of U.S. Telecom Companies is a "Very Serious Situation that we Face,"* CBS News (Nov. 3, 2024), available online at <*https://www.cbsnews.com/news/marco-rubio-chinese-hacking-american-telecom-companies/*>.

[81] *See, e.g.,* Ellen Nakashima, *White House Forms Emergency Team to Deal with China Espionage Hack,* Washington Post (Nov. 11, 2024) ("The White House on Tuesday convened a meeting of deputy secretaries of key agencies to stand up what's known as a 'unified coordination group.' The group's role is to ensure there is consistent interagency visibility into the response by the

Continued

tion,[82] and a nascent (and incomplete) investigation by the Cyber Safety Review Board (of which I was once a member),[83] not to mention a rushed regulatory effort by the Federal Communications Commission[84] (which has since been reversed by the current FCC in favor of a number of more focused actions directed at the Chinese threat as noted above and in line with a more "agile and collaborative approach to cybersecurity that has proven successful"),[85] the release of two security guidance documents jointly released by a significant number of law enforcement and intelligence agencies from multiple allied countries,[86] and legislation introduced,[87] we have precious little substantive action to show for this hack.

According to press reports, at least some of the telecommunications companies involved have managed to remove the attackers (or at least those they could identify),[88] and the breadth of the hack appears to have been global, affecting at least nine telecommunications companies,[89] at least a dozen nations,[90] and targeting senior U.S. government officials,[91] with significant amounts of metadata and the content of certain individuals' communications obtained.[92] And the FCC, while reversing its earlier rush to regulation, has obtained series of commitments from American communications companies to upgrade their cybersecurity practices by taking

FBI, the Office of the Director of National Intelligence, and the Department of Homeland Security's Cybersecurity and Information Security Agency (CISA)."); *see also Salt Typhoon Hacks, supra* n. 61 at 2 (discussing Salt Typhoon and noting that "[b]y publicly available counts, this is the fourth time that the U.S. government has established a Cyber UCG—which were previously established for China's compromise of Microsoft Exchange services in 2021, Russia's compromise of SolarWinds in 2021.")

[82] *See, e.g.,* Federal Bureau of Investigation, *FBI Seeking Tips about PRC-Targeting of U.S. Telecommunications* (Apr. 24, 2025), available online at *<https://www.ic3.gov/PSA/2025/PSA250424-2>*.

[83] Martin Matishak, *Cyber Incident Board's Salt Typhoon Review to Begin Within Days, CISA Leader Says,* The Record (Dec. 3. 2024), available online at *<https://therecord.media/salt-typhoon-csrb-review>*.

[84] *See* Federal Communications Commission, *Protecting the Nation's Communications Systems from Cybersecurity Threats,* Declaratory Ruling and Notice of Proposed Rulemaking (Jan. 15, 2025), available online at *<https://docs.fcc.gov/public/attachments/FCC-25-9A1_Rcd.pdf>*; *see also* Federal Communications Commission, *Chairwoman Rosenworcel Announces Agency Action to Require Telecom Carriers to Secure their Networks* (Dec. 5, 2024), available online at *<https://docs.fcc.gov/public/attachments/DOC-408013A1.pdf>*.

[85] *See* Federal Communications Commission, *Protecting the Nation's Communications Systems from Cybersecurity Threats,* Order on Reconsideration (Nov. 20, 2025), available online at *<https://docs.fcc.gov/public/attachments/FCC-25-81A1.pdf>*.

[86] *See* National Security Agency, *et al., Countering Chinese State-Sponsored Actors Compromise of Networks Worldwide to Feed Global Espionage System* (Aug/Sept. 2025), available online at *<https://media.defense.gov/ 2025/Aug/22/2003786665/1/1/0/CSA_COUNTERING_CHINA_STATE_ACTORS_COMPROMISE_OF_NETWORKS.PDF>*; Cybersecurity and Infrastructure Security Agency, *et al., Enhanced Visibility and Hardening Guidance for Communications Infrastructure* (Dec. 3, 2024), available online at *<https://www.ic3.gov/CSA/2024/241203.pdf>*.

[87] *See* Senator Ron Wyden, *Wyden Releases Draft Legislation to Secure U.S. Phone Networks Following Salt Typhoon Hack* (Dec. 10, 2024), available online at *<https://www.wyden.senate.gov/news/press-releases/wyden-releases-draft-legislation-to-secure-us-phone-networks-following-salt-typhoon-hack>*.

[88] *See* Matt Kapko, *AT&T, Verizon say they evicted Salt Typhoon from their networks,* Cybersecurity Dive (Jan. 7. 2025), available online at *<https://www.cybersecuritydive.com/news/att-verizon-salt-typhoon/736680/>*.

[89] *See* The White House, *On-the-Record Press Gaggle by White House National Security Communications Advisor John Kirby* (Dec. 27. 2024), available online at *<https://bidenwhitehouse.archives.gov/briefing-room/press-briefings/2024/12/27/on-the-record-press-gaggle-by-white-house-national-security-communications-advisor-john-kirby-38/>* ("[A]s we look at China's compromise of now nine telecom companies, the first step is creating a defensible infrastructure.") (statement of Deputy National Security Advisor Anne Neuberger).

[90] *See* Aamer Madhani, *White House Says at Least 8 U.S. Telecom Firms, Dozens of Nations Impacted by China Hacking Campaign,* Associated Press (Dec. 4, 2024), available online at *<https://apnews.com/article/china-hack-us-telecoms-salt-typhoon-88cabc592dae2fa870772c5ce4ace5ea>* ("A top White House official on Wednesday said at least eight U.S. telecom firms and dozens of nations have been impacted by a Chinese hacking campaign . . .").

[91] *Id.* ("The U.S. believes that the hackers were able to gain access to communications of senior U.S. government officials and prominent political figures through the hack, Neuberger said.")

[92] *See On-The-Record Press Gaggle, supra* n. 89 ("Our understanding is that a large number of individuals were geolocated in the Washington, D.C./Virginia area. We believe it was the goal of identifying who those phones belong to and if they were government targets of interest for follow-on espionage and intelligence collection of communications, of texts, and phone calls on those particular phones. So, we believe a large number of individuals were affected by geolocation and metadata of phones; a smaller number around actual collection of phone calls and texts. And I think the scale we're talking about is far larger on the geolocation; probably less than 100 on the actual individuals.") (statement of A. Neuberger).

coordinated actions to harden their networks against a range of cyber intrusions.[93] These actions include accelerating the patching of outdated or vulnerable equipment, updating and reviewing system access controls, disabling unnecessary outbound connections, improving threat-hunting efforts, and cybersecurity information sharing.[94] In addition, the FCC has recently been working more closely with regulators from the U.K., Canada, Australia, and New Zealand to strengthen cooperation amongst these partners to respond to threats against our communications networks.[95]

Yet the impact of these hacks, particularly when combined with other hacks, remains quite serious. The most recent security guidance document released by the U.S. and multiple allied intelligence and law enforcement agencies noted that the Salt Typhoon actors has been operating "globally since at least 2021" and indicated that "[t]he data stolen through this activity against *foreign telecommunications and Internet service providers (ISPs), as well as intrusions in the* lodging and transportation sectors, ultimately can provide Chinese intelligence services with the capability to identify and track their targets' communications and movements around the world."[96] And while that guidance document specifically offered recommendations to close known vulnerabilities in systems built at least three allied providers, the government agencies also noted that they suspected that at least six other vendors may also have been compromised.[97]

At the same time, earlier this year, more than six months after the hack was identified, the FBI sought the public's help in "report[ing] information about PRC-affiliated activity publicly tracked as 'Salt Typhoon' and the compromise of multiple U.S. telecommunications companies, especially information about specific individuals behind the campaign[,]" and specifically noting that if members of the public, "have any information about the individuals who comprise Salt Typhoon or other Salt Typhoon activity, we would particularly like to hear from you."[98] And the U.S. government—apparently having identified at least three Chinese entities involved in the incident[99]—has issued sanctions against one of them.[100]

And yet, in perhaps one of the most stunning revelations to come out of this incident, even as the FCC and White House were calling for significant regulation of American telecommunications companies,[101] the outgoing head of the Department of Homeland Security's Cybersecurity and Infrastructure Security Agency (CISA), published a blog post stating that "CISA threat hunters previously detected the same actors in U.S. government networks."[102] The next day, at an on-the-record event at the Foundation for the Defense of Democracies, the CISA Director stated that while the government had previously detected the Salt Typhoon actors on other Federal networks at the time "[w]e saw it as a separate campaign called another

[93] *See Order on Reconsideration, supra* n. 85 at 2, 9–10, 13–14 & 17.

[94] *Id.*

[95] *Id.* at 17.

[96] *See Countering Chinese State-Sponsored Actors, supra* n. 86 at 5.

[97] *Id.* at 6–7.

[98] *See FBI Seeking Tips, supra* n. 82.

[99] *See Countering Chinese State-Sponsored Actors, supra* n. 86 at 5 (naming Sichuan Juxinhe Network Technology Co. Ltd., Beijing Huanyu Tianqiong Information Technology Co., Ltd., and Sichuan Zhixin Ruijie Network Technology Co., Ltd. as being linked to Salt Typhoon operations and "provid[ing] cyber-related products and services to China's intelligence services, including multiple units in the People's Liberation Army and Ministry of State Security.").

[100] *See, e.g.,* U.S. Department of the Treasury, *Treasury Sanctions Company Associated with Salt Typhoon and Hacker Associated with Treasury Compromise* (Jan. 17, 2025) ("Additionally, OFAC is sanctioning Sichuan Juxinhe Network Technology Co., LTD., a Sichuan-based cybersecurity company with direct involvement in the Salt Typhoon cyber group, which recently compromised the network infrastructure of multiple major U.S. telecommunication and Internet service provider companies. People's Republic of China-linked (PRC) malicious cyber actors continue to target U.S. government systems, including the recent targeting of Treasury's information technology (IT) systems, as well as sensitive U.S. critical infrastructure.")

[101] *See Chairwoman Rosenworcel Announces Agency Action,* supra n. 84; *see also On-The-Record Press Gaggle, supra* n. 89 ("[W]e need to see every member of the—all the FCC commissioners vote to implement the required minimum cybersecurity practices across telecom, because once those are in place, once companies are taking those steps to make their networks defensible, we would feel more confident to say that the Chinese actors have been evicted and can continue to not be able to come in.") (statement of A. Neuberger).

[102] *See* Jen Easterly, *Strengthening America's Resilience Against the PRC Cyber Threats,* CISA (Jan. 15, 2025), available online at <*https://www.cisa.gov/news-events/news/strengthening-americas-resilience-against-prc-cyber-threats*>.

goofy name[.]"[103] According to newspaper reports, "CISA's observations didn't prevent Salt Typhoon from attacking the telecom networks en masse, but [the CISA Director] presented the agency's threat hunting and intelligence gathering capabilities as an example of intra-government and public-private collaboration improvements made under her stewardship of the agency." [104]

While all this may make one recall the findings of the 9/11 Commission report, which noted that the U.S. government had both successfully the potential of a major terrorist attack and knew of specific terrorists with visas to enter the United States, but critically failed to share actionable information in a timely fashion with those able to identify and stop those individuals,[105] it also raises important questions about where the responsibility for defending the Nation against these types of attacks ought properly lie.

As I previously noted in testimony before another House committee back in 2020, while we've established an entity with the theoretical responsibility for defending the Nation in the cyber domain in U.S. Cyber Command, we've never provided it with anywhere near the kind of authorities or resources it would take to actually do that job.[106] And while there may not be a consensus in our Nation today on what the government's role in defending our Nation's overall cyber infrastructure ought exactly be, the idea that we ought leave our critical infrastructure provider alone to defend themselves against foreign nation-state threat actors—or even worse penalize them when they find themselves unable to stop such actors who come to the fight with virtually unlimited resources—is not only unrealistic, it is setting up ourselves to fail every time.[107] Just as we don't expect Target or Walmart to have surface-to-air missiles on the roofs of their warehouses to defend against Russian Bear aircraft dropping bombs in the United States, we ought not expect the same from our telecommunications and infrastructure companies in the cyber domain.[108]

IV. Considering Effective Responses to Defend America's Communications Infrastructure

This, of course, puts front and center the question of what might be done to address this clear and present threat to the America's communications infrastructure and that of our allies and partners.

First and foremost, we must remember that private sector companies, including those in the telecommunications and infrastructure sectors, are not primarily in the business of defending themselves against cyberattacks; rather, they operate in order to provide products and services to customers and to generate economic returns from such business. And this is a net positive for our Nation and its allies. After all, without these companies, the vast majority of our AI tools and large language models, which rely often rely on connections to cloud infrastructure and access to massive amounts of data and compute, wouldn't be able to operate or service customers large and small across the globe. Without a strong American communications sector, we wouldn't have built, expanded, or maintained the freedom of access to the global information networks that form the Internet. And without American and allied telecommunications and infrastructure companies, we would likely not

[103] *See* Matt Kapko, *CISA clocked Salt Typhoon in Federal networks before telecom intrusions,* Cybersecurity Dive (Jan. 16, 2025), available online at <*https://www.cybersecuritydive.com/news/salt-typhoon-federal-networks-easterly/737552/*>.

[104] *Id.*

[105] *See* National Commission on Terrorist Attacks Upon the United States, *The 9/11 Commission Report* (July 22, 2004), at 155–59, 181–82, 266–72, available online at <*https://www.govinfo.gov/content/pkg/GPO-911REPORT/pdf/GPO-911REPORT.pdf*>.

[106] *See CISA Clocked Salt Typhoon, supra* n. 103.

[107] *See* GEN. Keith B. Alexander, Jamil N. Jaffer, and Jennifer S. Brunet, *Clear Thinking about Protecting the Nation in the Cyber Domain,* Cyber Defense Review 2, no. 1 at 29, 33 (2017), available online at <*https://nationalsecurity.gmu.edu/wp-content/uploads/2017/03/CDRV2N1_Clear-Thinking_Alexander_Jaffer_Brunet_032217-1.pdf*> ("The fact is that commercial and private entities cannot be expected to defend themselves against nation-state attacks in cyberspace. Such organizations simply do not have the capacity, the capability, nor the authority to respond in a way that would be fully effective against a nation-state attacker in cyberspace. Indeed, in most other contexts, we do not (and should not) expect corporate America to bear the burden of nation-state attacks.").

[108] *See id.; see also, e.g.,* GEN (Ret) Keith B. Alexander & Jamil N. Jaffer, *Iranian Cyberattacks Are Coming, Security Experts Warn,* Barron's (Jan. 10, 2020) ("Expecting individual companies to defend themselves against a nation state with virtually unlimited financial resources and human capital does not make sense. Yet today that is our national policy in cyberspace. This is so even though, in every other context, defense against nation-state attacks is the province of the government. We don't expect Target or Walmart to have surface-to-air missiles to defend against Russian Bear bombers. Yet when it comes to cyberspace, we expect exactly that of every American company, large or small.").

have seen the massive gains from innovation that have driven the U.S. and world economy for at least the last five decades.

To preserve the value these organizations—and many other private sector entities—provide us, the Federal government must partner tightly with industry to enable better cyber defense. This means sharing massive amounts of data (classified and otherwise), providing incentives to obtain and deploy better defensive cyber systems and capabilities, and aggressively imposing costs on adversaries, in appropriate circumstances, to deter the deployment or use of potentially disruptive or destructive capabilities. The fact of the matter is that we cannot cede this critical ground to our adversaries by leaving companies in the telecommunications, infrastructure, and technology sectors alone to defend themselves against nation-state attacks.

One example of providing the right incentives would be to consider—in reauthorizing (and ideally making permanent) the Cyber Information Sharing Act of 2015 (which having expired earlier this year was the subject of a short reauthorization in the recent government reopening deal)—providing the type of liability and regulatory protections that were contained when the original version of that legislation as passed by the House back in 2011.[109] Those protections, which fell out of the legislation negotiated by the House and Senate four years later when it was enacted,[110] are a key example of lining up the incentives between industry and the government and using carrots, instead of the proverbial regulatory stick.[111] Likewise, providing clear authority and direction to provide security clearances and share classified intelligence with the private sector in a manner that allows them to operationalize it, as well as ensuring that private sector entities can go anywhere in the government to share information, as the original legislation did, are also key elements to better collaborating with the private sector on cyber defense. The government cannot expect the private sector to do strong work sharing information within and across sectors, while also maintaining massive silos within the government. We can and should expect better of our Federal agencies.

Another key effort that the government ought take up is affirmatively harmonizing existing compliance requirements and regulations across various agencies, and to adopt the collaborative, voluntary approach taken by the FCC, in the first instance. At a minimum, the government ought permit compliance with one set of regulations—ideally those developed in the collaborative manner like that used by the FCC—that the serve as effective compliance with others where the subject matter of the regulation is similar. Likewise, getting unhelpful regulations out of the way and avoiding undermining our own national security policies for political gain by going after our best players—large and small—in the technology industry is critical to avoid. Efforts in recent years to amend longstanding and highly effective antitrust laws that have served our economy well for decades,[112] are a key example of the kind of new policies that would be highly detrimental in the context of the ongoing economic and national security competition with China. These efforts, which target a handful of technology companies based on the nature and scale of their business, are largely driven by policy issues unrelated to innovation or competition.[113] It also sends the wrong message to startup innovators, namely, that if

[109] *See* Cyber Intelligence Sharing and Protection Act, H.R. 3523, 112th Cong. (engrossed in the House), available online at <*https://www.congress.gov/112/bills/hr3523/BILLS-112hr3523eh.pdf*>.

[110] *See* Consolidated Appropriations Act of 2015, P.L. 114–113, 129 Stat. 2242 ("CISA"); *see also* Cybersecurity Information Sharing Act of 2015, S. 754, 114th Cong. (as passed by the Senate on Oct. 27, 2015).

[111] *See* Jamil N. Jaffer, *Carrots and Sticks in Cyberspace: Addressing Key Issues in the Cybersecurity Information Sharing Act of 2015,* 67 S. Car. L. Rev. 585, 589–98 (2016), available online at <*https://scholarcommons.sc.edu/cgi/viewcontent.cgi?article=4180&context=sclr*>.

[112] *See, e.g.,* American Innovation and Choice Online Act, S.2992, 117th Cong. (2021); Open App Markets Act, S.2710, 117th Cong. (2021).

[113] *See* Bill Evanina & Jamil N. Jaffer, *Kneecapping U.S. Tech Companies Is a Recipe for Economic Disaster,* Barron's (June 17, 2022), available online at <*https://www.barrons.com/articles/kneecapping-u-s-tech-firms-is-a-recipe-for-economic-disaster-51655480902*> ("Conservatives are often worried—sometimes for good reason—that certain social or mainstream media companies might actively seek to suppress or quiet conservative voices. On the liberal side, there are a range of legitimate concerns with technology companies, including the displacement of traditional labor in the new gig economy. . . Yet rather than tackling these concerns directly by going after the specific behaviors or actions that trouble ordinary Americans, politicians in Washington have chosen instead to vilify some of our most successful companies and to go after them economically."); *see also* David R. Henderson, *A Populist Attack On Big Tech,* The Hoover Institution (Mar. 3, 2022), available online at <*https://www.hoover.org/research/populist-attack-big-tech-0*>.

they thrive and become highly successful, the government might seek to target them for special attention, creating laws just to cut them down to size.[114] The White House has made clear it is on a strong deregulatory path, and action across all of these domains, could help significantly ensure that we are empowering the American private sector to innovate and create and implement better cyber defenses in partnership with the government.

Likewise, we ought work with our allies and partners across the globe—as well as investors and innovators who share our views—to advance American and allied interests, both by deploying capital effectively and ensuring that we don't undermine one another's strongest capabilities in the larger fight against our common adversaries. This also means that we must help our allies across the globe to better protect their own telecommunications infrastructure, which includes sharing information and intelligence ahead of potential threats and coming together to do what we did so effectively here in the United States—removing adversary capabilities, like Huawei and ZTE—from the global telecommunications infrastructure.

It likewise also means that we must lean aggressively forward—both globally and at home—as we look to put in place new technologies like 5G Advanced and 6G, including working collaboratively with across allied governments and industry to get the right international standards in place, including prioritizing allied collaboration on spectrum and on efforts like ORAN, while also protecting historical capabilities, like WHOIS, that have gone—or are going—dark.

The government also ought provide the right incentivizes for industry to build out both domestic and allied communications infrastructure and to invest in the capacity and innovation to deliver advanced technology capabilities globally. To that end, the government should provide tax and other economic incentives for increased private investment in the development of such technologies, the broader deployment of large-scale computing and communications infrastructure to support cloud and edge computing, and the expansion of AI capabilities being made available to U.S. and allied innovators across the globe.

These incentives are particularly important because the security of—and trust in—America's communications infrastructure (and that of our allies) is so central to our success in the larger competition with China. After all, no matter how secure our core technology capabilities themselves are, if we connect them to a weakly defended network, they will no longer be secure.

If we are to win this competition, therefore, we must ensure that we are properly incentivizing the buildout of these trusted communication capabilities in both the hardwired (including fiber) and wireless domains. Moreover, the government should also work with innovators and investors across the who share our interests to understand key government needs and priorities to develop the innovations and capabilities to address those needs.

Likewise, ensuring that the United States and our allies are able to access the manufacturing capacity and workforce necessary to support a modern technology and communications infrastructure—including consistent access to semiconductors, critical minerals, and other core materials necessary to support major technological innovation—will also be of critical strategic importance to the United States in the coming years, particularly as our competition with China heats up. It is critical that government and industry work together to create the right tax and regulatory incentives to ensure that American and allied companies invest their money here and in allied nations to create much-needed capacity, including in the communications, technology, and infrastructure industries, and to ensure that we have the skilled workers necessary to build and maintain this trusted capacity and capability.

When it comes to addressing lessons learned from the Salt Typhoon hacks and the Volt Typhoon capability deployments, Congress ought consider collaborating with the Executive Branch to appoint an independent third-party commission, tak-

[114] *See* Klon Kitchen & Jamil Jaffer, *The American Innovation & Choice Online Act is a Mistake,* The Kitchen Sync (Jan. 19, 2022), available online at <*https://www.thekitchensync.tech/p/the-american-innovation-and-choice*> ("Going after our technology companies, particularly a targeted shot at certain big ones, sends the wrong message to startups and investors alike; it tells them that if you are innovative enough to be successful and grow significantly larger, you may be targeted for different treatment. This undermines not only the companies that are likely to be investing in R&D over the next decade and generating some of the key innovations that will contribute to our national security, it also undermines a central proposition that has created a robust tech ecosystem in this country: take risk, innovate, fail fast and often, and when you succeed, reap the rewards so long as you don't exploit your position to gain unfair advantage."); Evanina & Jaffer, *Kneecapping U.S. Tech Companies, supra* n. 86 ("Picking and choosing individual companies to be treated differently than others under our antitrust laws is inconsistent with the heart of our economic system, which Seeks to reward innovation and success, not penalize them.").

ing a page from the successful 9/11, Intelligence Reform, and Cyberspace Solarium Commissions, putting legislators on the panel alongside distinguished private sector and policy leaders to identify key challenges and draft actionable proposals that can actually be enacted by Congress and implemented by the Executive Branch in the near-term.

As noted above, another key element of any effort to push back on adversary operations on our communications networks or to control those networks communications network is to effectively deter those threat actors from taking action in the first instance. While there are those who argue that deterrence doesn't work in the technology domain, the reality is we simply don't practice real, effective deterrence today.[115] We don't talk about the redlines that, if crossed, would provoke a response from the United States, we don't talk about our capacity to respond, we don't talk what a response might look like, and when our communications systems are threatened (or hit), we often simply fail to respond.[116] Even worse, in the rare circumstances when we do respond, we often do so in a fairly limited fashion and without any public acknowledgement or attribution.[117] The problem with this approach is that it undermines any deterrence benefit we might otherwise enjoy.

The fact is that if an attacked party is willing to deliver real consequences, and is seen to actually do so, deterrence can in fact work to protect our communications and technology infrastructure.[118]

As such, when it comes to threats to our communications infrastructure, we should be clear about our capabilities, put out a clear declaratory policy on our redlines, and be willing to take swift, decisive, and visible action when those lines are crossed. To do so, therefore, we must authorize, fund, and encourage more forward-leaning efforts by the government to overtly impose substantive costs on our cyber adversaries. It is only through such clear, public, and attributable action can we possibly expect to effectuate real deterrence in this domain.

And finally, the key rubric to apply in this domain, as well as in other key areas of technology across the board, is to apply the traditional American approach to innovation: first, do no harm. In practice, this means allowing innovation to flourish, only having the government intervene in the limited and clear cases, circumstances which ought be extremely rare. American and allied innovation deserves our protection and our support. We ought not, like some of our allies, regulate first and innovate latter. To the contrary, we ought do exactly the opposite.

V. Conclusion

Such an approach—across all these fronts—is all the more critical when, as now, the United States and our allies are in a massive competition—economic, military, and political—with a near-peer competitor, where technology and innovation is at the heart and soul of the competition. This is a fight we can—and should—win; we just have to get out of our own way and enable our best, most capable actors across the government and industry.

Senator FISCHER. Thank you, Mr. Jaffer. Ms. Jordan, you are now recognized for your opening statement.

STATEMENT OF DEBRA JORDAN, FORMER CHIEF, PUBLIC SAFETY AND HOMELAND SECURITY BUREAU, FEDERAL COMMUNICATIONS COMMISSION

Ms. JORDAN. Good morning, Chair Fischer, Ranking Member Luján, Chair Cruz, and members of the Subcommittee. Thank you for the opportunity to appear before you today.

[115] *See* Jamil N. Jaffer, *Statement for the Record, Safeguarding the Federal Software Supply Chain, Committee on Oversight and Accountability,* Subcommittee on Cybersecurity, Information Technology, and Government Innovation (Nov. 29, 2023), at 10, available online at <*https://oversight.house.gov/wp-content/uploads/2023/11/Written-Statement-Jaffer.pdf*> ("[T]he reality is that the United States does not effectively practice deterrence in the cyber domain for a variety of reasons.")

[116] *Id.*

[117] *Id.*

[118] *See* Keith B. Alexander & Jamil N. Jaffer, *Iran's Coming Response: Increased Terrorism and Cyber Attacks?,* The Hill (May 15, 2019) ("While some have suggested that deterrence doesn't work in the cyber domain, the reality is that if an attacked party is willing to deliver real consequences and is seen to do so, deterrence can in fact work.").

I am grateful to have served nearly 10 years at the Federal Communications Commission as a Deputy and then Bureau Chief for the Public Safety and Homeland Security Bureau. My responsibilities included national security, cybersecurity, and resilience of the communications sector. As a career civil servant, I was honored to have served under four Commission Chairs, from both parties.

Before joining the FCC, I spent three decades as a civilian with the U.S. Navy. There I implemented the Navy's first ever cybersecurity framework for critical systems such as electrical, water, and wastewater.

A little over a year ago, while I was at the FCC, the U.S. uncovered Salt Typhoon as a sophisticated campaign sponsored by the Chinese government. We now know that they infiltrated nine of our Nation's largest communications providers, and at least 200 other U.S. organizations, including government agencies. They exfiltrated millions of calls and text messages and metadata of targeted individuals, including then candidates President Trump, Vice President Vance, then Vice President Harris, as well as Members of Congress. Additionally, they compromised systems that log U.S. law enforcement requests for criminal wiretaps, potentially tipping off Chinese intelligence about American investigative targets.

And if Salt Typhoon does not make you shudder, let's go back a little further in time to Volt Typhoon. Active since at least 2021, but not revealed until much later, the attack was attributed to Chinese hackers who gained widespread access to critical infrastructure like coms, water, and power systems. They used a tactic known as "living off the land," where they stole credentials, quietly used administrative accounts to collect data, and retain high-level access to networks. They remain in the networks in preparation for potential armed conflict between the U.S. and China over Taiwan.

These attacks highlight the vulnerabilities in our communications networks, which provide the foundation of trillions of dollars of economic captivity. So how do we secure our communications networks, which serve as the underpinnings of our modern digital society? We can either lean forward, leveraging flexible cyber standards, to support our Nation's economy and security, or we can sit back and wait for the inevitable next attack to happen.

After the revelation of Salt Typhoon, the FCC leaned forward, in January 2025. The FCC ruled that Section 105 of the Communications Assistance for Law Enforcement Act, or CALEA, requires telecom providers to secure their networks against unlawful access. Also, the FCC proposed rules that would require communications providers to certify that they have created and implemented an up-to-date cyber risk management plan, which would strengthen network defenses from future cyberattacks.

However, on November 20, 2025, the FCC reversed the ruling, withdrew the proposed rules, putting the Nation at risk. The FCC cited engagement with providers and, quote, "their agreement to take extensive steps to protect national security interests," unquote. However, the FCC does not cite any process by which the providers will be held accountable to meet specific commitments. From my experience as Bureau Chief, I am not convinced that providers will take sufficient and sustained actions in the wake of Volt and Salt Typhoon without a strong verification regime. As things stand now, we can hope that providers are taking appropriate steps long-term, and hope is not really a strategy to secure our networks.

So what can Congress do? I have three recommendations.

First, we have tools such as the Cyber Risk Management framework developed by NIST. Congress should encourage the FCC to require the NIST Cybersecurity Framework, or similar guidance, for all telecom providers. The framework is flexible and developed in collaboration with industry and the public to assist organizations to manage and reduce cyber risks.

Second is to upgrade our communications infrastructure. Keeping communications infrastructure current is critical, but also costly. I encourage Congress to fully fund communications infrastructure such as Next Generation 911 and cyber funding for state, local, Tribal, and territorial entities. We cannot enable modern digital network security when running on old analog infrastructure.

And last, verification must be a part of trust. We must establish a verification regime to ensure the security of our Nation's communications infrastructure. We have seen, time and again, where providers have not implemented even some of the most basic cyber hygiene consistently across their networks, such as changing default passwords. Industry says they are committed to implementing extensive cyber protections, so let's establish a regime in a secure setting for them to share their progress and further plans.

Thank you, and I look forward to your questions.

[The prepared statement of Ms. Jordan follows:]

Testimony of Debra Jordan, Former Chief, Public Safety and Homeland Security Bureau, Federal Communications Commission

Good morning, Chair Fischer, Ranking Member Luján, Chair Cruz, Ranking Member Cantwell, and Members of the Subcommittee. Thank you for the opportunity to appear before you today.

I appreciate the Senate's interest in this critical and urgent topic and am honored to share my perspective on Defending America's Networks. I'm grateful to have served for nearly 10 years at the Federal Communications Commission as the Deputy and then Bureau Chief for the Public Safety & Homeland Security Bureau, where my responsibilities included national security, cybersecurity, and resilience of the communications sector. As a career civil servant, I was honored to have served under four Commission Chairs, from both parties. My responsibilities included interagency and multi-stakeholder engagements regarding the communications sector and its impacts on our Nation either directly or through cascading effects on other critical infrastructure sectors—such as electric, water, transportation, and healthcare.

Before joining the FCC, I spent three decades as a civilian with the U.S. Navy, serving as Command Information Officer for Naval Facilities and Engineering Command. There, I developed and obtained funding to implement the Navy's first ever cybersecurity framework for critical systems such as electrical, water, and wastewater.

A little over a year ago, while I was at the FCC, the U.S. uncovered Salt Typhoon, a sophisticated campaign sponsored by the Chinese government. We know now they infiltrated nine of our Nation's largest communications providers, and at least 200 other U.S. organizations, including government agencies. Believed to have been carried out by an advance persistent threat actor attributed to the Chinese Ministry of State Security (MSS), Salt Typhoon exfiltrated millions of metadata records and content associated with calls and text messages of targeted individuals to include then-candidates President Trump and Vice President Vance, then Vice President Harris, and members of Congress. To be specific:

- They monitored live phone calls, gaining access to cellphone and data networks, enabling real-time eavesdropping of calls and texts.
- They harvested sensitive data by collecting private communications, including those of individuals involved in government or political activities

- And they compromised law enforcement systems by accessing systems that log U.S. law enforcement requests for criminal wiretaps, potentially tipping off Chinese intelligence about American investigative targets.

If that doesn't make you shudder—let's go a little further back in time. Active since at least 2021 but not revealed until much later—is Volt Typhoon. The Volt Typhoon attack was attributed to Chinese hackers who gained wide-spread access to critical infrastructure systems using a tactic known as "living-off-the-land." These hackers stole credentials and quietly used administrative accounts to collect data and retain high level access to essential networks, remaining in the networks in preparation for a potential armed conflict—such as one between the U.S. and China over Taiwan.

This was an earlier advance persistent threat attributed to China. How did it work? Chinese-attributed hackers gained access to numerous critical infrastructure networks and systems with privileged admin-level accounts and valid passwords. They didn't use a virus—but rather gained access through stolen credentials and therefore look like valid users. Basically—living in our networks. They have been quietly using these accounts to:

(1) collect data, including credentials from local and network systems,

(2) put the data into an archive file to stage it for exfiltration, and then

(3) use the stolen valid credentials to maintain persistence.

These attacks highlight the vulnerabilities in our communications networks, which provide the foundation for 1/6 of our Nation's economy. And trillions of dollars of economic activity depend on these networks every day. So, how do we secure our communications networks—which serve as the underpinnings of our modern digital society? We can either sit back or lean forward regarding the security of our networks. We can lean forward leveraging flexible cyber standards to support our Nation's economy and security, or we can sit back and wait for the inevitable next attack to happen.

After the revelation of Salt Typhoon, the FCC leaned forward in January 2025, by adopting a Declaratory Ruling finding that Section 105 of the Communications Assistance for Law Enforcement Act ("CALEA") requires telecommunications carriers to secure their networks against unlawful access or interception of communications. That action was accompanied by a proposal to require communications service providers to certify to the FCC that they have created and implemented an up-to-date cybersecurity risk management plan, which would strengthen network defenses from future cyberattacks. Similar requirements had already been adopted or proposed in multiple regulatory actions, such as being required of recipients of universal service high-cost support through the Enhanced Alternative Connect America Cost Model. The specific requirements were carefully designed to provide a risk-based, flexible approach while offering the Department of Commerce's National Institute for Standards and Technology (NIST) cybersecurity framework as a recommended option to meet the requirements. This approach was also coordinated with other regulators through the Cybersecurity Forum for Independent and Executive Branch Regulators. It provides a non-prescriptive, risk-based approach that allows agile flexibility, while providing a foundational framework with which to collaborate in a multi-stakeholder environment.

However, on November 20, 2025, the Commission reversed the ruling and putting the Nation at risk. The FCC cited engagement with providers and "their agreement to take extensive steps to protect national security interests." However, the Commission does not cite any process by which providers will be held accountable to meet specific commitments. From my experience as Bureau Chief, I am not convinced that providers will take sufficient, sustained actions in the wake of Salt and Volt Typhoon without a strong verification regime. In my experience, the Commission could have incorporated the discussions and agreements from providers into the requirement to create, update, and implement a cyber risk management plan. That would have merged the accountability aspect with the providers' agreements. As things stand now, we can only hope that providers are taking appropriate steps and that these actions are sustained as the cyber threats evolve. And hope is not a strategy to secure our networks.

So, what can Congress do? I have three recommendations:

First, we have tools such as the Cybersecurity Framework developed by NIST. Congress should encourage the FCC to require the NIST Cybersecurity Framework (or similar guidance) for all telecommunications providers. The framework is flexible and developed in collaboration with industry and the public to assist organizations to manage and reduce cyber risks. The FCC already requires small subsets of communications providers to develop and implement cyber risk management plans, citing the NIST Cybersecurity Framework as a model framework; in fact, they just proposed in August to require this of subsea cable licensees. Why not make this a requirement across all communications providers to ensure a ubiquitous level of cyber risk management?

Second, is to upgrade our communications infrastructure. Keeping communications infrastructure current is critical, but also costly. I encourage Congress to fully fund communications infrastructure such as Next Generation 911 and cyber funding for state, local, Tribal, and territorial entities. We can't enable modern digital network security when running on old analog infrastructure.

And lastly, verification must be part of trust. I agree that it's critical for industry to own the implementation of cyber risk management and that collaboration among government and industry stakeholders is key. But trust without verify is an incomplete solution. We must establish a verification regime to ensure the security of our Nation's communications infrastructure from the largest to the smallest providers. We've seen time and again through outage and enforcement investigations, where providers have not implemented even some of the most basic cyber hygiene uniformly across their networks, such as changing default passwords. Their networks are large, complex and difficult to secure—and yet they are critical to our Nation's economy and security. Industry says they're committed to implementing extensive cyber protections, so let's establish a regime in a secure setting for them to share their progress and further plans.

Thank you and I look forward to your questions.

Senator FISCHER. Thank you, Ms. Jordan.

We have been joined by the Chairman of the Commerce Committee, Senator Cruz. Would you like to make some opening remarks, sir?

STATEMENT OF HON. TED CRUZ, U.S. SENATOR FROM TEXAS

Chairman CRUZ. Thank you, Madam Chairman. I appreciate it, and thank you for holding this hearing. We have a distinguished panel before us and I want to thank each of our witnesses for being here to share your expertise.

In our digital age, communications networks form the cornerstone of our economy and our national security. That makes them a top target not only for criminals seeking financial gain, but also for our adversaries.

America's enemies have learned they do not need to launch missiles or deploy troops to harm the United States. Instead, they can use teams of skilled and well-resourced cyber hackers to steal our intellectual property, to gather intelligence, and to hide within critical infrastructure to disrupt essential services, all while maintaining plausible deniability.

2025 has been a pivotal year in network security, marked by the rise of AI-empowered attacks and defenses, alongside persistent risks ranging from infrastructure sabotage to increased supply chain vulnerabilities. Incidents such as Salt Typhoon and the SIM farms recently discovered near the United Nations headquarters in New York have served as sobering reminders of how relentless and creative our adversaries continue to be.

Unfortunately, there is no single, silver-bullet solution to address cybersecurity. Protecting America's communications networks is a complex undertaking that demands continued vigilance and cannot be reduced to rote box-ticking.

The United States is a primary target for cyber threats precisely because we lead the world in technological innovation. Our challenge, therefore, is to secure communications infrastructure effectively without creating excessive and useless regulation that stifles the very innovation that gives us our competitive edge.

That is why I commend FCC Chairman Brendan Carr for moving last month to rescind the Biden administration's misguided January 2025 Declaratory Ruling, which tried to shoehorn new cybersecurity mandates into a 1994 law about cooperating with law enforcement. Chairman Carr's decision to shift away from ineffective and burdensome requirements is consistent with both the Commission's legal authority and sound policy.

Federal agencies cannot regulate their way into creating perfect network security, and attempts to do so will backfire. Forcing telecom carriers to chase the false security of compliance checklists instead of engaging real-world threats diverts resources away from the necessary partnerships and response capabilities that actually stop intrusions.

Worse still, the legal risks these compliance regimes impose have a chilling effect, as armies of lawyers focus on avoiding lawsuits and regulatory penalties instead of information-sharing and collaboration when every moment counts.

To meet these evolving threats, the Federal Government must incentivize genuine cooperation so that communications networks can focus on anticipating the next attack, not just responding to the last one.

This needed foresight and agility, and it does not come from imposing outdated checklists and top-down regulations. It arises from a strong partnership between the private sector and the government, working together to detect and deter attacks in real time.

I am proud of this Committee's progress toward strengthening network security, but much work remains. Our efforts show that success is possible. With full funding now secured, the Rip and Replace program is removing the remaining Huawei and ZTE equipment from our networks.

GPS offers another example. When threats to our positioning and timing capabilities were identified, we acted decisively by passing the National Timing Resilience and Security Act to establish backup systems. Now, alternative and complementary positioning, navigation, and timing systems are in development, with NTIA recently identifying at least 50 companies attempting to increase our resilience and complement this critical system.

Today's hearing is an opportunity to assess the current threat landscape, identify where our defenses fall short, and explore how the Federal Government and the private sector together can better protect America's communications infrastructure from both foreign and domestic threats. I look forward to a productive exchange.

Senator FISCHER. Thank you, Senator Cruz. We will now begin our questions for the panel, and I will start. We will do a five-minute round, please.

Mr. Jaffer, as you testified, the Salt Typhoon hacks proved that China obtained widescale access to our telecommunications network, and based on the publicly available information, what distinguishes Salt Typhoon from prior nation state operations targeting U.S. telecom networks?

Mr. JAFFER. Thank you, Chairman Fischer. I think the most distinctive thing about Salt Typhoon is the breadth and the depth of the access the Chinese government obtained to America's telecommunications infrastructure. Now again, only based on what we know publicly, it is clear that they were able to go after nine telecommunications providers. It appears that they actually obtained access to either our law enforcement or potentially our foreign intelligence surveillance systems at some level. Whether it was the collection or the task targets, we do not know the details.

But if you think about what that means, that depth of access, and that sustained access to that sensitive information is massively damaging not just to our communications capabilities, but to our national security. And so this is the real challenge, is the depth and breadth of the access they obtained.

Senator FISCHER. How difficult is it to be able to detect that, and what does that tell us about the current existing capabilities that we have to monitor?

Mr. JAFFER. Well, we obviously were able to eventually find them, but it took us too long. We now have assessed that they were in those systems, or were targeting those systems, since at least 2021, or at least going after them. And we do not know when they got in.

The other real problem is that once they got in, they burrowed so deep we are not sure whether we can or have gotten them all out completely. They may still very well be in our systems. At least one provider suggested they have successfully removed the actors they know about. The question is, how deep are those actors in our systems and how sustained is their access.

So we were not able to detect them when they came in. Could we have? Possible. Certainly we had plenty of warning that they were coming after our systems. And this is what is crazy to me. The government actually now has admitted that it identified them in different systems. It did not realize they were the Salt Typhoon hackers. But now having connected them to these hackers, they now realize they actually saw them.

Senator FISCHER. Is it easier now to be able to detect from lessons learned?

Mr. JAFFER. Well, look. Certainly every day that goes by we learn more about the adversary. We learn more about our capabilities. We develop new capabilities. The advent of AI, while it provided significant benefit to the offense, also provides a significant benefit to the defenders, as well. We should be deploying that at scale.

The real challenge today, though, remains that we remain in the situation sort of blaming via victim. In this case we are saying, look, if the telecom companies, they did not do their part, they did not update their systems—and there may be serious problems there and things that need to be addressed—but beyond that, the question is what did the government know about the attacks, why did it identify the attackers as different systems, and not take action to find them everywhere else they were, having found them once? And why didn't they share that information effectively with the private sector rapidly? I mean, this is like the CIA identifying Khalid Almidhar and Nawaf Alhazmi in Kuala Lumpur and not telling the FBI that they had visas to come to California, to come to the United States.

Senator FISCHER. You know, I mentioned the FACT Act, the bill that I passed here in the Senate. How concerned should we be about China in our hardware, in core networks? Briefly.

Mr. JAFFER. Well, there is no question that we need to go after the Chinese in this space. They are absolutely targeting those core networks. They have spent a lot of time trying to get into our hardware and infiltrate our supply chains. I think the FACT Act is a great piece of legislation. We need to get it enacted as soon as possible. But we need to go even further. We really have got to get aggressive about identifying the fact that China has infiltrated our infrastructure not just through hardware itself but through the chips, as well. China has a huge supply of large-format chips. They are trying to get advanced chips, as well. They are on the path to it. They are not going to get EUV for a while, but they are going to use advanced EUV, and that is a problem.

Senator FISCHER. You know, Mr. Mayer, as we are looking here in Congress to be able to remove a lot of that risky telecom gear from our networks currently, what policies do you think we need to prioritize with regard to supporting manufacturing of our domestic or our trusted ally equipment here, so we do not run into a lot of the situations that Mr. Jaffer was referring to?

Mr. MAYER. So to set the stage for responding, the equipment in the telecom ecosystem is massive. It spans many continents, overly concentrated, frankly, in an area of the world which we know is subject to disruption. The Chinese have expressed their interest in terms of what they want to accomplish in that region, and there are a lot of countries that are now moving their supply chain to countries in that region also.

So I think from a policy perspective, we have to understand that there is significant technology embedded in our systems, and I think what Congress did with Rip and Replace was admirable, because it recognized two vendors who we knew were responsible for malicious surveillance and presented a risk to our military establishments in some areas, but more importantly, an overall risk to our ability to manage and control network security.

Senator FISCHER. I am out of time so briefly, can you do like a one, two, three, what we need to do with our manufacturing on this?

Mr. MAYER. Right. I think we have to tighten the requirements on vendors to improve cybersecurity. I think the concept of security dies by design. It is critical. We have to build it in, not bolt it on afterwards.

Senator FISCHER. OK.

Mr. MAYER. And I think we need to have a very close relationship with our government intelligence community about what they discover, what is suspicious, and they have to share that with us so we can probe and help them resolve some of the insecurities in that realm.

Senator FISCHER. Thank you very much. Thank you. Senator Luján, you are recognized.

Senator LUJÁN. Thank you, Chair Fischer. Ms. Jordan, you were at the FCC as Chief of the Public Safety and Homeland Security Bureau when the FCC adopted the declaratory ruling that affirmatively required telecommunication carriers to secure their networks from unlawful access and interception of communication. The FCC also proposed rules to require covered communication service providers to submit an annual certification attesting that they created updated and implemented cybersecurity supply chain risk management plans, things of that nature.

Can you explain briefly why the FCC moved forward with the declaratory ruling and advanced additional proposals earlier this year?

Ms. JORDAN. As I mentioned earlier, part of what Salt Typhoon did was gain access into our law enforcement requests and records, giving China access to our administrative proceedings against adversaries. And so as I mentioned, Section 105 of CALEA, with its systems security and integrity, requires that they secure the systems from unauthorized access. So it was basically reemphasizing that.

With regard to the Cyber Risk Management Framework, that was developed by NIST, I think it is being referred to as a checklist, and I kind of take exception to that. It is a risk management plan. Yes, there are a number of steps that you go through. Do you have governance? Are you changing and not using default passwords? Are you assessing your risk against a number of things like installing patches in a timely manner? You know, the FCC just recently released another warning to the EAS, the alerting systems, that they need to patch their systems because again they have been hacked.

And so that proposal that was pulled back to implement the Cybersecurity Framework is already in place, voted unanimously in the past several years, for portions of the communications sector. In fact, in August it was proposed for subsea cable licensees to be required to do similar cyber risk management planning.

So again, it is not a checklist. It is do your cybersecurity in a methodical, planned way, and keep track of what you are doing so that you know internally, your leadership knows, and you can share it when asked, whether Congress or the FCC were to ask.

Senator LUJÁN. Ms. Jordan, with that being said, a couple of weeks ago the proposals were off the table after the Trump FCC voted along party lines to rescind these rulings. Has the FCC proposed any rules in the place of what it just rescinded to ensure that our networks are safe and secure against cyber threats?

Ms. JORDAN. I have not seen anything. I have seen and heard, both in Robert's testimony as well as in the statements released by the FCC and the policies, that industry has committed or said that they will take extensive steps. But as I mentioned during my comments, there are no assurances. We do not know what those extensive steps are.

Communications networks are large, complex, and they require significant measures to be taken to secure them. So without some sort of accountability regime, we do not really know what they are doing, how effective it is, how widespread those measures will be.

So the answer is no, there is nothing that I am aware of that they have put in place.

Senator LUJÁN. Mr. Mayer, Mr. Jaffer, you have both stressed the importance of American leadership in emerging technologies such as AI and quantum in your opening statements. In this Committee, in this year alone, we have had multiple hearings on AI, and we often hear that we are in a race against the Chinese government.

The question for both of you, yes or no—and if you want to editorialize I would invite you submit that into writing—yes or no, please. Is it possible to win a race against the Chinese government if America is constantly leaking our IP to them through hacks in our telecom networks? Mr. Mayer?

Mr. MAYER. Is it possible to beat the Chinese in the AI race if there are leaks in our infrastructure?

Senator LUJÁN. That is the question.

Mr. MAYER. Yes. So the answer is that——

Senator LUJÁN. Yes or no, sir. You can editorialize all you want, volumes and volumes, in writing.

Mr. MAYER. Yes, I do not think it lends itself to a yes or no.

Senator LUJÁN. I appreciate that. Mr. Jaffer?

Mr. JAFFER. No.

Senator LUJÁN. I appreciate that. The correct answer is no. If the Chinese government is able to get their hands on everything we are doing in the United States with IP, then what are we doing? We should just have open protocol everywhere and let them do whatever the hell they want. How can we ensure equally strong cybersecurity standards across our networks without proper Federal regulations? Is it possible, yes or no, Mr. Mayer?

Mr. MAYER. We can do it without Federal regulation. The regulation is a prescriptive, bureaucratic, static approach to a problem. It does not solve the environment we are in today.

Senator LUJÁN. So you are suggesting it can be done voluntarily?

Mr. MAYER. I am suggesting that there is a shared responsibility across all aspects of the digital ecosystem.

Senator LUJÁN. So if I heard you correctly earlier, you said that there should be tightening on the vendors. So there should be regulation on vendors?

Mr. MAYER. There should be expectations put on vendors to——

Senator LUJÁN. Should there be expectations put onto telecommunications companies?

Mr. MAYER. There are expectations put on telecommunications companies.

Senator LUJÁN. I appreciate. Mr. Jaffer?

Mr. JAFFER. I think you can do it without Federal regulation, but I think the better way to do it is with a partnership between the public and private sector. If we incentivize the kind of behavior we want from our industry, we are more likely to get it. Let me give you just one example why. The more regulations we put on our providers, the more you are saying put the lawyers in the room and have the lawyers decide what happens. And you know what lawyers do? I am a lawyer, a recovering lawyer. We tell our clients to do the minimum necessary, at the latest time possible, do only what you are required to do.

If, on the other hand, you incentivize people to do the right thing, you give them tax benefits, access to government programs, and the like, they are more likely to line up, your boards, your CEOs. Everyone is going to be in the same room because they are going to say, kook, we get a benefit by doing these things. Give me liability protection. Give me regulatory protection. Now I am going to tell my CFO, go share all the information you can. Now everyone is lined up in the same direction. To me that is a more effective way to get to the goal you want, which is exactly right. We cannot win the AI race if we are leaking stuff out to China. The question is how do we get there. do we regulate it in place or do we incentivize it?

Senator LUJÁN. Thank you, Mr. Jaffer. My time has expired. If we have another round of questioning I would like to come back. Thank you.

Senator FISCHER. Thank you, Senator Luján. Senator Blackburn, you are recognized.

STATEMENT OF HON. MARSHA BLACKBURN, U.S. SENATOR FROM TENNESSEE

Senator BLACKBURN. Thank you, Madam Chairman, and thank you all for being here.

I want to return to the subsea cable issue, which I think is so vitally important. And I had introduced the Undersea Cable Protection Act because of concerns over what was being done that would really preserve and make certain that we had these cables. Of course, attacks on these—tampering, cutting—is something that is there.

Mr. Jaffer, let me come to you because I want you to talk for a minute about the vulnerability of the landing stations and the cable routes to foreign adversaries and foreign attacks, and why we should prioritize these protections?

Mr. JAFFER. Well, Senator Blackburn, as you know, 90 percent of the world's Internet traffic travels over these cables, 99 percent of transoceanic communication goes over these cables. And so you are right. It is not just the cables themselves that are vulnerable. It is the landing stations, as well.

Talk about the cables first. You have got cable cuts that have happened, and we see them in Taiwan, we see them in the Baltics. The Chinese have been dragging their anchors intentionally. We think it is intentional, certainly maybe by accident. These things can happen at times. We have known for a decade the Russians have been targeting our cables for surveillance, and they are almost certainly if they are able to get devices on the cables to tap them, they can certainly disrupt them, as well. So it is a huge problem when you are talking about the quantity of communications that are there.

The other problem is once the cables are cut, getting capability out there to restore them is limited significantly, and that is why legislation like yours is so important. But we rely on Chinese companies to do a lot of the cable fixes, particularly in the Pacific. That is a huge problem. If these cable are cut, we are essentially blind. We have got a lot of capabilities with satellite, as well, but, of course, the Chinese are targeting our satellites, as well. It is a huge problem.

Senator BLACKBURN. Yes. Let me jump in there, on the satellite. And is it Mr. Gizinski—I want to be sure I am saying it right—talk for a little bit about that. Because our primary delivery system is the subsea cables, and then you look at what we can do with the satellite capacity, and I think that what we have, satellites would offer about 50 terabytes. You know, we understand how indispensable this subsea infrastructure is.

So talk with me about how we should look at the complementary role of the subsea cables and then also the satellite system?

Mr. GIZINSKI. Senator, thanks for the question. I think a couple of key points. Certainly the capacity for satellite communications is lower than that of subsea cables, but they do provide today both core critical infrastructure on an ongoing basis as well as key disaster failover capabilities.

One of the core areas of focus, though, is the same risks that are present to those subsea cables are also present to satellites. They are vulnerable to both physical, electromagnetic, and cyberattacks. It is a core area of focus, something that we have looked at closely. In many cases, those deployed and operational satellite systems are either owned and operated underneath a foreign flag or they have a number of foreign supply components into them. That same level of attention and focus that is paid to other aspects of the infrastructure is important to pay to that core aspect of failover infrastructure, as well.

Senator BLACKBURN. OK. Let me ask you this. Have you, by any chance, seen or are you aware of the Naval Capitation Project at the Port of Memphis? OK. It would be worth your time, because they are looking at the underwater and also the above, and it is a wonderful project there at the Port of Memphis.

Mr. Jaffer, I want to come back to you. SIM farms. I think that these SIM farms are powering the large robocall operations and the scams, and we are seeing a lot of these. There has been a lot of talk about that this week because of Black Friday and Cyber Monday. What are the weaknesses in our current authentication systems when it comes to isolating or actually pinpointing these SIM farms?

Mr. JAFFER. Yes. Well, as we have seen, we saw what happened. Chairman Cruz referred to it in his opening statement about the SIM farm that we saw up in New York during the U.N. hearings. You have talked about it, and the fraud that we have seen against our seniors and a lot of consumers. It is hugely problematic.

Obviously, we need to get better on this front. The question becomes how do you do it in a way that is effective and still deployable in our current infrastructure, and that is, I think, the hard part. You know, we have done a lot with eSIM, and I think eSIM is significantly more secure and has the ability to be leveraged to be more secure. So I think as we shift to more eSIMs that will make it more effective.

The adversary is always going to make a move. The offense is always going to have an edge. The best you can do as a defender is hope to keep up, and with the advent of modern technology, and AI in particular, people worry that the offense is going to get a lot better. But I believe, actually, it will allow our defense to get just as good and to keep up more effectively.

So I think applying those capabilities in the authentication domain is really important, not just, by the way, for SIMs, but for regular Internet authentication, as well, financial transactions, and the like. We have seen the pivot to passkeys from passwords. That is a significant move. I think that is going to be empowered by our new-found AI capabilities.

Senator BLACKBURN. Thank you. Thanks, Madam Chairman.

Senator FISCHER. Thank you, Senator Blackburn. Senator Rosen, you are recognized.

STATEMENT OF HON. JACKY ROSEN, U.S. SENATOR FROM NEVADA

Senator ROSEN. Thank you, Chair Fisher, Ranking Member Luján, for holding such an important hearing. It is really critically important because the security of our telecom industry is not only essential, I believe, for our national security but also for closing the digital divide, because connectivity must be secure and resilient, as we have all been talking about, for it to be successful. And I appreciate the discussion on Salt Typhoon. We need to be sure that we protect ourselves in every way possible, and building on our satellites and our undersea.

But I want to move on to something you just touched on, artificial intelligence and our threat environment. Because AI tools have made it easier than ever for threat actors to create realistic and sophisticated attacks to gain access to sensitive systems, to our valuable data. And even without the use of AI, we continue to see cyberattacks with increasing frequency.

In August, Nevada was hit with a devastating cyberattack, crippling its agencies while the state worked with CISA and the FBI to track down the cyber criminals and secure Nevada's data. Thankfully, the state made a full recovery. It appears that no sensitive data was taken.

But Ms. Jordan, I am going to start with you. In this environment with threats from cyberattacks growing every day, what is the risk of having a reactive Federal response rather than proactively encouraging, and in some cases requiring, certain levels of cybersecurity for our critical sectors?

Ms. JORDAN. Thank you for the question. The risk is high, and the consequences are severe. We saw Salt Typhoon. There could be things that happened that are even worse than that, or Salt Typhoon could continue. They could be continuing to exfiltrate information.

Senator ROSEN. And so we have cut resources at CISA. We have disbanded Cyber Safety Review Board. So how is this impacting what we are able to do?

Ms. JORDAN. It is of great impact. I think to CISA, with them putting out guidelines, them putting out known exploited vulnerabilities, sharing the patches and the criticality, in other words, you should do this one really soon because it is a high vulnerability. This one maybe can wait a little longer. So without that information, that information sharing that my colleagues have been talking about is limited.

Senator ROSEN. CISA is that bridge between public and private, between our grid and all of that. It is important that we do not just get rid of CISA.

Ms. JORDAN. I think so, yes.

Senator ROSEN. And so, you know, people have talked about the incentives for current telecom companies to ensure their networks are secure, commonsense cyber hygiene, all the kinds of things that you spoke about, encryption, dual-factor authentication, passkeys. Ms. Jordan, again I am going to ask you. Are there any Federal programs that incentivize smart cyber practices, and what do you think about those? Quickly because I have another question to ask Mr. Mayer.

Ms. JORDAN. Yes. I am not aware of any that incentivize other than regulations that require. I think if there were incentives I would be in favor of them, alongside an accountability regime like regulation that looked at incentivization, as well.

Senator ROSEN. Thank you. Mr. Mayer, I am going to move on to you. In an AI-enabled threat environment what can Congress do to help secure our networks? For example, some have suggested additional funding to support carriers and ISPs, ensuring that they have adequate cybersecurity protections. Quickly—I have one more question for a former Nevadan, I believe, worked for Sierra Nevada Corporation—how do you think we can provide that support here in Congress?

Mr. MAYER. I think you have to encourage innovation, not regulation. We had an incident two weeks ago reported by Anthropic, that for the first time, using commercial, off-the-shelf AI platforms they were able to initiate a cyberattack. Eighty percent of that attack did not require human intervention. It was fully executed by an AI platform that is currently commercially available. Over time, that 80 percent is going to move toward 100 percent. That is the environment we are in.

There is no way that a prescriptive checklist regulation is going to allow us to innovate in the way we need to innovate to address that threat.

Senator ROSEN. So investing in public-private partnerships and innovation in our universities, our research institutions, and with our private companies would be, in your advice, reasonable.

Mr. MAYER. Reasonable, vastly superior, and should be encouraged by Congress.

Senator ROSEN. Thank you. I have one last question about U.S. leadership in the telecom industry. It is essential to securing our network. We have to be on that leading edge of innovation, maintaining our U.S. leadership in international settings standards. So Mr. Gizinski, you worked for defense companies like Sierra Nevada Corporation, which is proudly headquartered in Sparks, Nevada. Can you speak to the importance of ensuring we have secure and resilient communication networks, how important is it to national security and U.S. jobs if we do not have a strong cyber posture across critical infrastructure sectors like telecom?

Mr. GIZINSKI. Senator, thanks for the question. It is critically important that we have a secure cyber infrastructure. One of the core areas that I have looked at and thought about quite a bit in this is promoting that culture throughout the defense industrial base of leaning forward and adopting strong cyber practices. I think that is something that we have seen some adoption driving toward strong incentive programs, encouraging the innovation that is being harnessed today to deliver next-generation technical innovations. We are seeing in the satellite industry the launch of a number, thousands of new satellites a year. That same innovation should be harnessed and driven to secure our cyber posture, as well.

Senator ROSEN. Thank you very much.

Senator FISCHER. Thank you, Senator Rosen. Senator Schmitt, you are recognized.

STATEMENT OF HON. ERIC SCHMITT, U.S. SENATOR FROM MISSOURI

Senator SCHMITT. Thank you, Madam Chair. Just to follow up on that a little bit, Mr. Jaffer. In December I had called for an investigation of the Department of War handling of the post-Salt Typhoon risk, in particular, the Department's failure to ensure its communications, voice, text, video were protected from foreign espionage vulnerabilities. In your view, what are the structural problems in Federal procurement that make it possible—or I should say, what should Congress consider as far as the Federal procurement process to make that better?

Mr. JAFFER. Well, Senator, certainly I think that the procurement system is one place where Congress and the Executive Branch can do a lot more to ensure effective cybersecurity. In the procurement process, because you are spending our taxpayer dollars and people want these contracts, we can impose whatever requirements we want on them. To me that is a much more preferable way to address the regulatory burden that folks want to put on industry. It is because if you a government contract, they should secure the systems to the government's standards.

At the same time, we are seeing the Department of War today pivot to a much more innovative approach to procurement, a much more commercial approach to procurement. I think that is the right thing to do. It allows us to get newer, better technology in faster. There we have to make sure we are not over-imposing cybersecurity burdens that will prevent us from getting the technology we want. There is a balance there that we can achieve, I think one that we can do successfully as we need to, going forward.

Senator SCHMITT. I agree in the sense that we have a lot of leverage as it relates to those contracts. In your view, what are some of the minimum cybersecurity standards or audit compliance that should be included in those contracts?

Mr. JAFFER. What I do think we should do is require companies that sell to the Federal Government to go through a security audit and to demonstrate, to an independent third party, that they have successfully met things like the NIST Cybersecurity Framework, that they are applying it effectively and they are implementing it effectively. That, to me, is a good starting point. If they are able to show that to the government, the government does not need to do additional work on its own to qualify them. They can do that ahead of time. They can get the audit paperwork, present it to the government, and then become a contractor much faster. To me, that is the way to get smaller, faster companies in and not put an additional Federal regulatory burden upon them while still requiring them to meet good cyber hygiene requirements like the NIST framework.

Senator SCHMITT. Mr. Mayer, I wanted to ask you, in your testimony you emphasized that prescriptive regulations cause us to lag behind adversaries, for a bunch of different reasons. You warned that this shift in attention from managing real risk to managing paperwork means a provider can legally and fully be compliant but still be very exposed.

Can you speak to the impact that we have seen already from the previous administration's more prescriptive checklist-driven approach what that has kind of left behind and what we can learn from that, moving forward?

Mr. MAYER. So we know that the checklist, and we have evidence of this, have not been successful. There are examples where individuals or organizations that was managed by checklists, they missed things. And in this environment where the adversaries are evolving on a daily basis, using a checklist would, in a sense, be looking in a rearview mirror. We have heard talk about the flexibility in the NIST framework. That was designed to withstand the test of time. It worked over a decade.

So I think the better approach, and we are doing this, is to engage with our government partners, on a regular basis, including the intelligence community and the law enforcement community, and talk about what we are observing, what the government is observing, how to mitigate those activities. And we do hold ourselves accountable. I can tell you, the frontline practitioners in our companies work every day to defeat these attacks. We do not hear about their success rate, but they are dedicated and passionate about security, and they are held accountable within their organizations, to their customers.

And finally I would say in the context of contracts, that is a legitimate avenue for negotiations, to talk about the security requirements that are needed, and we have been doing that for years, through service-level agreements and other ways to reach an understanding of what is expected.

Senator SCHMITT. So with the 43 seconds I have remaining, I will just throw two questions out for whoever wants to grab onto them, because I do think these are important. What we learned, I think, from Salt Typhoon is that there are a lot of deficiencies in the hardware that currently exists, that is outdated, and I know there are efforts to sort of update that. Can you give me an update on where that stands? And why, as it relates to satellite security, what are just some simple things like enabling encryption, why are we not further along with that?

So hardware issues and updating that and then encryption for satellites.

Mr. GIZINSKI. So I think a couple of aspects, certainly on the hardware side, major area of emphasis and ultimately very important to pay attention to the supply chain of not just the hardware but the software that is going into those systems, putting together transparent messaging around the source of all of the software aspects that are incorporated in deliverable systems.

There are a number of explanations that have been provided for some of the complexities that are created by enabling encryption. I would say it is a little bit of a surprise, and I think there is probably further discussion needed, on some of the limitations that are preventing encryption from being broadly used on satellites. It is something that we have strongly advocated for. We have made those tools available to many of our customers that are using that equipment over satellite links. And we are still seeing, to this day, that equipment not being enabled, that feature not being turned on, and those links being left out in the clear.

We do think a part of the driver for that, the shift toward the concept of zero trust architecture, where each system and subsystem is assumed to be untrusted, has not been fully adopted across the satellite industry, more broadly. Certainly it appears to be potentially a misunderstanding of who is responsible for that layer of security in the overall system.

Senator SCHMITT. Thank you. Thank you, Madam Chair.

Senator FISCHER. Thank you, Senator Schmitt. Senator Hickenlooper, you are recognized.

STATEMENT OF HON. JOHN HICKENLOOPER, U.S. SENATOR FROM COLORADO

Senator HICKENLOOPER. Thank you, Madam Chair, and I thank all of you for being here. I appreciate all the work you are doing. As a broad context, when I was finishing my first term as Governor of Colorado, we did an economic development trip around Asia, and it ended up in Israel. So we just saw a lot of the technologies you all are familiar with. We also saw Israel's ability to connect military with their academic research and their universities, with their entrepreneurs. And we have a National Center for Cybersecurity in Colorado Springs that tried to pick up on that. But I think that is an art, just as we discuss these issues.

And just to continue what Senator Schmitt was asking, and maybe I will turn to Ms. Jordan on this, Colorado's critical infrastructure from energy facilities to military installations, top to bottom, depends on secure communication links. And we know that adversaries are constantly trying to interrupt and disrupt our communications, penetrate our national security in every way they can.

In your view, what are the largest gaps in Federal-State information sharing on security as threats to our communications?

Ms. JORDAN. So I think that information sharing, in general, is important, both among industry and the government, and it should include state and local, for instance, state fusion centers, along with the Federal intelligence communities. And where that is not happening, that is a big gap.

I think that understanding what the threats are, implementing even the most basic cybersecurity hygiene, updating the patches to software, and those kinds of things, are critical.

Senator HICKENLOOPER. Right. So those are the easy parts. So we turn the page and we look at, as quantum advances, certainly the encryption systems protecting our communications networks eventually are going to become vulnerable to rapid—can you say decryption? Is that fair? Is that the right word? And this is a future threat window that is immense by most measure.

Now, NIST recently published the world's first Postquantum Cryptography Standards that can be adopted by the U.S. Government, which you were just describing is a pretty basic blocking and tackling. We need to go to that next level. So given your experience with the Public Safety and Homeland Security Bureau, how should the FCC begin incorporating quantum-resisting cryptography and post-quantum transition planning into its network security roles?

Ms. JORDAN. It is definitely an advanced area that needs to be looked it. I agree with my colleagues on collaboration. I think that having those joint discussions with industry on how that is being rolled out, the pace at which it is being rolled out, and then looking smartly at what needs regulation, where there should be secure by design, in other words, things that are built into products before they are deployed, and then where is there a need, for instance.

The FCC hosts something called the Communities Security Reliability Interoperability Council, CSRIC. It is a partnership, and they come up with beset practices. So that is like ripe for a CISREC committee. But then when those best practices are put out, they have to be used.

Senator HICKENLOOPER. Right. Well, that is the next big step. I agree.

Mr. Mayer, as you know, again, Colorado is home to many entrepreneurs and research labs up and down the Front Range, and definitely on the front lines of 5G and next-gen wireless communications. But we have been working in a bipartisan fashion to finally close the shortage of funding for the SEC's Rip and Replace, where we found that we had a lot of infrastructure that was not as secure as we would like. The Salt Typhoon showed how deeply adversaries can burrow into our communications networks.

How can Colorado's rural broadband providers, which operate on thin, very thin, margins, benefit from additional Federal guardrails or minimum cybersecurity baselines to make sure we do not have similar breaches?

Mr. MAYER. Well, I think, sir, that the notion of doing basic hygiene is very important, and my experience is that the companies understand that and they are basically implementing that. The challenge for the rural providers is not having the resources that the larger providers have.

Senator HICKENLOOPER. Exactly.

Mr. MAYER. So what you are asking basically is a local telephone operation be able to compete against a nation state that is throwing everything everywhere, all the time, on these networks. They view those providers as access points to the entire ecosystem, and they exploit that. And we have seen that with Salt Typhoon, how that works.

So I think the other opportunity for us is there is $20 billion in non-deployed defunding. Cybersecurity would be an excellent way to invest that money, both in cybersecurity workforce development, training, and also the fact that there are legacy technologies. Rip and Replace was a great start. The list is getting bigger.

Senator HICKENLOOPER. Right. No, I agree. I am out of time. Mr. Gizinski, I have got a couple of questions for you that I will put into written questions. But I appreciate all of you being here. Thank you for your service. I yield back the floor. Sorry.

Senator FISCHER. Thank you, Senator Hickenlooper. As a Senator you do not have to yield back time when you are finished.

Senator HICKENLOOPER. Really?

Senator FISCHER. "Thank you" works.

Senator HICKENLOOPER. Well, I was out of time, so thank you, Madam Chair.

Senator FISCHER. I am doing a rules thing now, too. Thank you. Senator Capito, welcome. You are recognized.

STATEMENT OF HON. SHELLEY MOORE CAPITO, U.S. SENATOR FROM WEST VIRGINIA

Senator CAPITO. Thank you. Thank you, Senator Fischer, and thank you all for holding this hearing. Nice to see you. I am all the way over here.

Mr. Mayer, you kind of got into what one of my questions was going to be, but let me begin with this. The BEAD program, the West Virginia application was just OKed by the NTIA several weeks ago, and if you followed it you probably know that the original $1.2 billion that was allotted for West Virginia, which was quite large for a small state, is now $600 million, to deliver the BEAD program in West Virginia, after it had been rebid and everything.

I guess, in my opinion, where do you think—and I think you already mentioned this, but if we could flush it out a little bit more—with those extra dollars that are allotted for broadband, it seems to me that cybersecurity and other areas—you mentioned workforce training—where would you see—I would like to keep those dollars captured for the deployment and the safety of broadband, particularly the rural broadband. So if you could expound on that a little bit more?

Mr. MAYER. I think we can do both. It is very important to use that money for broadband deployment, especially in the rural areas of the country. We need to make sure that these citizens are not left out of the revolution that is underway, AI and all of that.

I think there is a general understanding that the nature of the threat environment right now is different. It is becoming much more urgent, that we have resources available to support that community.

So I think what we are talking about is targeted funding, with full accountability, in areas that these companies can—and they know, you know, we need this system, or we can use this mechanism, or we need these professional supports—have them being able to access those funds for purposes of increasing their cybersecurity, protecting their customers, protecting their networks. That is how we view it.

Senator CAPITO. Well, I think for small systems, which we have in a small state like ours—some of them are small; some of them are major—they just do not have the money to be able to do that. So then you look at, well, what are you going to do? Are you going to not deploy service in a rural area? Because you are going to have to make a choice. And it would be nice since, in the case of West Virginia, $600 million is not going to be spent where it was initially intended to, would be, I think, a source of funds.

I would like to see some more of those funds still deployed, because there are still going to be people that are left out, even after the BEAD program. And those are very difficult areas. But it sounds like we are saying the same thing in terms of the affordability of a rural broadband deployment company to be able to do this. I mean, I think if you think of it in terms of 9/11, where did they get in? They got in in small airports where there were vulnerabilities. Same thing with cybersecurity, to take the whole system down.

Which brings me to another issue. There is a lot of talk about data centers and the deployment of data centers, and how critical they are in the race for AI, and critical for us to be able to take advantage of the great technologies that we have. But those are new vulnerabilities, I believe, that are going to be presented. I was thinking about undersea cables and other things. Is this something that you all—should we be designating data centers as critical infrastructure, so that it can be part of how CISA and others look at our critical infrastructure? I do not know if you have any thoughts on that.

Mr. MAYER. I will take that. I think, to a large extent, data center infrastructure is already reflected in some of the critical infrastructure, whether that is critical manufacturing, the IT sector, the communications sector. It is in there. It is something that we take very seriously, frankly, because we are seeing evidence now that the data centers are targets. And we also see, we saw this week, or two weeks ago, a situation where a cooling device in a data center resulted in a massive disruption, one cooling device affecting major e-commerce platforms and social media platforms across the globe.

So there is an element of systemic risk that is built into a highly complicated, distributed network ecosystem. And I think that understanding that we are talking about attacks that are everywhere, all the time, I like to talk about the fact that they are 22,300 feet in the sky, they are 4 miles underneath the surface of the sea, and everything in between. That is the attack vector. And for us, as network service providers, we are very concerned about the ability to infiltrate edge devices that do not have the appropriate security built in. They want to go to market quickly. They want to go with cheap prices. That is why the FCC action, for example, around clean cars, which would impose expectations on the retailers to not make those faulty edge devices available to the public. That is an important step going forward, recognizing that issue.

Senator CAPITO. Thank you. Thank you, Madam Chair.

Senator FISCHER. Thank you, Senator Capito, and thank you for bringing up the BEAD program, which you and I worked on in that infrastructure bill and the importance of that on making sure unserved areas are connected, and hopefully that funding that was provided to our states will remain there and be able to be used for things, not just connectivity but also the security that is needed.

Senator CAPITO. I think that would be a well-placed use of the funds, and it is so necessary, certainly in light of the testimony we have heard today. Thank you.

Senator FISCHER. Thank you very much. Senator Peters. Oh, I am sorry. Senator Cantwell has joined us, Ranking Member. Welcome, Senator Cantwell. Do you have opening comments you would like to make, or questions?

Senator CANTWELL. I will just make a few comments and then get to questions.

STATEMENT OF HON. MARIA CANTWELL, U.S. SENATOR FROM WASHINGTON

Senator CANTWELL. Thank you, Madam Chair. Thank you so much for holding this hearing, to you and to Ranking Member Luján.

I want to focus on Salt Typhoon. Obviously, the Chinese government's espionage operation deeply penetrated networks of at least nine U.S. telecom companies, including AT&T and Verizon. It has been described as the worst telecom hack in our Nation's history, and the Chinese government-sponsored hackers broke into our Nation's telecommunications backbone. They exploited the wiretapping system that our law enforcement agencies rely on under the Communications Assistance for Law Enforcement Act, known as CALEA.

These systems became an open door for Chinese intelligence. Salt Typhoon allowed the Chinese operation to track millions of Americans' locations in real time, record phone calls at will, and read our text messages. Their targets included then candidates President Trump and Vice President Vance, as well as senior government officials. And the hackers were also able to determine who the U.S. Government was wiretapping, including suspected Chinese spies, telling Beijing which of their operatives might be compromised.

So how did this happen? Senior national security officials said the breach occurred in large part because telecommunications companies failed to implement rudimentary cybersecurity measures. Investigators found legacy equipment not updated in years, router vulnerabilities with patches available for 7 years—7 years—that were never applied, and hackers acquiring credentials through weak passwords.

Security professionals across the industry were shocked because this kind of basic failure would not be acceptable in health care or banking or in technology firms. Yet here we are, the telecom system, and basically the most sensitive communications. AT&T and Verizon claimed they contained the attack, but government officials and cybersecurity experts remain deeply skeptical. The FBI said it cannot predict when we will have a "full eviction" of these bad actors, and even Chairman Carr acknowledging, when he was rolling back the rules that protected us, quote, "We are still being exploited," end quote.

Earlier this year, I wrote to the CEOs of AT&T and Verizon, demanding that they provide documentation of their remedies. Both companies refused—hardly a transparent effort. I believe that the American people deserve to know whether China is still inside our telecom networks. We deserve to know.

Perhaps the most telling response in the breach came from the FBI itself. In an unprecedented step, last December, the FBI and CISA urged all Americans to use encrypted messaging—basically apps like Signal—to protect their communications. Hmm, interesting. "Encryption is your friend," they said. Think about that. Our Federal law enforcement agencies are telling Americans, "You cannot trust the security of your own telephone networks." That is what they are saying, and "you should use encrypted communication".

So, Ms. Jordan, what level of requirements should we be putting on our wireless providers that make sure that we are getting the level of security that Americans deserve? And when we are handing them over such valuable resources like spectrum, and they are trying to constantly end-run important national security and DoD initiatives just to get their hands on the spectrum, what requirements should we be putting in place that really do make Americans more secure in their communications?

Ms. JORDAN. There must be structured cybersecurity requirements levied. I am not talking about a checklist, which has been referred to, but cyber risk management planning and executing those plans. That has to be put in place, and it should be a requirement. The FCC has already required it of certain subsections of the communications sector. In fact, in August, this Administration proposed it for subsea cable licensees.

So continuing along that path, the continued partnership of industry, the telecommunications industry, with government, the intelligence sector, CISA, others who know of the recent threats. And as you mentioned, doing basic cyber hygiene. You know, I would never let my iPhone go 7 years without a patch update, right? Ordering a pizza sometimes requires two-factor authentication. Why are our providers not implementing basic hygiene? They should be held accountable, and they should be doing a structured plan, and being held to a verification regime that would give you the information that you asked for and did not receive.

Senator CANTWELL. Well, what about the FCC, walking back requirements additionally? It is like they are supposed to be the overall entity that says, look, here is how you have these communications licenses to provide communication, yet if you are not going to do good hygiene, why should we keep your license?

Ms. JORDAN. Yes, I do not believe that a fallback of enforcement action is appropriate, because that is after the fact. So again, they should be leveraging this requirement to use the cybersecurity framework, or something similar, to do structured planning and execution of cyber risk management across the entire communications sector. They should not be doing it in little pieces like the E-ACAM or the subsea cable or this pocket. It should be done pervasively.

Senator CANTWELL. Well, the grid, NARUC, is a similar organization that does this for the grid itself. Do you think that that is what we need here, something like that, where, at least, there is a dynamic and input? I mean, me personally, I think this is—we know this is the information age. We know that this is what is going to happen. So, letting these guys off the hook when there is so much vulnerability for Americans that our FBI and law enforcement are telling us, "use encrypted networks," it has gotten to a point where we have got to do something to better help the public. Or basically you are just setting them up. You are just setting them up to say, "You are going to be a target."

Ms. JORDAN. I agree, and I think that there are some aspects of what China is doing that our Nation state, and therefore even the telecom providers, might not be able to stave them off. But if the providers are not doing basic hygiene across their networks consistently, then yes, they should be held accountable. I am not saying if a nation state comes in and does something that we could not predict. That is a different scenario. But they should be held accountable to doing the basic hygiene—patching, not default passwords, encryption, those kinds of things.

Senator CANTWELL. Well, I think that is the most shocking thing. And this Committee has had several hearings, and there was another big break, and that was exactly the same issue. There was a patch. It was available. You know, as we have looked at privacy laws and what you need to do if you are providing some sort of system, yes. Nothing against 20- or 21-year-old administrators, but you have got to have more hierarchy to your enforcement and capabilities on security than just hiring a bunch of very smart, talented people when you have consumers who are going to be vulnerable to these kinds of things.

So, we look forward to working with the Subcommittee, Madam Chair, and figuring out what we can do to better protect Americans. Thank you.

Senator FISCHER. Thank you, Senator Cantwell. Senator Peters, you are recognized.

STATEMENT OF HON. GARY PETERS, U.S. SENATOR FROM MICHIGAN

Senator PETERS. Thank you, Madam Chair and Ranking Member. Mr. Mayer, as Ranking Member of the Homeland Security and Governmental Affairs Committee, one of my biggest concerns and focuses has been on long-term extension of authorities that are contained in the Cybersecurity Information Sharing Act of 2015, which I know you are very familiar with. Over 80 companies now, and organizations, support legislation that I am working on with Senator Rounds, in a bipartisan way, entitled “Protecting America from Cybersecurity Threats Act”, which would basically extend those cybersecurity threat information sharing authorities for an additional 10 years. Like we all know, the last 10 years have been very successful. We need to continue to make sure that they are in place for long term, that industry and others can rely on it.

And I certainly appreciate how vocal USTelecom has been about the importance of extending this authority. Could you explain to this Committee how cyber threat information sharing is absolutely critical for defending telecommunications networks, and what more do you think the Trump administration should do to help us extend this essential authority? I am going to be hoping all my colleagues on this panel will support that. Give them reasons why it is important.

Mr. MAYER. It is critical. We are not going to be successful in addressing the threats that we currently face. It has been invaluable in terms of our ability to share information without concerns about liability, without concerns about punishment, enforcement.

We have an excellent relationship with our government partners—the intelligence community, CISA, all of these organizations. It is grounded on this Act. It is ability for us to have conversations about what we are seeing, what they are seeing, what we are doing to mitigate the risk. These conversations are happening constantly.

And I think it speaks to a broad consensus that this Act has worked for 10 years. it is lapsing in the end of January if we do not deal with it. I would say it is probably the number one issue for us in the short term, to in a sense get an improved cybersecurity writ large for this Nation.

Senator PETERS. So as you mentioned, it is riding along the CR, which would expire at the end of January. Tell us, riding along CRs is not the way to do it. Why do we need that 10-year extension?

Mr. MAYER. Well, because we do not want to do this every few years.

Senator PETERS. It is every few months right now.

Mr. MAYER. Or every few months. Yes, that is not good policy.

Senator PETERS. Right.

Mr. MAYER. So this is a cornerstone of our ability to collaborate with government.

Senator PETERS. Great. I am also extremely concerned, and we heard from my colleague, Ranking Member Cantwell, about the FCC's decision last month to roll back what are basically, I think, commonsense cybersecurity rules to safeguard America's data. These rules were announced, as you know, in the wake of Salt Typhoon, and I will not go into all of the challenges there. It has already been brought up before the Committee. But I think, without question, the rollback of these rules leaves Americans exposed and erodes our ability to prevent future attacks.

I think this is even more concerning when you look at that rollback as part of a broader trend that is being carried out by the Trump administration right now, where officials say—they talk a good game—they say cybersecurity is a priority. But at the same time they are basically gutting all of our cybersecurity institutions, from rolling back the FCC rule to ignoring their own guidelines regarding the handling of America's most sensitive personal information, as well as pushing out cybersecurity experts all across government, firing the people who know what needs to be done.

So my question for you, Mr. Mayer, is the FCC rule to require telecommunications providers to have a cybersecurity plan, and then stick to it, I think is pretty common sense and a step forward to ensuring cybersecurity. So my question is, why did USTelecom push the FCC to roll back these efforts in this case? And are you confident the vulnerabilities exposed of the Salt Typhoon will not occur again in the future? But why push to roll those back?

Mr. MAYER. Because they were ineffective. They would not have produced the results that we are looking for. We are not going to regulate our way out of this issue. We are going to have to innovate our way. We are going to have to match an adversary who is using the most sophisticated techniques possible.

It was not a checklist or a compliance thing that was bypassed. It was advanced defensive capabilities that are being deployed by our member companies that were bypassed. Why? Because the Chinese are masters at stealth. They use—when you talk about here the Salt Typhoon being identified in 2021, 2020—they used Asia's specific region as a testing ground for these types of techniques, these stealth techniques, on countries and organizations that were less hardened. And then they perfected it, they came to the United States, they came into our networks, they used stealth technology that is actually anti-forensic, in a sense. The breadcrumbs disappear. And once they are in the network, I mean, it does not take more—in some cases less than a minute to laterally move throughout the networks, operating support systems, business support systems.

So we have a very sophisticated adversary, and the way to deal with this is collaboration with government, partnership with government, accountability, absolutely. And I am in the conversations. I know how much we are talking to these different government entities, classified settings, unclassified settings, numerous venues. We are making progress, and we should not stifle that or kill that with a compliance regime where you have 40 to 70 percent of your practitioners doing paperwork.

We need to focus on the threat. We need to focus on the triage when it happens. And we are supportive of things like incident reporting that Congress passed in CIRCIA, if it implemented correctly.

Senator PETERS. Great. Thank you. My time has expired. But Ms. Jordan, I am going to ask you a question related to this, as to why you may think the FCC's actions were appropriate, and why it may have been wrong to have those rolled back? But I will ask that in writing.

Thank you, Madam Chair.

Senator FISCHER. Thank you, Senator Peters. Senator Young, you are recognized.

STATEMENT OF HON. TODD YOUNG, U.S. SENATOR FROM INDIANA

Senator YOUNG. Well, thank you, Madam Chair, for your interest in this topic, and I want to thank all of our panelists here today. Thank you for your thoughtful contribution as it relates to policymaking on this host of issues.

You mentioned in your testimony, Mr. Jaffer, that China is increasingly engaged in undersea cable cutting activities. This is something that, for a couple of years running, I have had a real interest in, and as a member of the Intelligence Committee I am trying to find countermeasures that might help us address this growing challenge.

Subsea cables, we know, serve as the backbone to today's world communication system, so we are going to have to come up with some checks. And I believe we must adequately address these broader challenges in coming months and years.

Earlier this year, relatedly, the FCC put forward rules to streamline submarine cable application reviews, protect submarine cables against national security risks, and incentivize cable buildout. In those rules, one requirement was for applicants and licensees to create cybersecurity and physical security risk management plans.

Can you identify maybe other areas that should be a focus for strengthening our resiliency of subsea cable infrastructure, especially as our adversaries continue to advance tactics to do harm?

Mr. JAFFER. Well, Senator Young, it is a great and important question. I think the most effective way that we can prevent our adversaries from cutting cables and the like is to create more cables, to have diversity of them, to have them owned by American companies, have more ships to be able to fix them, and frankly, make clear to our adversaries that if they cut our cables, we will treat it as an attack on our critical infrastructure, because that is exactly what it is.

Today, adversaries largely get away with it because it is an accident, it was a mistake, we did not know it was you. But we watched the Russians surveil our cables. We watched them look at them and consider cutting. We have seen the Chinese actually do it in Taiwan and in the Baltics. One might be an accident. Certainly three in a row is a pattern.

And so when our adversaries realize that we are actually watching them and are going to do something about it, that is when they will stop doing it, and if we build enough cables and enough access that we can rely on our own system. Then there are other things you can do. You can do physical security. You can put them in more robust casings and the like. You can have surveillance measures down on this undersea floor.

But at the end of the day, if you are really going to push back against a nation state action, it is going to have to be nation state response.

Senator YOUNG. And we are going to have to come up with protocols, it sounds like you are saying, or expectations that we will treat this almost in domestic law like a strict liability situation, or if not strict liability, the burden of proof or production will be on whomever supposedly accidentally cut a cable, right?

Mr. JAFFER. That is exactly right.

Senator YOUNG. OK. Mr. Mayer, same question to you. Are there other areas that should be a focus for strengthening our resiliency as it relates to subsea cables?

Mr. MAYER. Yes, I think so. We have to make sure, and we are doing this, we are an important stakeholder in the submarine cable. The transmissions are often transmissions that we are generating and moving along, both nationally and internationally, especially internationally.

So we are aware of what the FCC is doing. We have had conversations with the FCC National Security Council about cybersecurity practices related to protecting, well, all practices—it is physical, as well—to how we can support enhancing making these systems less vulnerable. But there is an inherent risk when there are so many—I think there are almost 500 to 700 submarine cables. Many of these are in the Indo-Pacific region. This is China's area. The ability for them to disrupt transoceanic communications at a time when suits their needs is real and serious. And to Mr. Jaffer's point, this really requires Federal engagement and activities. And we are willing and ready to collaborate with any government partner and organizations to make sure that these systems are more secure.

Senator YOUNG. Well, who should bear the cost of, let's say, redundancy, right, building out more cables? These are expensive capital investments. Would it be rational, from an economic standpoint, for us to say, OK, we have an idea who are the greatest users of these cables are, because they send data across them, across the ocean. Maybe we should put it on the companies. What would you say to that line of economic argument?

Mr. MAYER. Well, I think the economic argument would be you cannot impose costs that are going to make the business unprofitable and not attract investors. As you point out, you need big investment, huge investment to deploy, to maintain, to install these. The economic problem with dealing with asymmetrical issues like this is serious. And I think that this is a question for national policy in terms of what kind of assistance can we do to safeguard our infrastructure against what we are experiencing today and what we know is possible tomorrow.

Senator YOUNG. Well, I think coming up with a doctrine of deterrence——

Mr. MAYER. Absolutely.

Senator YOUNG.—just to be candid, will be as a matter of politics, internal congressional politics and with a broader public of telecom consumers, that will be an easier sell. So maybe we should focus, in the near term, on what is achievable, and it seems to me a deterrence approach is eminently achievable.

So thank you all. Chairman.

Senator FISCHER. Thank you, Senator Young. As I put out a last call for any members who are trying to get to this hearing to ask questions, Senator Luján and I are each going to ask a final question.

Mr. Gizinski, you stated that many of the satellites providing coverage to the United States expose network traffic outside of our borders. So how do we meaningfully improve encryption and security protocols across our satellite infrastructure, an inconsistency that you highlighted?

Mr. GIZINSKI. It is an excellent question. I think a few key points that are critical, the first is we seek consistently, and I think this is a true point across both telecom and the satellite industry, most of the operators are not vertically integrated, so they are heavily reliant on a supply chain to build those subsystems that go in, things that enable those encryption capabilities. It is important that we extend the threat-sharing information and the opportunity down into the supply chain and ensure that we are building the right secure-by-design subsystems, with flexible encryption protocols and other appropriate security considerations from the ground up.

We have seen, very publicly, some of the examples where that has gone poorly, where foreign-supplied components had security vulnerabilities present in them, from the initial delivery. Encouraging that same approach throughout the satellite industry I think is incredibly important.

The second point is recognizing that in most cases folks that are designing and building these systems have the best view of what the vulnerabilities are and may be. They can be a great partner in closing those. We have seen consistently the application of well-intended checklists on defense systems often are not designed with the end system architecture in mind. Having that in-depth, open conversation has been incredibly valuable in securing other systems that we have built and delivered over the years. I think that is a great model to following out into the future.

Senator FISCHER. Thank you. Mr. Jaffer, how severe do you think the threat is to our space systems that we have?

Mr. JAFFER. I mean, I think the threat is quite severe. You just look at a capability that China has. They have the SJ–21 satellite. This is a repair satellite. It is designed to remove debris, the demonstrated ability to grab another satellite and move it to a different orbit. Now, you think about what that could do if used in an offensive manner. That is obviously a huge problem. China has that capability. Other nations have that capability.

The threat to our infrastructure is huge, and they do not even have to take out a satellite directly. They can destroy one satellite and the debris itself, the debris field, can cause problems for our satellites. It is a huge issue in outer space, it is a real challenge, and we have got to make our satellites defensible.

And part of it is having a diversity of systems. Like we talked about the cables. If you can have more satellites going up faster, that is essentially going to create a more resilient and more capable system. It is also going to make it more technologically efficient, because it will get newer capabilities into space faster. So the better we can get at launch, the better we can get at building smaller and faster and more capable satellites, the better off we will be.

Senator FISCHER. Thank you. Senator Luján.

Senator LUJÁN. Thank you, Madam Chair. Mr. Mayer, in your testimony you said that any cybersecurity framework needs to be flexible and adaptive. I agree. Do you agree with me that the FCC has a role to play in ensuring that our communication networks are protected against cybersecurity threats?

Mr. MAYER. Absolutely, yes.

Senator LUJÁN. I appreciate that. Now, recently Senator Peters asked a question around USTelecom, their role, their advocacy to reverse the FCC's actions in response to Salt Typhoon. A few things that the FCC required was changing default passwords, requiring minimum password strength, adopting multifactor authentication, and patching known vulnerabilities, all simple things.

Congress is constantly told that we are behind the curve on technology, even if we have these basic protections in place. Which of these basic protections was too burdensome for your member organizations?

Mr. MAYER. Senator, I think what you are describing are not burdensome.

Senator LUJÁN. I appreciate that. That is an answer. I appreciate that. With that being said, do your member companies have cybersecurity risk management plans?

Mr. MAYER. Absolutely. They have been working on this for many, many years. They are evolving their risk management plans.

Senator LUJÁN. Are you willing to share those with the Committee?

Mr. MAYER. The risk management plans?

Senator LUJÁN. Yes.

Mr. MAYER. No. We are in a trade association. I cannot say what our members are willing to share.

Senator LUJÁN. So you are telling me to trust you.

Mr. MAYER. I am telling you that we are doing a lot, and we have been doing a lot, and you can ask our government partners whether they think we are doing a lot, because I do believe——

Senator LUJÁN. I have a follow up there, as well. But I appreciate it. The reason I am asking you these questions, sir, is you, of all the panelists today, my constituents depend on your members every day, all day, around the clock, all day long. As a matter of fact, most of my small businesses right now just rely on the services that your member companies provide. So I am picking on you, and I apologize for that. But it matters to my constituents.

Now, earlier there was a question asked by Senator Schmitt about requirements for contracts for the Federal Government to be wise around taxpayer dollars. And I heard at least two of the panelists suggest, well, that might be a good idea to require anyone doing work with the Federal Government to meet, is it fair to say, a floor of standards, a floor of requirements, in order to safeguard taxpayer dollars? Would that be fair? Well, that is my assumption. If I am incorrect I would invite you to submit into the record where I got that wrong.

Now, I asked my staff to let me know how much money the Federal Government, over the last few Fiscal Years, has spent in a very specific area, namely in telecommunication contracts. They told me that what GAO says is from 2014 to 2018, the government spent $30 billion—$30 billion—for telecommunication contracts, $4 billion for call center contracts, $6 billion per year that has likely gone up, $14.3 billion for IT services for Fiscal Year 2024 alone, $3.2 billion in IT and telecom products for Fiscal Year 2024.

I look forward to working with you all to have requirements. I just look forward to working with you all, that there is a floor of cyber requirements. That is a lot of money. And we talk about national security vulnerabilities and how we outsource all of our work to call centers. The smallest of the small in the most rural part of America that allows someone in, an actor in, infects the whole system.

And so I certainly hope that these are some areas that we can get together.

The last question I have, Madam Chair, is to Mr. Jaffer. You served on the Cyber Safety Review Board, CSRB, which was under the Department of Homeland Security. My question is a simple one. Was it a mistake to disband this Board?

Mr. JAFFER. Well, you know, we were asked to look at the Salt Typhoon hack, and because of internal government bureaucracy decisions we were unable to even get off the ground. We were not able to get our clearances in time. We were not able to do any questioning of any of the communications companies, of any of the government officials involved. So we were tasked with the Cyber Safety Review Board review months in advance. We took months, we did not get anything done, and then the Board was disbanded.

Should it have been disbanded? No. Should it be back? Absolutely. But even when it was in place, under the 4 or 5 months I served on that Board, we got nothing effectively done because it was not allowed to do its work. There were claims because there was a law enforcement investigation going on, because industry was partnering with the government they could not talk to us. We even asked to talk to providers that said they were not affected by Salt Typhoon. We were not allowed to do that. So the Board was not being used effectively. It should not have been disbanded. It would be better if it was back in. But if it is going to back in place it needs to be effective.

At the end of the day, I think what Congress ought to think about doing is empaneling an outside commission to look at what happened in Salt Typhoon and Volt Typhoon and make recommendations to you, like the 9/11 Commission did, about what we should do most effectively to get the Executive Branch and legislative branch and industry back together and working on this issue.

Senator LUJÁN. I am glad I asked that question. So if, in fact, that body is brought back, it needs to be fixed and it needs to be effective, and the tools need to be in place to be able to discover all the information, to be able to provide information to Congress. In addition to that, your recommendation is now of an outside commission, as well. I appreciate that. Thank you. Thank you, Madam Chair.

Senator FISCHER. Thank you, Senator Luján. I would say the problem with any commissions is by the time we get the report it is like past due. It is past due, and it is really, really difficult to be able to get any movement forward from the recommendations that are put into place. So I look forward to working with you, Senator Luján, and trying to figure out, as anything with the Federal Government, how do we cut through things and try and move quicker so that we can have private industry be able to work with the Federal Government to get us the information we need.

Mr. JAFFER. One thought, Madam Chairwoman, you know, the other committees, the Senate Intelligence Committee, for example, has a technical advisory group that it empanels, that brings industry and government together. It is something that the Commerce Committee could consider doing, and bring a panel together, and then you could do it on your own time schedules. You do not need to worry about getting it authorized by law and all that sort of stuff, and we could just advise the Committee itself.

Senator FISCHER. And a lot of the issues we have are jurisdictional, as well, you know, whether it is with Intel, whether it is with Armed Services Committee intersecting with Commerce Committee. And the time it takes is very, very frustrating.

Thank you, Senator Luján. Good hearing. Thank you to our panel today for the good information that you have provided to this Committee. With that we are adjourned.

[Whereupon, at 11:46 a.m., the hearing was adjourned.]

A P P E N D I X

Response to Written Questions Submitted by Hon. Ted Cruz to Robert Mayer

Question 1. The Federal Communications Commission (FCC) does not run cyber operations, nor does it investigate intrusions. It is a communications regulator, without direct insight into national security threats. Agencies like the Cybersecurity and Infrastructure Security Agency, the National Security Agency, and the Federal Bureau of Investigation handle cybersecurity every day. They track nation-state activity, run threat hunting teams, and respond to intrusions in real-time. Given the clear delineation in authorities and expertise, should the FCC be writing cybersecurity rules for the telecom sector when it lacks that operational understanding or legal authority to do so?

Answer. Federal agencies should closely adhere to the statutory boundaries on cybersecurity policymaking established by Congress. The FCC is no exception.

While the FCC has a role to play in protecting America's networks against foreign adversaries by ensuring equipment is properly authorized—a role defined by Congress in the Secure Networks Act, other Federal agencies in law enforcement, the intelligence community, and industry are the primary drivers of cybersecurity, vulnerability management, and critical-infrastructure protection. Introducing another layer of oversight that Congress never intended is duplicative and unhelpful. Fragmented oversight splinters accountability, complicates incident response, and forces operators to satisfy divergent mandates rather than focusing on effective risk management.

Question 2. Given the scale and the speed of nation-state threats to telecommunications networks, how should the Federal government engage on carrier cybersecurity in a way that recognizes its importance but avoids mandates that are so rigid they hinder the substantial security work industry is already doing?

Answer. Collaboration and information sharing are key to thwarting future attacks. The Office of the National Cyber Director (ONCD) should set a tone on Federal cyber policymaking that is supportive of public-private collaboration on cybersecurity—as is expected in the upcoming National Cybersecurity Strategy It is imperative that Congress pass a long-term reauthorization of the Cybersecurity Information Sharing Act of 2015 to ensure robust information sharing among public and private sector partners.

The Federal Government should also recognize that these are nation-state attacks, and use its full capacity to impose costs on state-sponsored adversaries to deter future cyberattacks. We cannot allow these entities to act with impunity.

a. How do you view the shift away from the prior declaratory ruling toward a more collaborative, less prescriptive framework?

Answer. The shift will allow cybersecurity practitioners to focus their attention squarely where it belongs—on cybersecurity innovation and partnerships designed to secure our Nation against state-sponsored adversaries.

Providers have been participating in biweekly briefings with the intelligence community, Federal law enforcement agencies, and the Department of War for several years. These briefings are designed to facilitate timely bidirectional information sharing, coordinate defensive measures, assess ongoing threats and align national response strategies following major cyber incidents.

Leading industry providers have established a formal forum for collaboration, bringing together the Chief Information Security Officers (CISOs) from the largest carriers in the United States and Canada. As a result, engagement and coordination at both the CISO and senior staff levels have significantly increased across the sector.

Question 3. Could you briefly discuss concerns about products and equipment sourced from foreign vendors—particularly those linked to the People's Republic of China—containing exploitable weaknesses or that could give adversaries opportunities to pre-position access deep inside U.S. networks?

Answer. Congress should establish a single point of contact within government where industry can obtain the latest intelligence about suspect suppliers. As we make decisions about suppliers for our networks, sharing information about these suppliers will help industry better assess potential risks, even for suppliers that may not be formally banned but are under investigation by the U.S. government.

USTelecom members are fully committed to taking the necessary steps to ensure our national security, and to ensure that the United States' supply chains are protected against bad actors. We are currently engaged with a wide variety of government partners:

- The Department of Commerce Bureau of Industry and Security (BIS) can review transactions and uses of services involving ICTS developed and controlled by a foreign adversary as set forth in the *Information and Communications Technology and Services Supply Chain* Rule pursuant to EO 13873 on Securing the ICTS Supply Chain and the International Emergency Economic Powers Act. BIS has numerous work streams that address ICTS run by the Office of Information and Communications Technology and Services (OICTS).
- The FCC has several workstreams that examine foreign adversary participation in regulated activities. One example is the Covered List implementing the Secure Networks Act, while others look at licensed activities and propose more comprehensive regulatory review of FCC-licensed equipment for sale in the United States.
- The Federal Acquisition Regulation Council is tasked with developing rules governing Section 889 of the 2019 NDAA, which imposes restrictions on Federal contractors' use of covered telecommunications equipment and services from specified foreign entities.
- The Department of War maintains a list of *Chinese Military-Civil Fusion contributors operating directly or indirectly in the United States* to implement section 1260H of the National Defense Authorization Act for Fiscal Year 2021.
- The Committee for the Assessment of Foreign Participation in the United States Telecommunications Services Sector (Team Telecom) assists the FCC in reviewing license applications for national security concerns and may prohibit the use of certain equipment on a case-by-case basis through deal-specific agreements negotiated with executive-branch agencies.

All of this work is in addition, or sometimes responsive to, company or product-specific actions by Congress, like the Select Committee on the CCP or specific directives in the National Defense Authorization Act. Agency work overlaps and in some areas is not consistent. Some work by the government is not transparent or results in abrupt changes to the legal status or risk related to products and services. Security concerns may not be transparently communicated to regulated entities. All of this creates an unpredictable environment. Congress and the President should promote coordination and deconfliction of supply chain related work across the Federal government. Again, a single point of contact within the government would assist providers as they seek to make informed decisions regarding suppliers.

a. Do you see evidence that adversaries view commercial telecom equipment as a strategic foothold that gives them long-term options to exploit crises?

Answer. State-sponsored adversaries continually probe for vulnerabilities across a broad array of industries and government, seeking opportunities to gain strategic, economic, or technological advantage. This dynamic threat landscape extends to commercial telecommunications equipment. For this reason, we remain committed to close coordination with our government partners—across all relevant agencies and collaborative forums—to ensure that risks are identified early, mitigated effectively and addressed through sound policy and technical safeguards. By working together, we can strengthen the resilience of our communications infrastructure and uphold the security and trust that our interconnected nation depends on.

RESPONSE TO WRITTEN QUESTIONS SUBMITTED BY HON. TODD YOUNG TO ROBERT MAYER

Artificial Intelligence

Mr. Meyer [sic]—In your testimony, you discuss how adversaries are using automation, machine learning, and tailored tradecraft to identify and exploit vulnerabilities and then are constantly updating or modifying their technologies to better advance their tactics. Technologies, like AI, have been actively discussed as a tool used by bad actors and criminals to not only damage our critical infrastructures but also conduct scam and fraud. What is not as often discussed is the "good guys" application of technologies like AI to identify, respond to, or effectuate resilient mechanisms to protect against these attacks to our communication networks.

Question 1. Why is that the case? Is technology too nascent to combat these criminals' tactics? Are companies not deploying it because of regulatory barriers? Or is it happening and it's just being overshadowed by the negative use cases of the technology?

Answer. While the technology is indeed nascent, we are already seeing emerging use cases that empower "good guys" to improve security.

AI can be used to identify vulnerabilities and early indicators of cyber threats by assessing network operations, system performance and technical signals at machine speed, allowing operators to detect and address risks before they disrupt service.

These capabilities support a more proactive security posture by enabling automated risk assessment, faster identification of abnormal conditions, and quicker response to potential attacks. AI can also help strengthen defenses by learning from prior incidents and shared threat intelligence, improving the ability to anticipate and counter increasingly sophisticated threats.

Ensuring U.S. leadership in AI is therefore closely tied to embracing new technological opportunities to protect critical infrastructure. Continued investment in advanced network technologies and close collaboration between industry and government will help reinforce the security, resilience and reliability of the Nation's communications networks.

Question 2. We are all aware of efforts to remove barriers to deployment of AI, but what else can we be doing that we haven't thought of, or worked on, to advance technologies or the capabilities of technologies to protect against attacks to our communications networks?

Answer. Among ways Congress can strengthen U.S. leadership in AI is by streamlining permitting on Federal lands. Simply put, permitting processes for AI-ready connectivity and broadband deployment at all levels of government are in desperate need of reform. These processes are the single most time-consuming aspect of a high-speed network build or upgrade. Streamlining NEPA and historical review approvals, including eliminating duplicative reviews on previously analyzed lands, would accelerate broadband deployment in rural America and allow providers to install the newest and most secure technologies more quickly.

In addition, the Federal government has a critical role in increasing the costs and consequences imposed on malicious cyber actors—using diplomatic, economic, law-enforcement and national security tools—to ensure that nation-state adversaries are deterred from targeting U.S. networks with impunity. Meeting this challenge requires a unified front between government and industry to confront foreign threats to critical infrastructure.

Response to Written Questions Submitted by Hon. Maria Cantwell to Robert Mayer

Cybersecurity and BEAD Non-Deployment Grants

The bipartisan Infrastructure Investment and Jobs Act of 2021 appropriated $42 billion for the BEAD program, $1.2 billion of which was allocated to the State of Washington to connect households to broadband.

What's more, the plan was designed to provide states with opportunities for programs beyond connecting unserved and underserved households, allowing some of the state's funding to go to non-deployment initiatives like adoption and network resiliency.

Yet while the Trump Administration has delayed states' access to funding and tacked on unrelated policy objectives conditioned on the deployment money, they've also been holding up other important non-deployment resources. Resources that could be used for improving cybersecurity in the communications networks we're investing billions in.

Question 1. Should NTIA and the Department of Commerce release the non-deployment funding for states to use?

Answer. We believe non-deployment funds should be made available to states, and they should use these funds for:

(1) Funding for states to upgrade 911 facilities to fiber and NG911

(2) Expediting broadband permitting at the federal, state and local levels

(3) Cybersecurity funding for end-of-life equipment and workforce training

Question 2. How can this funding help to strengthen network security?

Answer. The BEAD NOFO explicitly lists “cybersecurity training” and “workforce development” as eligible non-deployment activities. Using non-deployment funds to upskill local provider employees and replacing known insecure legacy equipment ensures that the people and equipment running the network are as modern as the fiber in the ground.

RESPONSE TO WRITTEN QUESTION SUBMITTED BY HON. AMY KLOBUCHAR TO ROBERT MAYER

Critical Infrastructure and Artificial Intelligence

Question 1. Recent cyberattacks, such as Volt Typhoon, have revealed the fragility of America’s critical infrastructure. Adversaries including China and Russia continue to attack our critical infrastructure, threatening systems including electrical, industrial control, and rail. In your testimony you wrote about the need to ensure American leadership in AI to defend our networks. How can we use AI to identify vulnerabilities to cyber-attacks and protect our critical infrastructure?

Answer. AI can be used to identify vulnerabilities and early indicators of cyber threats by assessing network operations, system performance, and technical signals at machine speed, allowing operators to detect and address risks before they disrupt service.

These capabilities support a more proactive security posture by enabling automated risk assessment, faster identification of abnormal conditions and quicker response to potential attacks. AI can also help strengthen defenses by learning from prior incidents and shared threat intelligence, improving the ability to anticipate and counter increasingly sophisticated threats.

Ensuring U.S. leadership in AI is therefore closely tied to protecting critical infrastructure. Continued close collaboration between industry and government will help reinforce the security, resilience, and reliability of the Nation’s communications networks.

RESPONSE TO WRITTEN QUESTIONS SUBMITTED BY HON. TED CRUZ TO DANIEL GIZINSKI

Question 1. Given the scale and the speed of nation-state threats to telecommunications networks, how should the Federal government engage on carrier cybersecurity in a way that recognizes its importance but avoids mandates so rigid they hinder the substantial security work industry is already doing?

Answer. The pace at which nation-state threats continue to advance makes it clear that industry and government must work together in a highly coordinated manner. We see a few key steps that can help promote an effective, consolidated approach:

1: Establish an appropriate forum for information sharing between government and telecommunications operators, inclusive of the supply chain, will help ensure that threats are communicated at the pace of relevance.

2: Frame an end-to-end view of cybersecurity that presents a legally sound and durable compliance framework along with thoughtful incentive programs that facilitate/a proactive cyber posture and collaborative information sharing.

3: Recognize that the advent of 5G Non-Terrestrial Networks (NTN)[1] blur the lines between satellite cybersecurity and telecom cybersecurity, any such compliance framework must consider the need to protect data across the various different networks that may be transited, including systems that may be served by both terrestrial networks and Supplemental Coverage from Space (SCS).[2]

How do you view the shift away from the prior declaratory ruling toward a more collaborative, less prescriptive framework?

Answer. U.S. communications security is far too important to address with anything other than wholehearted commitment from both industry and government—establishing a collaborative framework is a key first step. We see tremendous value in establishing and incentivizing participation in taking an active defense posture. Industry suppliers are well-placed to provide recommendations for approaches that are less disruptive to operators but effective against various threat actors.

[1] *Non-Terrestrial Networks (NTN)*

[2] *FCC Advances Supplemental Coverage from Space Framework | Federal Communications Commission*

Cyber warfare is inherently asymmetric. Our telecom operators must close every possible ingress point, while adversaries only need to find a single entry point. The more secure our systems are, the more difficult—and expensive—it becomes to find these entry points. The best opportunity to disrupt this is to move quickly and thoughtfully to provide baseline security for these systems in the immediate term and over the longer term, operate under a framework that makes clear that new vulnerabilities can and will be addressed as they are discovered—rather than on a predictable schedule.

Question 2. Could you briefly discuss concerns about products and equipment sourced from foreign vendors—particularly those linked to the People's Republic of China—containing exploitable weaknesses or that could give adversaries opportunities to pre-position access deep inside U.S. networks?

Answer. Hardware and software should be viewed thoughtfully when designing and developing critical infrastructure. Education and incentives should be established during the design phase to ensure that telecommunication operators are leveraging secure-by-design systems, ideally those that are designed and manufactured in the USA. "Rip and Replace" is a critical step from the position we are in today, but it is both more efficient and safer to avoid replicating the situation that created this risk in the first place. Encouraging the use of secure-by-design components with verifiable supply chain integrity will help ensure a strong security foundation.[3]

a. Do you see evidence that adversaries view commercial telecom equipment as a strategic foothold that gives them long-term options to exploit crises?

Answer. There is strong evidence that companies like Huawei are leveraging state support to underbid competitors by significant margins—in some cases with 70 percent lower prices than competitors and extended financing terms.[4] This practice appears to be enabled by state subsidies and favorable financing from Chinese policy banks. This has allowed these companies to crowd out competitors and embed their equipment in critical national networks. This entrenchment in critical infrastructure is a strategic foothold that could allow for possible surveillance, data exfiltration, or even disruption in times of crisis.[5]

Response to Written Questions Submitted by Hon. Ted Cruz to Jamil N. Jaffer

Question 1. The Federal Communications Commission (FCC) does not run cyber operations, nor does it investigate intrusions. It is a communications regulator, without direct insight into national security threats. Agencies like the Cybersecurity and Infrastructure Security Agency, the National Security Agency, and the Federal Bureau of Investigation handle cybersecurity every day. They track nation-state activity, run threat hunting teams, and respond to intrusions in real-time. Given the clear delineation in authorities and expertise, should the FCC be writing cybersecurity rules for the telecom sector when it lacks that operational understanding and legal authority to do so?

Answer. As your question highlights, traditional communications regulators like the Federal Communications Commission (FCC) have limited expertise and authorities relative to cyber threats, particularly on the former front and as compared to certain other government agencies and certainly as compared to industry leaders and cybersecurity innovators. The limited expertise and carefully bounded authority of the FCC certainly make it less effective for the FCC to try to be the key player writing the "cyber rules of the road" for the telecommunications industry in what is a very rapidly cyber evolving threat environment.

Indeed, as I describe more fully in my response to your second question below, I'm also quite skeptical of the ability of the FCC or other government departments and agencies to do an effective job of imposing detailed, specific regulatory measures in this domain. Rather, I support a collaborative approach where the government: (1) provides frameworks to industry to outline a broad, effective approach to cyber defense; (2) shares detailed, actionable information with industry; and (3) takes di-

[3] *Comtech-WP-Ground-Station-Cyber-Threats-and-Product-Design-Techniques-for-Defense.pdf*

[4] *China's Competitiveness: Huawei*

[5] *Huawei and Its Siblings, the Chinese Tech Giants: National Security and Foreign Policy Implications—United States Department of State*

rect action to impose costs on nation-state adversaries in order to deter them from targeting America's critical infrastructure.[1]

For far too long, nation-states like China, Russia, Iran, and North Korea and their private sector proxies have largely gotten off scot-free when infiltrating U.S. private sector systems and networks, including critical infrastructure systems, to steal data,[2] put in place potentially damaging capabilities,[3] and take destructive actions against certain companies.[4] The failure of the United States to effectively imposes costs on our adversaries, particularly in a public manner, creates an inherently unstable situation where our adversaries are more likely to get increasingly aggressive, increasing the risk of a significantly problematic scenario where the U.S. government has no choice to respond.[5] As such, rather than regulating, whether through the FCC or otherwise, the U.S. government ought do its part to enable private sector defense and take the fight to the enemy in the cyber domain.

Question 2. Given the scale and the speed of nation-state threats to telecommunications networks, how should the Federal government engage on carrier cybersecurity in a way that recognizes its importance but avoids mandates so rigid they hinder the substantial security work industry is already doing?

Answer. As you know, cybersecurity threats morph at a rapid rate, particularly in the modern age of AI-enabled attacks. One need only look at the recently released report by Anthropic about the use of its systems by Chinese nation-state attackers to engage in novel forms of automated exploitation to get a sense of how rapidly the threat landscape is changing.[6] Given this context, I am highly skeptical of the ability of any regulatory agency—whether the Federal Communications Commission, the Cybersecurity Infrastructure & Security Agency within the Department of Homeland Security, or any other—to effectively be able to keep up with this rapidly changing environment.

To the contrary, I actually worry that the promulgation of new regulations is likely to actually further solidify an already-problematic compliance culture, where regulatory lawyers are called in to identify the minimum a company might do to follow a given regulation. This problem, of course, is worsened when such regulation is rapidly outstripped by innovation, meaning that the very standard being complied

[1] *See, e.g.,* Jamil N. Jaffer, *Statement for the Record,* Signal Under Siege: Defending America's Communications Networks, Subcommittee on Telecommunications & Media, U.S. Senate Committee on Commerce (Dec. 2, 2025), at 19, available online at <*https://www.commerce.senate.gov/services/files/F12CC91A-03E8-44BD-9EE4-D3778C708D96*> ("To preserve the value these organizations—and many other private sector entities—provide us, the Federal government must partner tightly with industry to enable better cyber defense. This means sharing massive amounts of data (classified and otherwise), providing incentives to obtain and deploy better defensive cyber systems and capabilities, and aggressively imposing costs on adversaries, in appropriate circumstances, to deter the deployment or use of potentially disruptive or destructive capabilities.")

[2] *See, 3e.g.,* Keith B. Alexander, *Prepared Statement of GEN (Ret) Keith B. Alexander,* A Borderless Battle: Defending Against Cyber Threats, House Committee on Homeland Security (Mar. 22, 2017), at 2, available online at <*https://www.congress.gov/115/meeting/house/105741/witnesses/HHRG-115-HM00-Wstate-AlexanderK-20170322.pdf*> ("[T]he ongoing theft of intellectual property from American companies . . . continues to represent the greatest transfer of wealth in human history.").

[3] *See* Office of the Director of National Intelligence, *Annual Threat Assessment of the U.S. Intelligence Community* (Mar. 2025), at 9, available online at <*https://www.dni.gov/files/ODNI/documents/assessments/ATA-2025-Unclassified-Report.pdf*>

[4] *See* Director of National Intelligence James R. Clapper, *Opening Statement to Worldwide Threat Assessment Hearing,* Senate Armed Services Committee (Feb. 26, 2015), at 11, available online at <*https://www.armed-services.senate.gov/imo/media/doc/15-18%20-%202-26-15.pdf*> ("2014 saw, for the first time, destructive cyberattacks carried out on U.S. soil by nation-state entities, marked first by the Iranian attack against the Las Vegas Sands Casino Corporation, a year ago this month, and the North Korean attack against Sony in November.")

[5] *See, e.g.,* Jamil N. Jaffer, *Statement for the Record,* Safeguarding the Federal Software Supply Chain, Subcommittee on Cybersecurity, Information Technology, and Government Innovation, House Committee on Oversight and Accountability (Nov. 29, 2023), at 10, available online at <*https://oversight.house.gov/wp-content/uploads/2023/11/Written-Statement-Jaffer.pdf*> ("[W]hen our adversaries don't know how we might react—or worse, based on prior practices assume that we won't react all—they are more likely to push the envelope and test our boundaries. Not only is this bad for the United States because we pay the price for such adversary activity, but such a scenario is actually inherently unstable and therefore likely to lead to more conflict not less. That's because having been tempted by a lack of American response into trying the next more aggressive thing, at some point our adversary may—whether intentionally or inadvertently—cross a line that neither they nor we understood existed but which, once crossed, requires us to respond in a significant way.").

[6] *See* Anthropic, *Disrupting the First Reported AI-Orchestrated Cyber Espionage Campaign* (Nov. 2025), available online at <*https://assets.anthropic.com/m/ec212e6566a0d47/original/Disrupting-the-first-reported-AI-orchestrated-cyber-espionage-campaign.pdf*>.

with outdated even before the ink is try, potentially creating more vulnerabilities than less.

As such, in my view, the better approach is for the Federal government to collaborate tightly with innovators and industry players who have a real sense of what the threat landscape looks like and how it is changing, and to provide defensive frameworks to help industry get better at its own defense, rather than specific, detailed regulatory proceedings that can't keep up with adversaries. Moreover, rather than reaching first for the regulatory stick, as Federal agencies are often wont to do, Congress should encourage—and perhaps direct—such agencies to utilize carrots, including tax incentives and the benefits of Federal procurement, to align their interests with those of companies, their boards, and their investors.[7] Indeed, if the government were to do so, it would likely see a much more significant uptake in industry efforts to harden network defenses than the traditional regulate-first, get-smart later approach.

In addition, to the extent that Federal agencies or Congress believe that government ought be doing more than just incentivizing good behavior, I also agree. But rather than imposing high-cost (and likely ineffectual) regulation, the government ought instead seek to collect intelligence on the cyber threat actors coming after American industry and share that information with the private sector at scale, in detailed and actionable form (including in classified form if necessary), and assist industry with the right techniques and tools to effectively defend themselves against sophisticated nation-state actors.

The recent Salt Typhoon activity by Chinese actors against American telecommunications companies is instructive in this regard. In that case, not only did the government fail to provide detailed, actionable warnings of the type that could have actually help industry protect itself (or protect the government information their systems contained), the government also failed to effectively identify information it already had in its possession about those same threat actors in Federal networks and, as a result, didn't share that information with industry either.[8] Worse still, even after the government realized its own failure, rather than taking swift action to ensure that such errors don't happen again, the FCC instead sought to impose short-sighted regulations on industry without any accounting for the government's own failures.[9]

Finally, in addition to helping industry defend itself more effectively, given the stark reality that private sector companies operating in a constrained environment cannot possibly be expected to defend themselves against nation-state actors with access to virtually unlimited resources and manpower, it is critical that the Federal government engage in a much more robust set of responsive actions to deter nation-state actors.[10] The current Administration has demonstrated a willingness to push back against our adversaries in range of contexts over the last year and I am hope-

[7] *See, e.g.,* Jaffer, *Statement for the Record,* Signal Under Siege, *supra* n.1 at 21–22.

[8] *See id.* at 18 ("And yet, in perhaps one of the most stunning revelations to come out of this incident, even as the FCC and White House were calling for significant regulation of American telecommunications companies, the outgoing head of the Department of Homeland Security's Cybersecurity and Infrastructure Security Agency (CISA), published a blog post stating that 'CISA threat hunters previously detected the same actors in U.S. government networks.' . . . [A]ll this may make one recall the findings of the 9/11 Commission report, which noted that the U.S. government had both successfully the potential of a major terrorist attack and knew of specific terrorists with visas to enter the United States, but critically failed to share actionable information in a timely fashion with those able to identify and stop those individuals[.]"); *see also, e.g.,* Tim Starks, *'Whatever We Did Was Not Enough': How Salt Typhoon Slipped Through the Government's Blind Spots,* CyberScoop (May 20, 2025), available online at <*https://cyberscoop.com/salt-typhoon-us-government-response/*>

[9] *Id.*

[10] *See, e.g.,* GEN (Ret) Keith B. Alexander & Jamil N. Jaffer, *Iranian Cyberattacks Are Coming, Security Experts Warn,* Barron's (Jan. 10, 2020) ("Expecting individual companies to defend themselves against a nation state with virtually unlimited financial resources and human capital does not make sense. Yet today that is our national policy in cyberspace. This is so even though, in every other context, defense against nation-state attacks is the province of the government. We don't expect Target or Walmart to have surface-to-air missiles to defend against Russian Bear bombers. Yet when it comes to cyberspace, we expect exactly that of every American company, large or small."); see also, *e.g.,* Jaffer, *Statement for the Record,* Signal Under Siege, *supra* n.1 at 19 ("[W]e must remember that private sector companies, including those in the [] telecommunications and infrastructure sectors, are not primarily in the business of defending themselves against cyberattacks; rather, they operate in order to provide products and services to customers and to generate economic returns from such business.").

ful that the President's soon-to-be-released National Cybersecurity Strategy will take a forward-leaning approach in the cyber domain as well.[11]

a. How do you view the shift away from the prior declaratory ruling toward a more collaborative, less prescriptive framework?

Answer. I am strongly supportive of the government, including the Federal Communications Commission, shifting away from aggressive declaratory rulings that seek to blame and penalize the victims of nation-state architected cyber operations and instead moving towards a more collaborative, less-prescriptive framework that enables and supports the efforts of private sector actors to defend themselves.

Question 3. As adversaries adopt AI to scale cyber operations, industry is also leveraging AI-driven defenses to identify threats earlier and respond more effectively. Our adversaries are wasting no time leveraging AI to enhance their attack operations, but carriers are also using AI to strengthen defenses. From your perspective, what role do emerging AI tools play in helping telecom providers secure their networks?

Answer. In my view, the advent of AI-enabled capabilities is likely to effectively enable both offensive and defensive actors in the cyber domain. As such, I think that there are significant benefits to our telecommunications industry working with innovative technology companies, from venture-backed startups to large companies building scaled capabilities, to obtain, deploy, and utilize AI-enabled defensive capabilities.

While there are many who fear that the widespread deployment of AI capabilities will benefit attackers more than defenders, my view is that the outcome is likely to be significantly more nuanced. While it is true that in the cyber domain—as in the physical world—the offense often has a slight edge, in part because of its first-mover advantage, and that AI-enabled capabilities may very well enhance that edge, it is also the case that AI-enabled cyber defenses will allow rapid and evolving responses to cyber threats and will help defenders not only keep up, but on occasion, even get ahead of potential threats.[12] As such, while I am not blind to the very real challenges that AI will bring to the cyber defense domain, I also believe there are terrific opportunities for innovation and advantage here and that the American systems of capital allocation and innovation is best positioned to take advantage of these opportunities.

a. What role should the Federal government play in this space?

Answer. Helping enable the creation and development of AI-enabled cyber defenses not only for industry but for government is an area where Congress can play a major role by providing incentives to industry players to create, obtain, and deploy such capabilities. Specifically, Congress might consider the development of tax incentives to encourage investors and innovators—particularly those who agree to not provide capabilities to American adversaries, not take adversary capital, nor invest alongside adversaries—to build such capabilities. Likewise, Congress might provide similar incentives to industry, particularly American critical infrastructure organizations, to acquire and deploy such capabilities across their networks, including telecommunications systems and backbone networks.

Moreover, Congress might helpfully to encourage Federal agencies to avoid imposing unhelpful regulations that encourage the adoption of legacy capabilities or the creation of new defenses against legacy threats.

Finally, Congress can also help in a major way by taking action to "occupy the field" with pro-innovation policies—like those that you have championed[13]—to stave

[11] *See* Tim Starks, *Five-Page Draft Trump Administration Cyber Strategy Targeted for January Release,* CyberScoop (Dec. 4, 2025), available online at <*https://cyberscoop.com/trump-national-cybersecurity-strategy-2025-release/*> ("National Cyber Director Sean Cairncross recently offered a preview of some of those themes and plans. 'As a top line matter, it's going to be focused on shaping adversary behavior, introducing costs and consequences into this mix,' Cairncross said last month at the 2025 Aspen Cyber Summit.").

[12] *See* House Committee on Energy & Commerce, Subcommittee on Communications & Technology, *Global Networks at Risk: Securing the Future of Communications Infrastructure* (Apr. 30, 2025), Serial No. 119–17, Government Printing Office, at 73, available online at <*https://www.congress.gov/119/chrg/CHRG-119hhrg60348/CHRG-119hhrg60348.pdf*> ("[T]here is a big debate about will AI improve the attacker more or improve the defender more, and I actually [think] it is a mixed bag []. In some ways, it will definitely, as Ms. Galante pointed out, enable attackers who don't have capabilities today to have more capabilities. At the same time, the defender will have an edge as well because they will be able to get ahead of the threats, identify vulnerabilities, cut them off at the pass and go after the attackers. So[,] while the offense, like in football, always has a little bit of an edge, [] and AI will enhance that, AI is going to enhance defenders as well.")

[13] *See, e.g.,* Senator Ted Cruz, *Sen. Cruz: Adopting Europe's Approach on Regulation Will Cause China to Win the AI Race* (May 8. 2025), available online at <*https://www.commerce*

off unhelpful state-based and Federal regulation that would actually limit the ability of forward-leaning, innovative AI companies to develop the very advanced capabilities that can help the government and industry better protect ourselves from America's adversaries.

RESPONSE TO WRITTEN QUESTIONS SUBMITTED BY HON. AMY KLOBUCHAR TO DEBRA JORDAN

Next Generation 911:

Question 1. As co-chair of the Next Generation 911 caucus with Senator Budd, I was pleased to see your recommendation to fully fund Next Generation 911 as one of your recommendations to secure our networks. I also lead the Enhancing First Response Act with Senator Blackburn, which would reclassify 911 operators as emergency responders. Can you speak to the importance of this reclassification?

Answer. Reclassification of 911 operators is a long overdue action that would recognize these critical first responders. They are the first person in the 911 emergency process, the voice of calm reassurance to individuals in a crisis—whether a mass casualty event, domestic violence, or any other emergency. Continuing to classify them as administrative personnel simply ratifies the injustice. Their duties typically involve triaging of emergency calls, providing emergency medical assistance and dispatch, and handling other life-or death situations until field units arrive.

In my career as Chief and Deputy Chief of the Public Safety and Homeland Security Bureau at the Federal Communications Commission, I was privileged to visit many Public Safety Answering Points. There I spoke with 911 operators and witnessed them in the midst of their work. These visits solidified for me that they are indeed first responders and not administrative personnel. Whether talking a caller through an active labor/delivery situation, domestic violence, or a child through an unresponsive parent situation, these 911 operators handled the situation with the professionalism of their field counterparts.

Reclassification as first responders would recognize their critical role as first point of contact and grant them much needed access to benefits such as mental health support, training, and the appropriate recognition. It would likely also improve recruitment to this career field that is too often understaffed. It is simply the right thing to do.

Public Safety:

Question 2. Recently the Federal Communications Commission rolled back a ruling that affirmatively requires telecommunications carriers to secure their networks from unlawful access or interception of communications, despite, according to one report, more than 60 percent of telecommunications operators experiencing a cyberattack in the last year. How does this action threaten the work of emergency responders relying on telecommunications networks to reach people who need their help?

Answer. Our digital society is highly dependent on telecommunications networks in nearly every aspect of our lives from finance to education to healthcare and more. Emergency responders specifically, must be able to assume that critical communications services will be consistently and securely available at all times. This includes citizens' ability to dial 911 and reach first responder services, for 911 Operators to be able to dispatch field agents, and for the wide range of public safety personnel to communicate and collaborate. They must be able to rely on their communications being reliable and secure from compromise. If a law enforcement agency serves legal process for a wiretap, they must have the legally required assurance that those requests will be confidential and secure from adversaries' access. Emergency alerting systems that support presidential and every day alerts must be confident that when an alert is issued to the public, that it is done so by authorized alert originators.

.senate.gov/2025/5/sen-cruz-adopting-europe-s-approach-on-regulation-will-cause-china-to-win-the-ai-race> ("[Senator] Cruz announced he will soon release a new bill that creates a regulatory sandbox for AI—modeled on the approach taken by Congress and President Clinton with respect to the internet—to remove barriers to AI adoption, and prevent needless state over-regulation."); *see also, e.g.,* Senator Ted Cruz, *Sen. Cruz Unveils AI Policy Framework to Strengthen American AI Leadership* (Sept. 10, 2025) available online at <*https://www.commerce.senate.gov/2025/9/sen-cruz-unveils-ai-policy-framework-to-strengthen-american-ai-leadership*> ("Today, U.S. Senate Commerce Committee Chairman Ted Cruz (R-Texas) released a legislative framework designed to promote American leadership in artificial intelligence. . . . The bill creates a regulatory 'sandbox,' a policy endorsed by President Trump's AI Action Plan, that gives AI developers space to test and launch new AI technologies without being held back by outdated or inflexible Federal rules.").

These are just a few examples of how emergency responders must be able to rely on the confidentiality, integrity, and availability of telecommunications networks.

The declaratory ruling and notice of proposed rule making that the FCC recently overturned would have made clear to telecommunications providers that they are responsibility for the security of their networks. The declaratory ruling specifically clarified that Section 105 of the Communications Assistance for Law Enforcement Act (CALEA) requires only lawful intercepts of telecom networks. And the Notice of Proposed Rulemaking would have leveraged basic cyber risk management requirements across all of our Nation's telecom providers. Those common sense requirements basically required providers to develop, update, and implement cyber risk management plans, leveraging the Cyber Security Framework developed by the National Institute of Standards and Technology through extensive public and private sector collaboration. The Commission already has similar rules in place for a small subset of telecom providers, and in fact in August 2025, proposed similar requirements for undersea cable licensees.

Instead, the FCC Chairman says the Commission is talking with providers about securing their networks. As we all know, there are thousands of telecom providers, large and small. They should all have clear common sense guidelines to assess risk and implement at least basic hygiene to reduce and manage cyber risk. The ongoing public-private dialog between government regulators, intel agencies, and telecom providers would then provide an excellent addition to adapt to emerging threats.

○