S. HRG. 118–739

COMMUNICATIONS NETWORKS SAFETY AND SECURITY

HEARING

BEFORE THE

SUBCOMMITTEE ON COMMUNICATIONS, MEDIA, AND BROADBAND

OF THE

COMMITTEE ON COMMERCE, SCIENCE, AND TRANSPORTATION
UNITED STATES SENATE

ONE HUNDRED EIGHTEENTH CONGRESS

SECOND SESSION

DECEMBER 11, 2024

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

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

U.S. GOVERNMENT PUBLISHING OFFICE
61–952 PDF WASHINGTON : 2025

SENATE COMMITTEE ON COMMERCE, SCIENCE, AND TRANSPORTATION

ONE HUNDRED EIGHTEENTH CONGRESS

SECOND SESSION

MARIA CANTWELL, Washington, *Chair*

AMY KLOBUCHAR, Minnesota	TED CRUZ, Texas, *Ranking*
BRIAN SCHATZ, Hawaii	JOHN THUNE, South Dakota
EDWARD MARKEY, Massachusetts	ROGER WICKER, Mississippi
GARY PETERS, Michigan	DEB FISCHER, Nebraska
TAMMY BALDWIN, Wisconsin	JERRY MORAN, Kansas
TAMMY DUCKWORTH, Illinois	DAN SULLIVAN, Alaska
JON TESTER, Montana	MARSHA BLACKBURN, Tennessee
KYRSTEN SINEMA, Arizona	TODD YOUNG, Indiana
JACKY ROSEN, Nevada	TED BUDD, North Carolina
BEN RAY LUJÁN, New Mexico	ERIC SCHMITT, Missouri
JOHN HICKENLOOPER, Colorado	J. D. VANCE, Ohio
RAPHAEL WARNOCK, Georgia	SHELLEY MOORE CAPITO, West Virginia
PETER WELCH, Vermont	CYNTHIA LUMMIS, Wyoming

LILA HARPER HELMS, *Staff Director*
MELISSA PORTER, *Deputy Staff Director*
JONATHAN HALE, *General Counsel*
BRAD GRANTZ, *Republican Staff Director*
NICOLE CHRISTUS, *Republican Deputy Staff Director*
LIAM MCKENNA, *General Counsel*

SUBCOMMITTEE ON COMMUNICATIONS, MEDIA, AND BROADBAND

BEN RAY LUJÁN, New Mexico, *Chair*	JOHN THUNE, South Dakota, *Ranking*
AMY KLOBUCHAR, Minnesota	ROGER WICKER, Mississippi
BRIAN SCHATZ, Hawaii	DEB FISCHER, Nebraska
EDWARD MARKEY, Massachusetts	JERRY MORAN, Kansas
GARY PETERS, Michigan	DAN SULLIVAN, Alaska
TAMMY BALDWIN, Wisconsin	MARSHA BLACKBURN, Tennessee
TAMMY DUCKWORTH, Illinois	TODD YOUNG, Indiana
JON TESTER, Montana	TED BUDD, North Carolina
KYRSTEN SINEMA, Arizona	ERIC SCHMITT, Missouri
JACKY ROSEN, Nevada	J. D. VANCE, Ohio
JOHN HICKENLOOPER, Colorado	SHELLEY MOORE CAPITO, West Virginia
RAPHAEL WARNOCK, Georgia	CYNTHIA LUMMIS, Wyoming
PETER WELCH, Vermont	

CONTENTS

WITNESSES

APPENDIX

COMMUNICATIONS NETWORKS SAFETY AND SECURITY

WEDNESDAY, DECEMBER 11, 2024

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

The Subcommittee met, pursuant to notice, at 2:34 p.m., in room SR–253, Russell Senate Office Building, Hon. Ben Ray Luján, Chairman of the Subcommittee, presiding.

Present: Senators Luján [presiding], Klobuchar, Markey, Peters, Rosen, Hickenlooper, Welch, Cruz, Moran, Sullivan, Blackburn, and Budd.

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

Senator LUJÁN. This hearing of the Subcommittee on Communications, Media, and Broadband will now come to order. Today, the Subcommittee is convening a hearing on communications networks safety and security.

I want to recognize our Ranking Member, Mr. Thune, and Senator Moran for filling in for him today, as well as Chair Cantwell and Ranking Member Cruz for working with me to schedule this hearing on such an important topic. I think every member of this committee can agree that there is nothing more important than keeping our communities safe.

That is why I worked with my Commerce Committee colleagues to make our aviation system safer, to prevent roadway fatalities, and to protect consumers from fraud and scams. It is also our responsibility to keep our communication networks safe, to ensure that foreign threat actors like China cannot infiltrate our infrastructure or steal Americans' data.

Currently, our communities, our schools, our hospitals, our libraries, our police departments, and emergency responders do not have the resources to defend themselves against foreign adversaries.

The Salt Typhoon hacks that were discovered last month demonstrate that even the largest corporations in the United States are vulnerable. This attack likely represents the largest telecommunications hack in our Nation's history. There is a lot that we still don't know about the damage that was done by the Salt Typhoon hacks, but what we do know is that more must be done to prevent attacks like this in the future.

There are outstanding recommendations from Federal agencies that must be fully implemented across our networks. This includes standards and best practices recommended by the FCC, Team Telecom, and other Federal partners. One obvious thing we can do today is get equipment manufactured by companies that collaborate with foreign adversaries out of our American networks.

Congress passed the Secure and Trusted Communication Networks Act in 2020, making it clear that we understand the vital importance of removing Huawei and ZTE equipment from every network across the country. Unfortunately, the Rip and Replace program has remained partially unfunded for years, opening up our networks to unnecessary risks and preventable threats.

I am hopeful that there is strong bipartisan agreement to fully fund this program through this year's National Defense Authorization Act and address one of the major known vulnerabilities facing our networks every day once and for all. We also need to protect our networks at every access point, from phones to cars, and even baby monitors.

Critically, this includes the undersea cables that carry traffic across the entire world. As the pressure on our networks continues to increase, it is vital that Federal partners do everything in their power to keep the bad actors out at every point at the supply chain.

We are fortunate to have an expert panel with us today who will speak to the vulnerabilities in our communication system and how we can address them to protect our constituents.

James Lewis, Senior Vice President and Director of the Technology and Public Policy Program at the Center for Strategic and International Studies will speak to how foreign threat actors like China work to infiltrate global telecommunication infrastructure to further their intelligence goals.

Justin Sherman, Founder and CEO of Global Cyber Strategies and Nonresident Senior Fellow for the Cyber Statecraft Initiative at the Atlantic Council, will speak to how companies and the Federal Government keep our networks safe, especially undersea cables.

Tim Donovan, President and CEO of Competitive Carriers Association, will discuss how small carriers across the country navigate cybersecurity challenges, including the need to remove Chinese equipment from their networks.

And finally, James Mulvenon—pronounce that for me, sir—Mulvenon, Ph.D., Chief Intelligence Officer at Premier Consulting, who Senator Moran will introduce, is joining us today as well. I look forward to a productive conversation today, and I want to thank each of you for being here.

With that, I want to turn this over to our Acting Ranking Member, Senator Moran, for his opening statement.

STATEMENT OF HON. JERRY MORAN,
U.S. SENATOR FROM KANSAS

Senator MORAN. Chairman Luján, thank you very much. Thank you for suggesting and making certain that this important hearing took place. I have a goal of working more closely with you now and in the future, and this is a nice way to start.

I am also pleased to be here because my introduction and understanding of this issue mostly comes from my service on the Senate Committee on Intelligence, where it seems to me we are handicapped in our ability to explain to the public and to make awareness of the necessities of making significant changes in the way that we do our business.

So I am pleased that we are having an open hearing to discuss and provide information to our constituents. Chinese hackers have infiltrated our telecommunication system, invaded the privacy of millions of Americans, and compromised our national security, exposing glaring weaknesses in our communications infrastructure.

We need to understand how this attack happened and what we need to do to bring it to an end. We also need to know how to establish effective deterrence that makes China think twice about future violations of American infrastructure.

While it is important that we act quickly, we need to make certain that the policies that we implement work to solve the problem and don't have those things we often call unintended consequences. I am particularly concerned that rushed regulations could increase compliance costs for smaller telecom companies, thereby decreasing resources that are actually available for cybersecurity efforts.

We must not only address this single event, but also investigate the path forward that ensures growth of secure networks for all Americans in all parts of the country. Securing our telecommunications network is not a new topic for this committee or for Congress as a whole.

As Chairman Luján indicated, I joined in 2019 my colleagues in sponsoring the Secure and Trusted Telecommunications Network Act, which established the commonly known Rip and Replace program.

That program, which will reimburse eligible telephone companies for removing and replacing unsecure Chinese equipment in their networks, is currently facing a $3 billion shortfall in funding.

There are companies in Kansas like United Wireless in Dodge City, Kansas that have been able to remove the problematic equipment while still providing their customers with the same level of service they have come to expect, but yet in the absence of the funding that Rip and Replace has been offered to provide.

That is not the case for everyone, and I am pleased to see that the NDAA included a bipartisan provision to fill this funding gap. Rip and Replace program demonstrates that Congress can take bipartisan action to secure our networks, an approach that is urgently needed now as we take steps to confront the challenges posed by China.

As a member of this committee and the Select Committee on Intelligence, I will continue to work with my colleagues and Federal agencies on a coordinated effort to secure our telecommunications network.

But as I said earlier, I think one of the most important things is for the public to understand the challenges that they face and that we face. Mr. Chairman, thank you once again for calling this hearing. I look forward to hearing from our witnesses.

Senator LUJÁN. Thank you very much, Mr. Chairman. To our colleagues, we are to move on to questions now, but we may have

some opening remarks from the Chair and the Ranking Member of the full committee as well later in this. But let's get to questions and I will recognize myself right now for five minutes.

The providers that Competitive Carriers Association represents are the smallest, most rural providers across the country. They not only serve thousands of Americans, but thousands of our most vital community institutions, schools, libraries, hospitals.

Well, I apologize. I have just been corrected that I am just jumping straight to my questions with my interest in this hearing as opposed to hearing from our distinguished panel. So let me jump to that. I appreciate that.

I appreciate that, Senator Moran. But with that being said, why don't we jump to Dr. Lewis for his opening statement. We will each recognize you for five minutes. And Dr. Lewis, you are up, sir.

STATEMENT OF JAMES ANDREW LEWIS, SENIOR VICE PRESIDENT; PRITZKER CHAIR; AND DIRECTOR, STRATEGIC TECHNOLOGIES PROGRAM, CSIS

Mr. LEWIS. Thank you, Mr. Chairman. Thank you, Ranking Member Moran. I thought you would let us off the hook, so I am a little disappointed. But let me thank the Committee for the opportunity to testify on one of the most pressing strategic problems facing the U.S. The scale and audacity of Chinese espionage is unprecedented.

Microsoft must have a machine that generates funny names because the Chinese don't call themselves Salt Typhoon. It appears they may be Unit 61938, an intelligence unit first indicted in 2014.

If it is 61938, we know their names. We have their pictures. It has been 10 years, and they have been very busy. Our response has been to give them a stern lecture and send a few strongly worded notes. We even managed to convict a Chinese spy in 2022, but then we let him go. The signal this sends is that it is open season on the U.S. The conventional responses to espionage do not work with China.

Also, a country can't lose two wars and expect the same level of respect. Every year the Chinese are less cautious. Chinese exploitation of telecommunications for spying began in the early 2000s and has continued across four Administrations. It is increasingly dangerous. All great powers use communications intelligence.

The U.S. is no slacker in this regard, something the Chinese will happily point out to you if you discuss it with them. The Internet has made spying even easier. China has built a comprehensive system for global communications espionage.

China targets space assets, undersea cables, and telecom infrastructures, all accompanied by extensive hacking. The Chinese have remarkable—have had remarkable successes against the U.S. and Salt Typhoon is only the latest. It should not be seen as an isolated incident, but as part of a larger Chinese campaign to systematically exploit global telecommunications networks.

Salt Typhoon may have let China see some surveillance orders submitted to U.S. telecoms, FISA surveillance orders showing which of its agents had been compromised. And there are reports that China acquired metadata and content from numerous high value U.S. targets by accessing their phone calls and texts.

Everyone on this committee is a target. The U.S. hopes it can improve its defenses to the point where a giant resourced—well-resourced and hostile opponent will face insurmountable obstacles. This hasn't worked. Countering China requires two sets of actions. The first is a sustained and forceful effort to disincentivize Chinese espionage. So far, espionage has been penalty free for China.

Second, we need an expanded effort to harden telecommunications networks. Rip and Replace is an important part of this. Hardening falls within the remit of the Committee. This committee can make clear that FCC is the agency in charge and that regulation is necessary. Using CALEA as a stopgap, the current Administration has taken steps to improve security, and the next Administration should continue them.

This committee can perform a valuable service by making clear that securing telecommunications networks must be an immediate priority for the U.S. In preparing for this, someone asked me, why should your average consumer, why should your citizen care?

Putting aside the larger issues of national security, having a foreign power, a hostile foreign power with the ability to turn off the lights, turn off your phones, is not a position that is very comfortable for your average American.

And so I hope one thing we can get from this hearing is a better understanding of that. I thank you and will be happy to answer any questions.

[The prepared statement of Mr. Lewis follows:]

PREPARED STATEMENT OF JAMES ANDREW LEWIS, SENIOR VICE PRESIDENT; PRITZKER CHAIR; AND DIRECTOR, STRATEGIC TECHNOLOGIES PROGRAM, CSIS

Chairman Luján, Ranking Member Thune, distinguished Members of the Subcommittee, I'd like to thank the Committee for the opportunity to testify.

Let me thank the Committee for the opportunity to testify on one of the most pressing strategic problems facing the United States, the security of the U.S. telecommunications system. This kind of problem is not new. In 1863 the Secretary of State warned the United States' representative in France that messages sent to Washington over telegraph networks were being read. In 1900 Britain's dominance of the first global networks gave it strategic advantage. In the 1980s, the Reagan Administration gave senior officials special "white" phones to protect against ubiquitous Soviet telecommunications surveillance. While China's actions are not new, the scale of our dependence on global networks and audacity of Chinese communications espionage is unprecedented.

All great powers engage in communications espionage. The United States itself is no slouch in this regard, something the Chinese will happily point out if you discuss it with them. The Internet has made communications espionage even easier and for the last decade, the problem for major intelligence agencies became not just to acquire information but to find ways to store and analyze it, given the vast quantities involved.

The global telecommunications network is comprised of satellites, undersea cables, terrestrial fiber optics, and wireless networks. This includes devices connected to the internet, cloud services, and the hardware and software that make up the telecommunications infrastructure. These are all interconnected and vulnerable, making this the golden age of communications intelligence. The mobile phone is a gift to spies. A wealthy and hostile nation like China can afford to exploit them all with programs that target space assets, undersea cables, and telecommunications infrastructures, all accompanied by extensive efforts at hacking internet-accessible assets.

Chinese espionage began shortly after the opening of the Chinese economy to the West. Chinese cyber espionage began around 2003 when it built high-speed connections to the new internet. Suddenly, the poorly protected data and networks of U.S. companies, universities and government agencies became easily accessible to China's cyber spies.

There are many examples of this. China leads the world in espionage-related hacking against the United States. Telecommunications has always been a part of this. Beginning more than two decades ago, large scale Chinese government support for Huawei provided both commercial and intelligence benefits, and embedded China in the telecommunications infrastructure of many strategically significant countries, giving it access and potentially control of vital networks. And several years ago, there were incidents involving China Telecom, when it diverted massive amounts of Internet traffic to pass thought China where it could be collected. The famous spy balloon incident was most likely an effort to collect mobile telephone communications (among other things). China is also active in other intelligence areas, such as the use of clandestine agents and satellites, but communications espionage is their centerpiece.

The Chinese have had some remarkable successes against the United States, most recently with what some call 'Salt Typhoon.' This is only the latest Chinese effort, affecting more than two dozen countries. Investigations into the scope and damage are still ongoing. It is premature to say the full effect has been understood or remedied or what, if anything, the Chinese may have left behind on the networks they penetrated. Salt Typhoon should not be seen as an isolated incident but as part of a larger Chinese campaign to systematically exploit global telecommunications networks.

Judging from initial reporting on Salt typhoon, the operation would allow China to be able to see Foreign Intelligence Service Act (FISA) intercept orders submitted to U.S. telecommunications companies, showing which of its agents had been detected (as well as anyone else the United States was interested in surveilling). And while it is unclear what other data China obtained with Salt Typhoon, there are reports that it acquired metadata and content from numerous high value U.S. targets by accessing their telephone calls and texts messages. Everyone on this Committee is a target.

It is also likely that Salt Typhoon has elements that go beyond espionage. An earlier incident named by some companies as "Volt Typhoon" saw China preposition malicious code on U.S. critical infrastructure networks. Salt Typhoon may have also been used in prepositioning malicious code on telecommunications networks. Prepositioning goes beyond espionage as it is a precursor to attack.

To understand and counter China, we must consider the whole picture and not just a single aspect. China has constructed a broad global signals intelligence (SIGINT) surveillances system. China often "mirror images" or copies what it thinks the United States is doing. The model China is copying here is sometimes called "Echelon," which in the vivid imaginations of those hostile to the United States is a global system for intercepting all digital communications. This is inaccurate, but China tries to go one better than the United States and it has different tools, such as state control of telecommunications equipment manufacturers, which it is using to build a global communications espionage network where the United States is the primary target.

From the outside it appears that China has a comprehensive strategy for cyber espionage and communications intelligence that began soon after China gained access to the Internet more than two decades ago. For years, the United States accepted this as the cost of doing business in China. China's initial focus was on commercial and technological espionage as well as conventional politico-military espionage. In the last decade it has expanded in both scale and scope to include preparing for disruptive actions against critical infrastructure including telecommunications networks, monitoring and coercing Chinese citizens who are resident in the United States, and collecting reams of personal data from American citizens. Access to the U.S. telecommunications network is vital to all these efforts.

Huawei remains the exemplar of this effort. It first benefited from the theft of technology (although it no longer needs this as much). It still benefits from immense subsidies from the Chinese government, and these helped it drive Western competitors out of the telecommunications infrastructure business and left it as the major supplier of network infrastructure (in terms of deployed networks) around the world. It was a brilliant strategy that has made China dominant in global telecommunications networks in the way that Britian dominated them 120 years ago. Huawei's success makes 'rip and replace' even more important and its inclusion in the National Defense Authorization Act (NDAA) for eventual passage is an important step for which the Committee is to be congratulated.

Countering China requires two sets of actions. The first is to begin a sustained, direct, and more forceful effort to disincentivize Chinese espionage. The second is to accelerate and expand efforts to harden our own networks and, if possible, those of allies. The United States' response has been too restrained. Economics have outweighed security, something the Chinese count on to hobble the U.S. response.

China faces no real penalty for espionage and the traditional remedies have been insufficient. One of the most serious drawbacks for U.S. strategy is a reluctance to actually engage directly and effectively with hostile actors. As our opponents become more brazen in their actions, a reliance on limited and reactive measures guarantees that hostile actions will only increase. This is the unpleasant reality in which the United States finds itself.

None of the traditional counter-espionage remedies, which are intended to signal displeasure to an opponent and persuade them to reduce their actions, have worked. Expelling diplomats, arresting spies, even closing a Chinese consulate has not persuaded China to scale back. Until recently, the United States and its allies were largely supine in the face of Chinese espionage. The one exception to this was the 2015 intervention by President Obama after the OPM hack, but the effort was short-lived and reportedly even opposed by some of his staff.

Finding an appropriate and effective response to aggressive Chinese espionage is one of the central diplomatic and foreign policy challenges facing the United States. Deterrence in cyberspace has been a complete failure. Developing a program of active defense with our allies is essential for changing China's behavior. What has been done so far, largely the occasional complaint, is insufficient. More assertive measures could include political campaigns to exert pressure on China's leaders, operations to interfere with opponent cyber capabilities, or more comprehensive and damaging sanctions (an approach that European allies would find more acceptable). When China complains about tariffs, it could be useful to remind them of the need to change their behavior.

This is a complicated issue as there is some risk of increased conflict and the Chinese will respond vigorously, perhaps by threatening to use their market leverage. It comes at a time when bilateral relations will become even more difficult, but the damage from accepting Chinese espionage has grown to the point where it is a major security risk, if only because it suggests to the Chinese that the United States will fail to respond to other provocations matter how grave.

Instead, the United States has focused on hardening its defenses. In themselves, these efforts are valuable although still insufficient. As we improve the security of U.S. telecommunications defense, some less sophisticated opponents will be unable to overcome these defenses. Unfortunately, China is not one of them. While our patchwork efforts to build resilience and security make the task of surveillance more difficult and expensive and is a necessary step, China has the resources and commitment to prevail.

Interagency disputes hamper the hardening of networks, and it should be made clear that the Federal Communications Commission (FCC) is the regulatory agency in charge (and regulation is necessary since the alternative has been shown many times to be inadequate for cybersecurity). This may not require new legislation, but it will require Congressional oversight. The FCC has taken action, but more is needed.

In 2022, the FCC banned new telecommunications equipment from Huawei, ZTE, and other Chinese firms, citing national security concerns. This was under the agency's "Covered Equipment Authorization" rules. In 2022 it also revoked authorizations for China Unicom Americas, China Telecom Americas, and Pacific Networks and its subsidiary ComNet to provide telecommunications services in the United States as these gave China a presence on U.S. telecommunications networks. In 2021, the FCC implemented rules requiring carriers to remove and replace existing equipment from these companies in what is known as the 'rip and replace' program. Rip-and-replace by most accounts is 80 percent complete, making continued progress essential.

The recent FCC effort to use CALEA (Communications Assistance for Law Enforcement Act) authorities to require telecommunications companies to meet cybersecurity requirements could, if carefully constructed, usefully improve defenses. CALEA calls on telecommunications carriers to protect intercept controls and data from unauthorized access, implement access controls and audit mechanisms, and ensure the secure transmission of intercept data to law enforcement.

There is an easy comparison between the effort and resources banks put into cybersecurity versus the amount spent by telecommunications companies. Publicly available documents suggest that on average, major banks spend between 6–12 percent of their IT budgets on cybersecurity compared to 3–5 percent spent by major telecommunications companies. Major telecom firms do take cybersecurity seriously but may not fully match the depth and resourcing of efforts in the financial sector.

Major U.S. telecommunications companies could strengthen cybersecurity through infrastructure modernization, use of zero-trust architectures, and increased network segmentation. Copying the financial sector practices, they could improve their threat detection by deploying advanced monitoring tools, AI-based anomaly detection, and

automated incident response. Stronger access controls and robust identity management would help. Telecommunications companies could invest more in acquiring cybersecurity talent and expanding security teams. The challenge is balancing these improvements against operational requirements and costs.

As the Committee knows, telecommunications modernization comes in regular cycles. We are now at the in the midst of the latest cycle to the next generation of telecommunications (5G) and the greater use of Open Radio Access Networks (ORAN). This transition offer an opportunity to remedy some of the technical vulnerabilities that China exploited for Salt Typhoon, but 5G and ORAN and their reliance on cloud services also increase the need for improved cybersecurity.

There is always a cost to regulation and it would be best if decisions on regulation and best practices were informed through a consultative process led by the Office of the National Cyber Director (ONCD). ONCD should work with the telecommunications, cloud, and financial sector companies to identify additional steps and cooperative measures to improve the security and resilience of the national telecommunication infrastructures.

Despite some good work, not enough has been done and the Committee can perform a valuable service by changing this. It can make clear that the FCC is the regulatory agency in charge (and judging from the financial sector experience, regulation is necessary). This Administration has taken several steps to improve cybersecurity and hopefully the next will continue them. Securing telecommunications networks must be a higher priority. A reliable, resilient telecommunications infrastructure is essential for security and economic strength, and this requires minimizes the opportunities for communications collection by adversaries and putting China on notices that its actions will no longer be tolerated without penalty.

China had a comprehensive strategy (to exploit communications) and the United States does not have a comprehensive strategy to defend them. The advantage lies with our opponents and the work of this committee can help change that. Thank you for the opportunity to testify.

Senator LUJÁN. Dr. Lewis, thank you very much. Mr. Sherman, Founder, CEO of Global Cyber Strategies; Nonresident Senior Fellow for the Cyber Statecraft Initiative at the Atlantic Council.

STATEMENT OF JUSTIN SHERMAN, FOUNDER AND CEO, GLOBAL CYBER STRATEGIES; NONRESIDENT SENIOR FELLOW, CYBER STATECRAFT INITIATIVE, ATLANTIC COUNCIL

Mr. SHERMAN. Subcommittee Chair Luján, Ranking Member Moran, and distinguished members of the Subcommittee, thank you for the opportunity to testify today. When most Americans go on the internet, they connect via Wi-Fi on their laptops or cell service on their smartphones.

What often goes unnoticed is a critical piece of the infrastructure behind it, which carries 99 percent of the world's inter-continental Internet traffic, submarine cables. More than 500 submarine cables as thick as a garden hose—and we can thank staff. We have a little snippet of one here.

These carry Internet data between cities, between continents. Dozens more of these cables are on the way. We will easily hit 600, 700 in the next few years. They enable worldwide information flows, commerce, scientific research, military communications, and much more.

Private sector American companies have long played a pivotal role in the financing, construction, laying, and management of submarine cables connected to the United States and between other countries around the world.

Historically, cable investment and ownership from the United States was led by firms such as AT&T and Verizon. Today, the dominant investors and owners of subsea cables are four compa-

nies: Alphabet, Amazon, Meta, and Microsoft. Submarine cables are expensive and complex, and frequently cross many borders.

And so international collaboration is an important and necessary and a largely positive fact of maintaining this global network. It is likewise essential for U.S. companies to continue competitively innovating in this area and playing their part around the world. But, there are serious threats to the security and the safety and the resilience of submarine cables and to U.S. national security that require Government action.

Submarine cables are damaged hundreds of times a year, most often by accident, such as from fishing boats that go close to shore, drag an anchor, and snap this very thin cable that we have here on the table.

Most damage is not intentional, but at the same time, this doesn't fully capture, and industry often fails to appreciate the serious, persistent, and ongoing national security threats to cables across espionage, supply chain compromise, and even physical targeting, especially from the Chinese and Russian governments.

Foreign actors can potentially tap into cables at numerous points along the route, including during repairs or by hacking into remote cable systems. Cutting one cable is thankfully not going to knock out our country's Internet or the world. But damaging a cable could disrupt data flows, could cause traffic to be diverted through points. For example, the Chinese government can intercept and much, much more.

Beyond that, Chinese state owned telecoms are the major investors out of China in these cables. Chinese firms are heavily involved in subsea cable repair. And Russia, meanwhile, is accelerating development of military and intelligence capabilities to surveil and physically target, including cut subsea cables. Incidents in Hawaii, the Baltic Sea, most recently the Red Sea, numerous and growing incidents in the South China Sea and elsewhere underscore these national security threats.

This is why for decades the U.S. has had Team Telecom, an interagency group advising the FCC on national security threats, including to submarine cables. It operated informally for decades, and President Trump formally established Team Telecom as a committee by Executive Order in 2020, which President Biden has kept in place.

Team Telecom has struggled before with a lack of focus on China, with major operational transparency issues, but especially since President Trump's Executive Order and other actions, it has made huge progress in transparency and a focus in particular on the Chinese government's threat to this infrastructure.

Given the risks particularly from Beijing and Moscow, Congress should consider at least four things. One is keep encouraging Team Telecom's transparency. The second is to statutorily authorize Team Telecom to make sure it has the appropriate authorities. The third is to commission a study on China's involvement in and thrust of subsea cables.

And the fourth is to request a lessons learned report from Team Telecom to inform future action. Thank you.

[The prepared statement of Mr. Sherman follows:]

PREPARED STATEMENT OF JUSTIN SHERMAN, FOUNDER AND CEO, GLOBAL CYBER STRATEGIE; NONRESIDENT SENIOR FELLOW, ATLANTIC COUNCIL'S CYBER STATECRAFT INITIATIVE

THE GLOBAL SUBMARINE CABLE NETWORK, CYBERSECURITY AND RESILIENCE, AND RISKS TO U.S. NATIONAL SECURITY

Subcommittee Chair Luján, Ranking Member Thune, and distinguished members of the Subcommittee, I appreciate the opportunity to testify today about the global submarine cable network, cybersecurity and resilience, and protecting our national security from foreign threats.

I am the founder and CEO of Global Cyber Strategies, a Washington, DC-based research and advisory firm, and a nonresident senior fellow at the Atlantic Council's Cyber Statecraft Initiative. I teach, consult, research, and write on cybersecurity, privacy, submarine cable resilience, geopolitical risk, and China and Russia—and am sanctioned by the Russian government. I'm also the author of the forthcoming book *Technology and National Security Collide,* on the history and future of U.S. national security regulations and review programs focused on technology.

Hundreds of submarine cables globally carry 99 percent of Internet traffic between continents. This network's security and resilience are vital to worldwide information flows, commerce, scientific research, military communications, and U.S. national security. Private-sector companies' ability to competitively build and maintain this network is also vital: to economic security, national security, and the US' ability to differentiate its Internet approach from Beijing's model. Simultaneously, companies involved in subsea cables often have major national security blind spots, and foreign actors, particularly the Chinese and Russian governments, pose sophisticated, persistent threats to the global submarine cable network and the security of U.S. data flows. This makes the interagency "Team Telecom" committee critical to protecting U.S. national security, countering Chinese state efforts to compromise the cable supply chain, and helping companies to better understand the risks.

Congress should keep encouraging Team Telecom's transparency; statutorily authorize Team Telecom to ensure it has appropriate authorities and funds; commission a study on Beijing's threats to submarine cables; and request a Team Telecom lessons-learned report to inform future action.

In this written testimony, I describe how:

- Submarine cables globally carry 99 percent of Internet traffic between continents. There are more than 500 submarine cables "in service" worldwide, with dozens more underway.
- Private-sector American companies have long played a pivotal role in the financing, construction, laying, and management of submarine cables connected to the United States and between other countries around the world. Historically, cable investment and ownership from the United States was led by firms such as AT&T and Verizon. Today, the dominant U.S. investors in and owners of submarine cables are Alphabet (Google), Amazon, Meta (Facebook), and Microsoft. They are pouring money into these activities.
- Worldwide, a variety of entities—private-sector, government, and both—are involved in financing, constructing, laying, and managing submarine cables. Not every country has what are typically considered large Internet companies driving subsea cable investments.
- Submarine cable projects are highly expensive, resource intensive, and logistically complex—and frequently cross many borders. International collaboration on financing, constructing, laying, managing, and repairing submarine cables is therefore an important, necessary, and largely positive fact of maintaining and expanding the global network.
- There are many threats to submarine cables: accidents, natural weather events, and persistent, ongoing risks of espionage, sabotage, disruption, and supply chain infiltration from foreign actors, particularly from the Chinese and Russian governments. These threats put at risk the cable network, its cybersecurity and resilience, and U.S. national security.
- More than 80 percent of the hundreds of cable outages and breaks each year are due to fishing and anchoring incidents, and many of the remainder are due to natural weather events. However, industry does not always capture or appreciate the national security risks at play.
- Submarine cables are a potential surveillance goldmine. Foreign actors can potentially tap into cables at multiple points throughout the route, including by hacking into cable-adjacent, internet-connected systems. Malicious actors can

also physically damage cables, and while cutting one cable is not going to knock out the world's internet, damaging or destroying cables in certain regions can disrupt some data flows, have the effect of encouraging traffic to flow via other means, force repair ships to be sent out, and more.

- Recent cable cuts in the Baltic Sea by a Russia-departing Chinese vessel, an attempted cyber operation against a cable-linked system in Hawaii, accidental cable cuts in the Red Sea due to the Houthis sinking a ship, and suspicious Chinese government and company activity near Asia-Pacific cables, among others, speak to these security risks.
- Chinese state-owned telecoms China Mobile, China Telecom, and China Unicom are also major Chinese investors in subsea cables, and Russia's Main Directorate for Deep Sea Research is accelerating development of undersea surveillance and targeting capabilities.
- For decades, an informal interagency group, dubbed "Team Telecom," advised the Federal Communications Commission on the national security risks to infrastructure like submarine cables. President Trump formally established Team Telecom as an Executive Branch committee with E.O. 13913 in 2020, which President Biden kept in place. Today, Team Telecom plays a vital role in advising the FCC on the national security risks to cables.
- Recent Team Telecom decisions informed the FCC's effective expulsion of China Telecom from the United States in 2021 and mitigations for a proposed cable that would have had landing stations in California and in Hong Kong. Team Telecom's bipartisan-supported work must continue—and is even more essential given threats from Beijing and Moscow.

The Global Submarine Cable Network

Submarine cables globally carry 99 percent of Internet traffic between continents.[1] These cables vary in thickness from about one centimeter to about 20 centimeters, about the thickness of a garden hose, and contain a hair-thin inner fiber than transmits Internet data across the cable, whether e-mails, videos, or sensitive documents.[2] Fiber-optic cables are faster, cheaper, and generally more reliable than satellites.[3] (In fact, while satellite communications have important uses and value-adds in specific, defined scenarios, it's on the whole not even close in speed, bandwidth, and reliability, among other metrics.)[4] Companies and other entities build different components of these cables, assemble them, and lay them across the ocean floor to connect disparate masses, like South America and Europe. Every undersea cable has at least two "landing points," or the locations where the cable meets the shoreline. Facilities at these landing points can provide multiple functions, including terminating an international cable, supplying power to the cable, and acting as a point of domestic and/or international connection.[5] The owner of a submarine cable may not be the same entity as the owner of the landing station, just as a company or government agency that invests in a submarine cable's construction may not be the same entity managing its operation once live.

As of September 2024, according to TeleGeography, there are 532 cable systems "in service" (actively operating) around the world—with another 77 cable systems

---

[1] This figure was broken down well by Alan Mauldin for TeleGeography: Alan Mauldin, "Do Submarine Cables Account For Over 99 percent of Intercontinental Data Traffic?" TeleGeography.com, May 4, 2023, *https://blog.telegeography.com/2023-mythbusting-part-3.*

[2] This and other portions of this testimony point to: Justin Sherman, *Cyber Defense Across the Ocean Floor: The Geopolitics of Submarine Cable Security* (Washington, D.C.: Atlantic Council, September 2021), *https://www.atlanticcouncil.org/in-depth-research-reports/report/cyber-defense-across-the-ocean-floor-the-geopolitics-of-submarine-cable-security/,* 4. As noted in the report, on the page cited, thanks as well to experts such as Bill Woodcock for discussion of these points at the time of the 2021 report's authoring.

[3] For some good explainers, see, *e.g.,* Jeff Fraleigh, "Fiber vs. Satellite Internet: Why Fiber Optics Lead the Future of High-Speed Connectivity), ETI Software, April 24, 2024, *https://etisoftware.com/resources/blog/fiber-vs-satellite-why-fiber-optics-lead-the-future-of-high-speed-connectivity/;* Airband, "Fibre optic vs. satellite: What's the difference?" Airband.co.uk, accessed December 3, 2024, *https://www.airband.co.uk/fibre-optic-vs-satellite-difference/.*

[4] Of course, other nuances exist too, such as how these means of communications transmission can interact.

[5] United Nations International Telecommunication Union, "Cable Landing Stations: Building, Structuring, Negotiating and Risk," 2, 2017, *https://www.itu.int/en/ITU-D/Regional-Presence/AsiaPacific/SiteAssets/Pages/Events/2017/Submarine%20Cable/submarine-cables-for-Pacific-Islands-Countries/Cable%20Landing%20Stations%20SNCC.pdf,* 2.

planned and on the way.[6] This number is continually growing, due to companies' investments, and for some countries, governments' investments, in the infrastructure; increased digital connectivity; growing consumer and business use of online services with greater data demands; and new data center demands driven by the explosion of cloud service provider infrastructure and the explosion of companies and other organizations training and deploying artificial intelligence (AI) and machine learning (ML) applications, among others.[7] Even systems like 5G telecommunications networks will likely increase submarine cable demands in some form or another, as the mobile telecom networks send more and more data to, and retrieve more and more data from, Internet data servers and cloud infrastructure located around the world. All to say, submarine cables are critical to global communication flows—and the modern Internet as we know it would not exist without this subsea cable network.

Private-sector American companies have long played a pivotal role in the financing, construction, laying, and management of submarine cables connected to the United States and between other countries around the world.[8] Historically, cable investment and ownership from the United States was led by firms such as AT&T and Verizon. Today, the dominant U.S. investors in and owners of submarine cables are Alphabet (Google), Amazon, Meta (Facebook), and Microsoft.[9] These four companies have invested in and bought major capacity on dozens of subsea cables around the world in recent years,[10] making clear that they do not just have outsized influence in areas such as cloud computing, social media, e-commerce, and search but physical Internet infrastructure under the ocean. Alphabet, Amazon, Meta, and Microsoft's investment ramp-up has been tremendous. In roughly a decade, the content providers (such as Meta and Alphabet) went from consuming 6.3 percent of total international cable capacity to 69 percent of total international cable capacity, and these four companies went from investing in only one long-distance subsea cable to investing in dozens and dozens.[11]

Looking forward, these four companies are going to spend even more money on subsea cables and increase their influence over the global infrastructure even further in the next decade. Just several days before this hearing, for instance, *TechCrunch* reported that Meta is planning to build a new subsea cable more than 40,000 kilometers (~24,855 miles) long that could require more than $10 billion in investment—with Meta to be the cable's sole owner and user.[12]

Worldwide, a variety of entities are involved in financing, constructing, laying, and managing submarine cables. As of September 2021, for example, 65 percent of submarine cables had a single owner and 33 percent had multiple owners (and 2 percent without readily accessible ownership data).[13] Approximately 59 percent of cables had only private owners, 19 percent had all state owners, and 19 percent had both private and state owners (and 3 percent without readily accessible data).[14] The organizations involved in different elements of the submarine cable supply chain, including financing, are wide-ranging: from content providers such as Google; to large, traditional telecommunications companies like Vodafone, Airtel, and Algar Telecom; to investment firms like SoftBank; to subsea cable manufacturers like SubCom, Alcatel, and Huawei Marine; to state-owned entities such as Djibouti Telecom,

---

[6] Lane Burdette, "How Many Submarine Cables Are There, Anyway?" TeleGeography.com, September 9, 2024, *https://blog.telegeography.com/how-many-submarine-cables-are-there-anyway*.

[7] See, *e.g.,* Ibid.; Emma Chervek, "Ciena CTO talks subsea cables, data center efficiency vs. demand," SDXCentral.com, November 2, 2023, *https://www.sdxcentral.com/articles/interview/ciena-cto-talks-subsea-cables-data-center-efficiency-vs-demand/2023/11/;* Diana Goovaerts, "Thanks to cloud, hyperscalers are changing the way subsea cables make landfall," Fierce-Network.com, September 26, 2023, *https://www.fierce-network.com/data-center/hyperscalers-are-changing-way-subsea-cables-make-landfall*.

[8] For an excellent discussion and analysis of some of this history, see: Nicole Starosielski, *The Undersea Network* (Durham: Duke University Press, 2015).

[9] See, *e.g.,* Global Data, "Hyperscalers turning the tide in subsea cables," *Yahoo! Finance,* December 6, 2024, *https://finance.yahoo.com/news/hyperscalers-turning-tide-subsea-cables-150705832.html*.

[10] Alan Mauldin, "A (Refreshed) List of Content Providers' Submarine Cable Holdings," TeleGeography.com, June 27, 2024, *https://blog.telegeography.com/telegeography-content-providers-submarine-cable-holdings-list-new*.

[11] Andrew Blum and Carey Baraka, "Sea change," Rest of World, May 10, 2022, *https://restofworld.org/2022/google-meta-underwater-cables/,* citing TeleGeography data; Global Data, "Hyperscalers turning the tide in subsea cables."

[12] Ingrid Lunden, "Meta plans to build a $10B subsea cable spanning the world, sources say," *TechCrunch,* November 29, 2024, *https://techcrunch.com/2024/11/29/meta-plans-to-build-a-10b-subsea-cable-spanning-the-world-sources-say/*.

[13] Sherman, *Cyber Defense Across the Ocean Floor,* 7.

[14] Ibid., 9.

Instituto Costarricense de Electricidad, and the Telecommunication Infrastructure Company of Iran; and many more. Not every country has what are typically considered large Internet and platform companies driving submarine cable investments.

Submarine cable projects are highly expensive, resource intensive, and logistically complex. It is worth reemphasizing that it has been and will likely remain a largely positive—and necessary—fact that so many different organizations around the world are able to collaborate on continuing to build out the global submarine cable network to meet resiliency challenges and deliver speed, bandwidth, and so on. Likewise, the U.S. private sector has played a significant role in helping to build out the global subsea cable network, and it is essential for them to be able to continue doing so. At the same time, however, there are considerable risks to submarine cables—and, related, to national security—that demand policymaking and other involvement from the U.S. government.

Risks to Submarine Cables

There are many threats and risks to the global submarine cable network. These threats span accidents (responsible for most damage to subsea cables each year), natural weather events, and persistent, ongoing risks of espionage, sabotage, disruption, and supply chain infiltration from foreign actors, particularly from the Chinese and Russian governments. Such threats, particularly from Beijing and Moscow, put at risk not just the global cable network and its cybersecurity and resilience—but U.S. national security.

Most of the publicly documented instances of damage and disruption to submarine cables around the world are due to accidents, such as boats moving close to a shoreline, not properly checking their maps for cables in the area, and then accidentally ripping up or damaging a cable with a dragging anchor. Other incidents of damage and disruption, though far less frequent than accidents, are caused by natural weather events, such as underwater earthquakes, underwater volcanic eruptions, and abrasion and erosion that damage cables and require repairs.[15] In May 2024, for example, the International Cable Protection Committee said that more than 80 percent of all cable outages and breaks are due to fishing and anchoring incidents.[16] There are typically hundreds of incidents of damage to submarine cables reported every year (lately, around 150–200 annually),[17] and most of those incidents—as with the vast majority of all damage to subsea cables since 1959—fall into the category of accidents caused in shallow water.[18] It is important to recognize this data for at least two reasons: companies and governments need to keep ensuring robust, rapid repairs to maintain the global subsea cable network's resilience; and the U.S. government needs to ensure its understanding of the cable landscape incorporates this data and does not get distracted by occasional media stories on scenarios such as sharks attacking subsea cables.[19]

There are also routine risks to submarine cables that result from criminals and other malicious actors looking to exploit vulnerabilities in technological systems and take advantage of companies with insufficient investments in basic cybersecurity best-practices, such as comprehensive multifactor authentication, robust encryption, access controls, audits, continuous monitoring, supply chain security assessments, vendor and contractor controls, meaningful empowerment and resourcing of company decision-makers and staff focused on cybersecurity, and so on.

At the same time, however, the data on ships accidentally dragging their anchors and telecoms getting hacked by criminals does not adequately capture another important risk set: risks from sophisticated foreign threat actors, particularly the Chinese and Russian governments.

---

[15] Mike Clare, *Submarine Cable Protection and the Environment* (Portsmouth: International Cable Protection Committee, March 2021), *https://www.iscpc.org/publications/submarine-cable-protection-and-the-environment/ICPC_Public_EU_March%202021.pdf,* 4–5.

[16] Graham Evans, "Report of the International Cable Protection Committee," Presentation for International Hydrographic Organization: Hydrographic Services and Standards Committee, May 27–31, 2024, *https://iho.int/uploads/user/Services%20and%20Standards/HSSC/HSSC16/HSSC16_2024_07.10A_EN_ICPC%20activities%20 affecting%20HSSC.pdf,* 5.

[17] International Telecommunication Union, "Launch of international advisory body to support resilience of submarine telecom cables," ITU.int, November 29, 2024, *https://www.itu.int/en/mediacentre/Pages/PR-2024-11-29-advisory-body-submarine-cable-resilience.aspx.*

[18] Clare, *Submarine Cable Protection and the Environment,* 4–5.

[19] See, *e.g.,* Peter H. Lewis, "Phone Company Finds Sharks Cutting In," *The New York Times,* June 11, 1987, Section A, Page 1; Tim Starks, "Sharks, earthquakes and cyberattacks: The threats to undersea cables," *The Washington Post,* June 28, 2023, *https://www.washingtonpost.com/politics/2023/06/28/sharks-earthquakes-cyberattacks-threats-undersea-cables/.* See also: "Sharks are not the Nemesis of the Internet—ICPC Findings," International Cable Protection Committee, July 1, 2015.

Espionage: Submarine cables are a potential surveillance goldmine. For well over a century, nations have used their access to cables to conduct espionage, such as when British intelligence, in the late nineteenth century, used an international hub of telegram cables in Porthcurno to gain eavesdropping advantage.[20] Today's submarine cables carry enormous volumes of data—as mentioned, 99 percent of all intercontinental Internet traffic in the world. Foreign actors can potentially tap into these cables at multiple points throughout the cable route (*e.g.,* as the cable is exposed above water when coming up on the shoreline, at landing stations, by putting a cable landing point in a place under state control) and in the cable supply chain (*e.g.,* during installation, repairs), including by hacking into the remote, internet-connected software systems (and the other systems around them) that companies increasingly use to manage submarine cable networks.[21] These latter systems can increase the cybersecurity attack surface for cable networks. The many actors involved in cable financing, construction, laying, management, and repair also create opportunities for governments and government-linked actors to exert influence over submarine cables and the broader submarine cable network, such as by legally requiring or extralegally coercing companies or individuals at those companies to assist with government surveillance operations.

Damage and Disruption: Malicious actors could also damage cables with the intent of disrupting traffic flows or blacking out subsea cable traffic to an area. To be clear, in most cases, chopping a subsea cable is not going to sever an entire country's internet. (There are some narrow cases where this is possible, such as when a devastating volcanic eruption in 2022 off the coast of Tonga damaged a submarine cable and knocked out the country's Internet connectivity.)[22] Nor is one cable cut going to bring down the global Internet and knock the world's communications offline. But damaging or destroying cables in certain regions can disrupt some data flows, have the effect of encouraging traffic to flow via other means (*e.g.,* through a new point from which traffic can be intercepted), force repair ships to be sent out, and much more. There is much discussion in the submarine cable space, and especially among academics and industry experts working at the United Nations and other bodies, of norms—including norms of what governments will and will not do to submarine cables. While these are important discussions, including insofar as they encourage dialogue between countries, it is impractical to think that in a wartime, armed conflict, or crisis scenario, a country with sophisticated military and intelligence capabilities would not be willing to violate what some consider a norm and attack submarine cable infrastructure. (Of course, some would hold this norm does not even exist now.) This is especially the case when considering the normative postures of governments in Beijing and Moscow.

Strategic Network-Shaping: At a higher level, cable construction and maintenance can provide strategic value to governments. Many private-sector and government actors, frequently in collaboration, are involved in important submarine cable construction activities. Building more cables in and of itself, in a sense, arguably increases the resilience of the global Internet in absolutist terms: there are new routes over which data can travel in the event of failure. But choosing where, when, and how to build cables is also a way to shape where global Internet traffic is routed.[23] Changes to traffic routing patterns generate profits for companies and can move new volumes of traffic through different countries' borders—which can enable data interception and the development of technological dependence.[24] This is an important consideration as authoritarian governments increasingly work to reshape the internet's physical topology (structure) and digital behavior by exerting control over companies.

---

[20] Ben Buchanan, *The Hacker and the State: Cyber Attacks and the New Normal of Geopolitics* (Cambridge: Harvard University Press, 2020), 16–17.

[21] See, *e.g.,* DJ Pangburn, "Wiretapping Undersea Fiber Optics Is Easy: It's Just a Matter of Money," *VICE,* July 22, 2013, *https://www.vice.com/en/article/undersea-cable-surveillance-is-easy-its-just-a-matter-of-money/;* Jonathan E. Hillman, *Securing the Subsea Network: A Primer for Policymakers* (Washington, D.C.: Center for Strategic & International Studies, March 2021), *https://www.csis.org/analysis/securing-subsea-network-primer-policymakers,* 10; Sherman, *Cyber Defense Across the Ocean Floor,* 17.

[22] Ian Ralby and Justin Sherman, "Tonga's Devastating Volcanic Eruption Has Left the Island Without Internet," *Slate,* January 21, 2022, *https://slate.com/technology/2022/01/tonga-volcano-internet-underseas-cables.html.*

[23] This is reflected in the fact that "traffic that appears to be traveling via separate network paths could potentially be relying on the same physical resource." Zachary S. Bischof, Romain Fontugne, and Fabián E. Bustamante, "Untangling the world-wide mesh of undersea cables," *HotNets '18: Proceedings of the 17th ACM Workshop on Hot Topics in Networks* (November 2018): 78–84, *https://dl.acm.org/doi/abs/10.1145/3286062.3286074,* 81.

[24] Sherman, *Cyber Defense Across the Ocean Floor,* 10.

For example, among other events that underscore national security risks to submarine cables:

- *Cable Cuts in Baltic Sea:* In November 2024, a Chinese bulk carrier, the Yi Peng 3, dragged its anchor along the Baltic Sea's seabed for over 100 miles and severed two undersea cables: one between Sweden and Lithuania and another between Finland and Germany.[25] When the ship traveled through the Baltic Sea, it also crossed over four gas and oil pipelines, a power line, and another subsea cable under construction.[26] As others have already noted, it is extremely unlikely a ship would accidentally have an anchor drag for 100 miles without immediately noticing the impacts on speed. Germany's defense minister has said the damage appears to be sabotage, but did not yet specify any further evidence.[27] Investigations are reportedly still unfolding in Europe, and complicating the situation further is that the ship originally departed from Vistino, Russia.[28] (As Lithuania's Foreign Minister commented, this incident, to him suspiciously, follows a Chinese-registered vessel damaging two subsea cables in the Baltic Sea in October 2023.)[29]
- *Attempted Cyber Attack or Intrusion in Hawaii:* In 2022, agents at the Department of Homeland Security's Homeland Security Investigations arm said they disrupted what they described as a cyber attack on a critical undersea cable linking Hawaii and the Pacific.[30] DHS said "an international hacking group" had carried out a "significant breach involving a private company's servers associated with an undersea cable" and that "HSI agents and international law enforcement partners in several countries were able to make an arrest"[31]—suggesting a threat actor or actors based outside of the United States.
- *Damages in South China Sea:* Cables around Taiwan have been cut over two dozen times in the last five years, typically due to Chinese vessels, or vessels that are suspected to be from China, severing the cables.[32] Chinese sand dredgers have reportedly accounted for at least 10 of these breaks.[33] Some experts, in response, have noted both the frequency of accidental submarine cable damage around the world—and others the strangeness of many similar, repeat incidents in a highly monitored and contested zone of the world.
- *Chinese Coast Guard near Vietnam:* The *Washington Post* reported in October 2024 that, in April 2024, a Vietnamese naval vessel was escorting a crew aboard a private subsea cable ship within Vietnam's 200-mile exclusive economic zone, when a Chinese coast guard vessel confronted the ships. (As noted in the story, this is hundreds of miles from the Chinese mainland.) Then, "the Chinese vessel came within one mile of the repair ship and demanded over radio to know the nature of the ship's activities, according to executives at the cable company as well as photos of the encounter between the two vessels and

---

[25] Bojan Pancevski, "Chinese Ship's Crew Suspected of Deliberately Dragging Anchor for 100 Miles to Cut Baltic Cables," *The Wall Street Journal,* November 29, 2024, *https://www.wsj.com/world/europe/chinese-ship-suspected-of-deliberately-dragging-anchor-for-100-miles-to-cut-baltic-cables-395f65d1;* Bojan Pancevski, "Russia Suspected as Baltic Undersea Cables Cut in Apparent Sabotage," *The Wall Street Journal,* November 20, 2024, *https://www.wsj.com/world/europe/russia-suspected-as-baltic-undersea-cables-cut-in-apparent-sabotage-801cb392.*

[26] Sophie Tanno, "Sweden asks China to cooperate in Baltic Sea cable investigation," CNN, November 29, 2024, *https://www.cnn.com/2024/11/29/europe/sweden-china-baltic-sea-cable-intl/index.html.*

[27] Shweta Sharma, "Sweden formally asks China to cooperate with investigations into undersea cables damage," *The Independent,* November 30, 2024, *https://www.the-independent.com/asia/china/sweden-china-cable-damage-baltic-sea-b2656390.html.*

[28] Tanno, "Sweden asks China to cooperate in Baltic Sea cable investigation."

[29] Sophia Besch and Erik Brown, "A Chinese-Fallged Ship Cut Baltic Sea Internet Cables. This Time, Europe Was More Prepared," Carnegie Endowment for International Peace, December 3, 2024, *https://carnegieendowment.org/emissary/2024/12/baltic-sea-internet-cable-cut-europe-nato-security?lang=en.*

[30] "Federal agents disrupted cyberattack targeting phone, Internet infrastructure on Oahu," Hawaii News Now, April 12, 2022, *https://www.hawaiinewsnow.com/2022/04/13/hsi-agents-honolulu-disrupted-cyberattack-undersea-cable-critical-telecommunications/.*

[31] AJ Vicens, "DHS investigators say they foiled cyberattack on undersea Internet cable in Hawaii," *CyberScoop,* April 13, 2022, *https://cyberscoop.com/undersea-cable-operator-hacked-hawaii/.*

[32] Huizhong Wu and Johnson Lai, "Taiwan suspects Chinese ships cut islands' Internet cables," Associated Press, April 18, 2023, *https://apnews.com/article/matsu-taiwan-internet-cables-cut-china-65f10f5f73a346fa788436366d7a7c70.*

[33] Rachel Cheung, 'A Warning Sign': Chinese Ships Accused of Cutting Off Internet to a Taiwanese Island," *VICE,* March 17, 2023, *https://www.vice.com/en/article/taiwan-internet-cables-matsu-china/.*

text messages from the repair crew on the day of the incident . . . After the Vietnamese naval ship withdrew several miles away, the Chinese ship spent a day circling the repair vessel, then left it, and the crew finished the job." The company's head of maintenance said it was clearly a "show of strength" by the Chinese coast guard ship.[34]

- *Russia's GUGI:* US officials told CNN in October 2024 that Russia is building up its fleet of surface ships, submarines, and naval drones through the General Staff Main Directorate for Deep Sea Research (GUGI). One official expressed concern "about heightened Russian naval activity worldwide" and that "Russia's decision calculus for damaging U.S. and allied undersea critical infrastructure may be changing," which could leverage the capabilities mainly being developed through GUGI.[35] The GUGI works independently from Russian naval command and answers directly to the Ministry of Defense, as an intelligence and special mission organization.[36] It operates specialized submarines that can operate in extreme depths (*i.e.,* able to reach undersea cables), surface vessels that collect intelligence, and remotely operated and autonomous underwater vehicles hosted on those surface vessels.[37] For instance, in November 2024, the Russian ship Yantar entered Irish-controlled waters and moved around an area with critical energy pipelines and submarine cables;[38] Yantar is one of the surface fleet ships, with intelligence-gathering capabilities, operated by the GUGI.[39] This is one of several such incidents in recent years, as analysts of the Russian military warn about Moscow's increased emphasis on its submarine fleet.[40]
- *Cable Cuts Amid Houthi Red Sea Conflict:* As conflict erupted in the Red Sea in March 2024, three submarine cables were cut. There was speculation at first that the Houthi rebels deliberately sabotaged the cables,[41] with the supposed means unspecified, but the White House National Security Council subsequently said that the three cables were likely severed after the Houthis attacked a ship, it started sinking, and its anchor caught the cables.[42] The incident increased the risk of installing new cables in the Red Sea and especially of ships going out to repair the ones that were severed as the conflict continued.[43]
- *Huawei Repairing Subsea Cables:* Huawei Marine Networks, part of Chinese telecom Huawei, had by October 2020 built or repaired (by one estimate) rough-

---

[34] Rebecca Tan, "Escalating contest over South China Sea disrupts international cable system," *The Washington Post,* October 3, 2024, *https://www.washingtonpost.com/world/2024/10/03/south-china-sea-underwater-cables/*.

[35] Jim Sciutto, "Exclusive: U.S. sees increasing risk of Russian 'sabotage' of key undersea cables by secretive military unit," CNN, September 6, 2024, *https://www.cnn.com/2024/09/06/politics/us-sees-increasing-risk-of-russian-sabotage-undersea-cables/index.html.*

[36] Michael Kofman, "Fire aboard AS–31 Losharik: Brief Overview," RussianMilitary Analysis.wordpress.com, July 3, 2019, *https://russianmilitaryanalysis.wordpress.com/2019/07/03/fire-aboard-as-31-losharik-brief-overview/*.

[37] Sidharth Kaushal, "Stalking the Seabed: How Russia Targets Critical Undersea Infrastructure," Royal United Services Institute, May 25, 2023, *https://rusi.org/explore-our-research/publications/commentary/stalking-seabed-how-russia-targets-critical-undersea-infrastructure.*

[38] Lisa O'Carroll, "Russian spy ship escorted away from area with critical cables in Irish Sea," *The Guardian,* November 16, 2024, *https://www.theguardian.com/world/2024/nov/16/russian-spy-ship-escorted-away-from-internet-cables-in-irish-sea.*

[39] Kaushal, "Stalking the Seabed"; H. I. Sutton, "Russian Spy Ship Yantar Loitering Near Trans-Atlantic Internet Cables," Naval News, August 19, 2021, *https://www.navalnews.com/naval-news/2021/08/russian-spy-ship-yantar-loitering-near-trans-atlantic-internet-cables/*.

[40] Andrii Ryzhenko, "Russia Looks to Target Achilles' Heel of Western Economies on Ocean Floor," Jamestown, September 17, 2024, *https://web.archive.org/web/20240918081949/https://jamestown.org/program/russia-looks-to-target-achilles-heel-of-western-economies-on-ocean-floor/;* Mark Galeotti, "Bear underwater: Russia's undersea capabilities," Council on Geostrategy, June 26, 2023, *https://www.geostrategy.org.uk/britains-world/bear-underwater-russias-undersea-capabilities/;* Ellie Cook, "NATO Has a Russian Submarine Problem," *Newsweek,* May 13, 2023, *https://www.newsweek.com/nato-russia-submarines-nuclear-deterrent-ukraine-arctic-pacific-fleet-kola-peninsula-baltic-1798368.*

[41] Jon Gambrell, "3 Red Sea data cables cut as Houthis launch more attacks in the vital waterway," Associated Press, March 4, 2024, *https://apnews.com/article/red-sea-undersea-cables-yemen-houthi-rebels-attacks-b53051f61a41bd6b357860bbf0b0860a.*

[42] Eleanor Watson, "Ship sunk by Houthis likely responsible for damaging 3 telecommunications cables under Red Sea," CBS News, March 6, 2024, *https://www.cbsnews.com/news/houthis-ship-cutting-red-sea-telecommunications-cables/*.

[43] Nadine Hawkins, "The underwater digital super highway," CapacityMedia.com, March 11, 2024, *https://www.capacitymedia.com/article/ 2cxmm34wcyeqqxqoo54w0/big-interview/the-underwater-digtal-super-highway;* Tim Stronge, "What We Know (And Don't) About Multiple Cable Faults in the Red Sea," TeleGeography, March 5, 2024, *https://blog.telegeography.com/what-we-know-and-dont-about-multiple-cable-faults-in-the-red-sea.*

ly 25 percent of the world's submarine cables.[44] After the Trump administration issued sanctions on Huawei, many companies stopped working with Huawei Marine.[45] In 2020, the UK company Global Marine Group sold its 30 percent stake in Huawei Marine to the Hengtong Group, China's largest power and fiber optic cable manufacturer.[46] The Hengtong Group then changed Huawei Marine's name to HMN Technologies Co., Ltd., or HMN Tech (ostensibly, HMN as an abbreviation of Huawei Marine Networks),[47] though it has neither helped the brand nor boosted its economic position. Today, Huawei Marine plays a seriously diminished role in submarine cable repairs around the world compared to its market stature just a few years ago.[48]

These are just some examples of the reasons for national security concern. And analyzing the potential threats to the network, whether accidental or intentional, and the available risk mitigations and incident responses are still critical to submarine cable security in any case.

Zooming In: National Security Risks from China and Russia

The Chinese government is highly active in the submarine cable arena through a variety of companies. Some of the top Chinese investors in and operators of submarine cables are China Mobile, China Telecom, and China Unicom. For example:

- The *Asia Direct Cable (ADC)* is expected to be ready for service in Q4 2024. It has landing points in China, Japan, the Philippines, Singapore, Thailand, and Vietnam. Its owners include China Telecom and China Unicom.[49]
- The *Asia Pacific Gateway (APG)* is active and has landing points in China, Japan, Malaysia, Singapore, South Korea, Taiwan, Thailand, and Vietnam. Its owners include China Mobile, China Telecom, and China Unicom.[50]
- The *SeaMeWe-5* is active and has landing points in Bangladesh, Djibouti, Egypt, France, Indonesia, Italy, Malaysia, Myanmar, Oman, Pakistan, Saudi Arabia, Singapore, Sri Lanka, Turkey, the UAE, and Yemen. Its owners include China Mobile, China Telecom, and China Unicom.[51]
- The *New Cross Pacific (NCP)* cable system is active and has landing points in China, Japan, South Korea, Taiwan, and the United States. Its owners include China Mobile, China Telecom, and China Unicom.[52]

China Mobile, China Telecom, and China Unicom are all state-owned telecommunications companies. They began significantly increasing their investments in submarine cables in 2021.[53] This is a potential national security risk, as they are directly owned by the Chinese government and therefore subject to Chinese government decisions about cable projects—including the possibility of legal and extralegal demands and pressures to assist with government objectives, such as supply chain compromise or espionage. (The FCC, underscoring these risks, denied a China Mobile telecommunication services license application in 2019,[54] revoked China

---

[44] U.S. Federal Communications Commission. *Process Reform for Executive Branch Review of Certain FCC Applications and Petitions Involving Foreign Ownership.* FCC–20–133. Washington, D.C.: Federal Communications Commission, October 2020. *https://www.fcc.gov/document/fcc-improves-transparency-and-timeliness-foreign-ownership-review.* 82.

[45] Anna Gross *et al.,* "How the U.S. is pushing China out of the internet's plumbing," *Financial Times,* June 13, 2023, *https://ig.ft.com/subsea-cables/*.

[46] Global Marine Group's subsidiary Global Marine Systems Limited established Huawei Marine Networks as a joint venture with Huawei Technology in Tianjin, China, in 2008. Winston Qiu, "Global Marine Group Fully Divests Stake in Huawei Marine Networks," Submarine Networks.com, June 6, 2020, *https://www.submarinenetworks.com/en/?view=article&id=1334:global-marine-*.

[47] HMN Tech, "Huawei Marine Networks Rebrands as HMN Technologies," HMNTech.com, November 3, 2020, *https://www.hmntech.com/enPressReleases/37764.jhtml.*

[48] Conversations with submarine cable industry experts.

[49] "Asia Direct Cable (ADC)," submarinecablemap.com, accessed December 4, 2024, *https://www.submarinecablemap.com/submarine-cable/asia-direct-cable-adc.*

[50] "Asia Pacific Gateway (APG)," submarinecablemap.com, accessed December 4, 2024, *https://www.submarinecablemap.com/submarine-cable/asia-pacific-gateway-apg.*

[51] "SeaMeWe-5," submarinecablemap.com, accessed December 4, 2024, *https://www.submarinecablemap.com/submarine-cable/seamewe-5.*

[52] "New Cross Pacific (NCP) Cable System," submarinecablemap.com, accessed December 6, 2024, *https://www.submarinecablemap.com/submarine-cable/new-cross-pacific-ncp-cable-system.*

[53] Sherman, *Cyber Defense Across the Ocean Floor,* 13.

[54] U.S. Federal Communications Commission. *FCC Denies China Mobile Telecom Services Application.* FCC–19-38. Washington, D.C.: Federal Communications Commission, May 2019. *https://www.fcc.gov/document/fcc-denies-china-mobile-telecom-services-application-0.*

Telecom Americas' Section 214 authority in 2021,[55] revoked China Unicom Americas' telecom services authority in 2022,[56] and added China Telecom Americas and China Mobile to the covered list in 2022.)[57] In fact, many Chinese investors in submarine cables globally are state-owned or state-controlled, widening the same national security risk. For example, these firms include:

Entity	Relationship to Chinese Government
China Mobile	State-owned
China Telecom	State-owned
China Unicom	State-owned
CITIC Telecom International	State-controlled
CTM	State-controlled

It is additionally possible that the Chinese government legally compels or extralegally coerces a privately owned Chinese company to assist in these activities—though the risk assessment in those scenarios can be complex and depend on a variety of case-specific factors and insights. And it is also possible that organizations that do not appear to be operating out of China, such as certain consortium groups, are in fact subject to Chinese government control. This is not to feed conspiracy theories, but to point out cases such as the National Grid Corporation of the Philippines: nominally, it is only partly owned by a Chinese state-owned electrical company, but CNN reported in 2019 on an internal Filipino government report stating that the Corporation was in fact "under the full control" of the Chinese government and vulnerable to disruption.[58] The National Grid Corporation of the Philippines is the sole owner of an undersea cable connecting two parts of the country—a cable that is also supplied by HMN Tech, previously known as Huawei Marine.[59]

Beyond financing, construction, and management, China's involvement in submarine cable repairs is also a national security concern. Enormous volumes of data traverse submarine cables every day. It is difficult to imagine a scenario in which the Chinese government, with its legal and extralegal ability to coerce technology companies, would not consider placing specific pressure on submarine cable repair companies—or even an individual or individuals at those companies—to assist with tapping into or otherwise compromising that infrastructure for its own advantage.

The U.S. has, in many ways, at least one success story in mitigating this national security risk: the case of Huawei Marine, aka HMN Tech. Huawei Marine went, in just a few years, from repairing or building roughly 25 percent of the world's subsea cables to a significantly diminished role in the global network. However, Huawei Marine aka HMN Tech does not stand alone. Other Chinese firms such as S.B. Submarine Systems (SBSS) are active in submarine cable repair. SBSS has repaired cables whose owners have included U.S. companies, and its vessels have reportedly, and highly unusually, turned off their transponders at sea and hidden their locations from radio and satellite tracking services, including when traveling and making stops around Singapore, Hong Kong, the Yellow Sea, and even Taiwan.[60] Chinese cable repair ship companies such as SBSS present serious national security

---

[55] U.S. Federal Communications Commission. *China Telecom Americas Order on Revocation and Termination*. FCC–21–114. Washington, D.C.: Federal Communications Commission, November 2021. *https://www.fcc.gov/document/china-telecom-americas-order-revocation-and-termination.*

[56] U.S. Federal Communications Commission. *China Unicom Americas Order on Revocation.* FCC–22–9. Washington, D.C.: Federal Communications Commission, February 2022. *https://www.fcc.gov/document/china-unicom-americas-order-revocation.*

[57] U.S. Federal Communications Commission. *Announcement of Additions to the Covered List.* DA–22–320. Washington, D.C.: Federal Communications Commission, March 2022. *https://www.fcc.gov/document/announcement-additions-covered-list.*

[58] James Griffiths, "China can shut off the Philippines' power grid at any time, leaked report warns," CNN, November 26, 2019, *https://edition.cnn.com/2019/11/25/asia/philippines-china-power-grid-intl-hnk/index.html;* CNN Philippines Staff, "Carpio: Chinese 'control' of national power grid a cause for concern," CNN, November 26, 2019, *https://www.cnnphilippines.com/news/2019/11/26/Antonio-Carpio-Chinese-control-NGCP.html.*

[59] "Sorsogon-Samar Submarine Fiber Optical Interconnection Project (SSSFOIP)," submarinecablemap.com, accessed December 7, 2024, *https://www.submarinecablemap.com/submarine-cable/sorsogon-samar-submarine-fiber-optical-interconnection-project-sssfoip.*

[60] Dustin Volz *et al.,* "U.S. Fears Undersea Cables Are Vulnerable to Espionage From Chinese Repair Ships," *The Wall Street Journal,* May 19, 2024, *https://www.wsj.com/politics/national-security/china-internet-cables-repair-ships-93fd6320.* See also a comment in: Daniel F. Runde, Erin L. Murphy, and Thomas Bryja, *Safeguarding Subsea Cables: Protecting Cyber Infrastructure amid Great Power Competition* (Washington, D.C.: Center for Strategic and International Studies, August 2024), *https://www.csis.org/analysis/safeguarding-subsea-cables-protecting-cyber-infrastructure-amid-great-power-competition.*

risks that need to be assessed and considered, including by companies and partners operating in the Asia-Pacific region.

The Russian government, for its part, is not as active as the Chinese government in financing and constructing submarine cables globally. But the Russian government has clearly demonstrated a pattern of thinking about how to physically target and seize control of Internet and technological infrastructure to further control over a population (*e.g.,* as it does at home) and to advance its security objectives. Even compared to the views held by the Russian security services in the 1990s and early 2000s, and to the conspiratorialism and concern that cemented in the Kremlin in the late 2000s and early 2010s, the Kremlin has an increasingly paranoid, securitized view of the global Internet and of technology.[61] This, coupled with Moscow's aforementioned investments in GUGI, suggests a troubling possibility of Russian government willingness to target submarine cable and other undersea infrastructure for intelligence or military purposes. In that vein, the U.S. intelligence community said in its annual 2024 threat assessment that "Russia maintains its ability to target critical infrastructure, including underwater cables and industrial control systems, in the United States as well as in allied and partner countries."[62] Its annual threat assessment from the year prior noted Russia not just maintains these capabilities but "is particularly focused on improving its ability" to use them, "because compromising such infrastructure improves and demonstrates its ability to damage infrastructure during a crisis."[63]

It is worth again emphasizing two points, which are not mutually exclusive:

- To avoid threat inflation and ensure an accurate picture of the cable network landscape, it is important for U.S. policymakers and the national security community to recognize the current reality, based on publicly available data, where the majority of damage and disruption to subsea cables is accidental (*e.g.,* a ship dragging an anchor close to a shoreline), as well as caused by natural weather events (*e.g.,* underwater earthquakes), as industry has routinely and repeatedly stressed.
- There are real national security risks facing submarine cables, especially from the Chinese and Russian governments, which may not be accounted for in that data, which often go unconsidered or unprioritized by industry, and which require tailored risk assessment, risk mitigation, and scenario planning—such as for wartime or armed conflict possibilities.

The Vital Role of "Team Telecom"

When submarine cable companies speak publicly and privately about "security," and conceptualize their own approaches to submarine cable network "security," they are typically speaking about—and thinking about—security in the sense of resilience.[64] This focuses on how submarine cable companies and related organizations, such as governments supporting cable repairs, can ensure cables are quickly and reliably repaired in the event of damage or disruption. And this is an important function, including one performed by the U.S. private sector. Companies may also talk about cybersecurity measures for their systems, such as encryption, and physical access control measures for their facilities, such as fences and cameras around landing stations.

However, this approach to submarine cable "security" fails to capture the wide range of threats posed by foreign actors, including espionage, sabotage, disruption, supply chain infiltration, and the strategic shaping of the global submarine cable network counter to democratic interests. The frequent industry paradigm for subsea cable security also fails to appreciate and factor in the sophistication and persistence of the United States' foreign adversaries, particularly the Chinese and Russian

---

[61] Justin Sherman, *Russia's Digital Tech Isolation: Domestic Innovation, Digital Fragmentation, and the Kremlin's Push to Replace Western Digital Technology* (Washington, D.C.: Atlantic Council, July 2024), *https://dfrlab.org/2024/07/29/russias-digital-tech-isolationism/;* Andrei Soldatov and Irina Borogan, *The Red Web: The Struggle Between Russia's Digital Dictators and the New Online Revolutionaries* (New York: PublicAffairs, 2015).

[62] U.S. Office of the Director of National Intelligence. *Annual Threat Assessment of the U.S. Intelligence Community.* Washington, D.C.: Office of the Director of National Intelligence, February 2024. *https://www.dni.gov/files/ODNI/documents/assessments/ATA-2024-Unclassified-Report.pdf.* 16.

[63] U.S. Office of the Director of National Intelligence. *Annual Threat Assessment of the U.S. Intelligence Community.* Washington, D.C.: Office of the Director of National Intelligence, February 2023. *https://www.dni.gov/files/ODNI/documents/assessments/ATA-2023-Unclassified-Report.pdf.* 15.

[64] I have had numerous conversations with submarine cable companies in the United States and around the world about these issues, from technical specialists to executives, as well as other involved organizations.

governments, to a degree that far exceeds risks posed by accidental insider behavior and even criminals. Moreover, it does not consider how routine and important functions such as repairing a damaged cable may be difficult already in deep, rough waters, but another scenario entirely when—akin to the Houthi case—rockets or bullets are flying overhead. And this paradigm especially does not account for how a foreign actor may cast typical norms and practices (to the extent norms even exist) out the window in a wartime, armed conflict, or other crisis scenario.

This is precisely why the U.S. government has an Executive Branch committee, with decades of bipartisan-supported work under its belt, to review submarine cable license applications in the United States and screen them for national security risks. The committee is "Team Telecom."[65] It does not handle every possible risk, such as the risk of a foreign military destroying or damaging a submarine cable in wartime, but it plays an important and necessary role in strategically mitigating national security risks of espionage and supply chain compromise—and in building a base of Executive Branch expertise about the national security risks facing telecom infrastructure.

In 1995, the Federal Communications Commission (FCC) issued a Report and Order stating that it would consider in foreign carrier applications "any national security, law enforcement, foreign policy, and trade concerns raised by the Executive Branch."[66] The FCC cemented this practice in 1997 with a Report and Order reiterating its interest in soliciting Executive Branch agencies' views on national security, law enforcement, foreign policy, and trade considerations[67] vis-à-vis the FCC's Section 214 authority (certificates for foreign carriers),[68] licenses for submarine cable landing stations, and petitions for declaratory rulings under the FCC's Section 310(b) authority (limiting foreign government and certain foreign ownership of telecom licenses).[69] So, for more than 20 subsequent years, the FCC turned to an informal group of Executive Branch agencies—including the Departments of Defense, Homeland Security, State, and Justice, the U.S. Trade Representative, and the Commerce Department's National Telecommunications & Information Administration (NTIA)—to provide input, including national security input, on its application reviews.[70] This included input on submarine cable license applications as well as proposed assignments or transfers of control of a license for a submarine cable landing.[71]

In 2020, President Trump signed Executive Order 13913 that turned the ad hoc, informal group of agencies advising the FCC into a formal committee.[72] Its new title became the Committee for the Assessment of Foreign Participation in the United States Telecommunications Services Sector—though it still is known by its prior name, Team Telecom. The Department of Justice chairs the committee, through its National Security Division, with committee members from the Department of Defense, Department of Homeland Security, and any other agency or department, or Assistant to the President, that the President designates. The E.O. also specified several committee advisors, from the Secretaries of State, Treasury, and Commerce to the Director of National Intelligence and the President's national security advi-

---

[65] As I describe in a report for the Hoover Institution, many U.S. government organizations are involved in submarine cable security, though for today's purposes I will focus on Team Telecom's role. See: Justin Sherman, *Cybersecurity Under the Ocean: Submarine Cables and U.S. National Security* (Stanford: Hoover Institution, January 2023), *https://www.hoover.org/research/cybersecurity-under-ocean-submarine-cables-and-us-national-security.*

[66] U.S. Federal Communications Commission. *Market Entry and Regulation of Foreign-Affiliated Entities.* FCC–95-475. Washington, D.C.: Federal Communications Commission, November 1995. *https://www.fcc.gov/document/market-entry-and-regulation-foreign-affiliated-entities-0.* 3897.

[67] U.S. Federal Communications Commission. *Rules and Policies on Foreign Participation in the U.S. Telecommunications Market.* FCC–97–398. Washington, D.C.: Federal Communications Commission, November 1997. *https://www.fcc.gov/document/rules-and-policies-foreign-participation-us-telecommunications.* 29.

[68] 47 U.S. Code § 214. *https://www.law.cornell.edu/uscode/text/47/214.*

[69] 47 U.S. Code § 310. *https://www.law.cornell.edu/uscode/text/47/310.* See also: U.S. Federal Communications Commission, "Foreign Ownership Rules and Policies for Common Carrier, Aeronautical En Route and Aeronautical Fixed Radio Station Licensees," FCC.gov, accessed December 3, 2024, *https://www.fcc.gov/general/foreign-ownership-rules-and-policies-common-carrier-aeronautical-en-route-and-aeronautical.*

[70] U.S. Federal Communications Commission. *Process Reform for Executive Branch Review of Certain FCC Applications and Petitions Involving Foreign Ownership.* FCC–20–133. 2–3.

[71] Ibid.

[72] Executive Order 13913. Establishing the Committee for the Assessment of Foreign Participation in the United States Telecommunications Services Sector. April 4, 2020. *https://www.federalregister.gov/documents/2020/04/08/2020-07530/establishing-the-committee-for-the-assessment-of-foreign-participation-in-the-united-states.*

sor.[73] President Biden kept E.O. 13913 in place when he entered into office, underscoring consensus on this issue set of U.S. telecommunications cybersecurity and resilience, U.S. national security, and foreign adversaries such as Beijing.

From 2013 to 2019, the FCC referred an average of 15 percent of all international Section 214 and submarine cable applications to Team Telecom for review.[74] Compared to other national security review programs, like the Committee on Foreign Investment in the United States (CFIUS), this program has a relatively narrow, focused purview on a sector of activity with tremendous implications for U.S. economic and national security—and an area of tremendous interest to actors like the Chinese and Russian governments.

Public Team Telecom actions, and recent demonstrations of its mitigation of potential national security risks, include:

- *China Telecom:* The FCC's aforementioned, 2021 revocation of China Telecom's Section 214 authority was based on a Team Telecom recommendation, unanimous from the committee's members. Team Telecom found China Telecom to be a national security risk because of the Chinese government's control over China Telecom, the state-owned enterprise's inaccurate public representations of its cybersecurity practices, the nature of China Telecom's U.S. operations, and evolving technological threats from Beijing.[75]
- *Pacific Light Cable Network (PLCN):* Team Telecom recommended in June 2020 that the FCC refuse to approve cable licensing for the PLCN—a submarine cable involving Google, Facebook, a New Jersey-based telecom, and a Hong Kong-based telecom owned by a Chinese firm—because its routing of U.S. data through Hong Kong allegedly posed a national security risk. One of Team Telecom's specific concerns was that Beijing would compel the Chinese owner of the Hong Kong subsidiary to access data on U.S. persons, and other sensitive data and traffic, traversing the cable. It cited the "current national security environment, including the PRC government's sustained efforts to acquire the sensitive data of millions of U.S. persons" as well as the cable project's "connections to PRC state-owned carrier China Unicom" as reasons for blocking the cable's development.[76] Google and Meta's subsidiaries then withdrew their original FCC application and filed a new one with Hong Kong removed—leaving the landing stations in the United States, Taiwan, and Philippines—which Team Telecom recommended the FCC approve, conditional on the companies' compliance with national security agreements with the committee.[77]
- *ARCOS–1 Cable System:* Team Telecom recommended in June 2022 that the FCC deny an application by ARCOS–1 USA Inc. and A.Surnet Inc. to modify the ARCOS–1 Cable System—at the time, between the United States, Mexico, Belize, Guatemala, Honduras, Nicaragua, Costa Rica, Panama, Colombia, Venezuela, Curazao, Puerto Rico, the Dominican Republic, Turks and Caicos Islands, and the Bahamas[78]—to add a landing station in Cuba. It cited three factors (non-exhaustive): that Cuba "has long represented a significant counterintelligence threat to the United States," where its direct access to a landing station could be leveraged to further that threat; the risk that traffic not intended for Cuba could be misrouted by a provider to send the traffic over the

---

[73] The full list of committee advisors as specified in E.O. 13913: the Secretary of State; the Secretary of the Treasury; the Secretary of Commerce; the Director of the Office of Management and Budget; the United States Trade Representative; the Director of National Intelligence; the Administrator of General Services; the Assistant to the President for National Security Affairs; the Assistant to the President for Economic Policy; the Director of the Office of Science and Technology Policy; the Chair of the Council of Economic Advisers; and any other Assistant to the President, as the President determines appropriate.

[74] U.S. Federal Communications Commission. *Process Reform for Executive Branch Review.* FCC–20–133. 5.

[75] U.S. Department of Justice, "Executive Branch Agencies Recommend the FCC Revoke and Terminate China Telecom's Authorizations to Provide International Telecommunications Services in the United States," Justice.gov, April 9, 2020, *https://www.justice.gov/opa/pr/executive-branch-agencies-recommend-fcc-revoke-and-terminate-china-telecom-s-authorizations.*

[76] U.S. Department of Justice, "Team Telecom Recommends that the FCC Deny Pacific Light Cable Network System's Hong Kong Undersea Cable Connection to the United States," Justice.gov, June 17, 2020, *https://www.justice.gov/opa/pr/team-telecom-recommends-fcc-deny-pacific-light-cable-network-system-s-hong-kong-undersea.*

[77] U.S. Department of Justice, "Team Telecom Recommends FCC Grant Google and Meta Licenses for Undersea Cable," Justice.gov, December 17, 2021, *https://www.justice.gov/opa/pr/team-telecom-recommends-fcc-grant-google-and-meta-licenses-undersea-cable.*

[78] "ARCOS," submarinecablemap.com, accessed December 5, 2024, *https://www.submarinecablemap.com/submarine-cable/arcos;* "ARCOS–1," submarinenetworks.com, accessed December 5, 2024, *https://www.submarinenetworks.com/en/systems/brazil-us/arcos-1.*

cable and to Cuba; and "the Cuban government's relationships with other foreign adversaries, including the People's Republic of China and the Russian Federation," which could enable information-sharing with those governments.[79]

Team Telecom's work has consistently identified national security risks facing the United States through the submarine cable network, particularly vis-à-vis foreign ownership, foreign partnership, landing station, and supply chain risks from the Chinese government, Chinese state-owned telecommunications companies, and other Chinese government-controlled entities. It has also done so in a sector where the traditional industry calculus around "security" and risk does not put U.S. national security at the center—and thinks about "security" in resilience-oriented ways, rather than additionally appreciating the nature of sophisticated foreign threat actors. Team Telecom has also built up a base of expertise within the U.S. government on this problem set and can provide those recommendations to companies, such as through national security agreements, on how to best approach and, if possible, mitigate national security risks that manifest through issues such as company cybersecurity practices, cable network routes, and foreign influence.

The committee's work is also continually evolving. For example, the FCC issued a Notice of Proposed Rulemaking in November 2024, undertaking a major comprehensive review of its submarine cable rules in light of, among others, the "significant" evolution in the national security threat environment in the last two decades.[80] These are welcome and strategically important efforts from the FCC to update national security review processes and regulations to ensure U.S. private-sector companies can keep playing an innovative, competitive role in the global telecommunications system—while simultaneously implementing national security reviews and safeguards to protect against fast-changing threats from foreign governments, especially Beijing and Moscow. Russia's full-on war against Ukraine, concerns about the Chinese government's potential invasion of Taiwan, other escalating security concerns with Beijing's technology activities, and a fast-evolving global threat environment make Team Telecom's work an essential part of identifying and mitigating national security risks in the coming years.

Steps Congress Can Take Now

There are four steps Congress should consider taking now and into the next year.

1. Congress should *consider encouraging Team Telecom to continue efforts to increase transparency around the committee and its activities.* Team Telecom has been repeatedly criticized over the years for a lack of transparency into its review processes.[81] As I detail in my forthcoming book, there are plenty of reasons for U.S. national security regulations and review programs such as Team Telecom to limit the information shared about their activities, in ways industry sometimes does not recognize—including due to classification issues and the dynamic nature of the geopolitical and cyber threat environment—but it is also important for these review processes to not operate as "black boxes" with opaque criteria that are overly difficult for U.S. companies to navigate. Transparency is important in a democracy. It is important for the U.S. government to be able to simultaneously achieve the objectives of protecting national security and minimizing unnecessary costs to industry. And it is also important for the U.S. government to be able to communicate publicly about risks (such as from Beijing) and earn the trust of private-sector companies, civil society groups, and international partners on these risk mitigations. Team Telecom has made significant progress in increasing the transparency around its processes in the last several years and since President Trump's executive order, including Team Telecom providing public justifications for some of its recent license recommendations and the FCC adopting a set of publicly accessible "Standard Questions" in August 2024[82] that companies must submit in Section

---

[79] U.S. Department of Justice, "Team Telecom Recommends the FCC Deny Application to Directly Connect the United States to Cuba Through Subsea Cable," Justice.gov, November 30, 2022, *https://www.justice.gov/opa/pr/team-telecom-recommends-fcc-deny-application-directly-connect-united-states-cuba-through.*

[80] U.S. Federal Communications Commission. *Noticed of Proposed Rulemaking.* FCC–24–119. Washington, D.C.: Federal Communications Commission, November 2024. *https://docs.fcc.gov/public/attachments/FCC–24-119A1.pdf.*

[81] See, *e.g.,* U.S. Federal Communications Commission. *Statement of Commissioner Jessica Rosenworcel Re: Process Reform for Executive Branch Review of Certain FCC Applications and Petitions Involving Foreign Ownership.* Washington, D.C.: Federal Communications Commission, August 2024. *https://docs.fcc.gov/public/attachments/FCC-20-133A5.pdf.*

[82] U.S. Federal Communications Commission. *Executive Branch Review Rules/Standard Questions Effective August 23, 2024.* Washington, D.C.: Federal Communications Commission, August

214, submarine cable license, and Section 310(b) filings.[83] These are all important steps. Congress should consider how it can continue to support the committee's efforts at transparency, including by publicly explaining and highlighting the national security risks facing submarine cables, such as from the Chinese government.

2. Congress should *consider statutorily authorizing Team Telecom to ensure it has the appropriate authorities, on an ongoing and codified basis, to mitigate national security risks to subsea cables.* The statutory authorization of CFIUS in 2007[84] was recognized to be an important moment in cementing the committee's role in screening certain foreign investments in the United States for national security risks. In 2020, a Senate report that reviewed Team Telecom's activities found that the sharing of staff between CFIUS and Team Telecom was counterproductive because some agencies would dual-assign their staffers to both CFIUS and Team Telecom—and the former would receive most of the attention.[85] While they are different review programs with different authorities, scopes, and volumes of reviewed transactions and activities, the finding still underscores how statutory authorization from a procedural standpoint can ensure an organization like Team Telecom is effectively staffed. It could ensure it has the authority and Congressional mandate to engage more publicly, including with industry, to the extent possible, on the risks. And it would also be a way to address previously identified, critical national security gaps: Congress could require Team Telecom to periodically reassess foreign carriers, allow Team Telecom to inspect foreign carriers with which it has no existing security agreement, and include a specific requirement for Team Telecom to proactively identify risks associated with changes in ownership throughout the entities involved in the cable supply chain. Congress should consider how statutory authorization of Team Telecom—which could be coupled with an increase in funding and personnel resources—is an appropriate measure to achieve these objectives and continue enabling the committee to confront national security threats, especially from the Chinese and Russian governments.
3. Congress should *consider commissioning an open-source study on Chinese government involvement in and risks to the global submarine cable supply chain.* There is significant open-source information and data available on the global submarine cable network that can be gathered, coded, and analyzed into a study that is shareable with members of Congress and the public in an open setting. Congress, such as via the Subcommittee, should consider commissioning such a study to give a perspective independent of the submarine cable industry and of the Executive Branch on the global infrastructure and the national security risks facing the infrastructure; to provide insights of practical use to the Subcommittee and other Members on Chinese government involvement in all aspects of the submarine cable supply chain, including via investments and repairs; to help get a better grasp on Subcommittee and relevant Member-specific questions that are not yet clearly answered; and to better evaluate the national security risks facing subsea cable infrastructure from a geopolitical threat and United States policymaking vantage point. This open-source study could be complemented with public briefings to raise awareness on the issue as well as private briefings for more sensitive open-source findings.
4. Congress should *consider requesting a report from the Department of Justice (Team Telecom chair) in conjunction with the Department of Defense on "lessons learned" from Team Telecom in its three decades-long history and since President Trump formalized it into an interagency committee in 2020.* Team Telecom has faced significant challenges in its now-decades-long history, ranging from strategic problems (*e.g.,* an insufficient focus on Chinese government activity) to operational roadblocks, due to the nature of Team Telecom's setup (*e.g.,* staff

---

2024. *https://www.fcc.gov/document/executive-br-review-rulesstandard-questions-effective-aug-23-2024.*

[83] See the list of questions: U.S. Federal Communications Commission, "Requirements for Applications and Petitions Subject to Executive Branch Review," FCC.gov, accessed December 4, 2024, *https://www.fcc.gov/international-affairs/requirements-applications-and-petitions-subject-executive-branch-review.*

[84] This was with the Foreign Investment and National Security Act of 2007 (P.L. 110–49).

[85] U.S. Senate Committee on Homeland Security and Government Affairs: Permanent Subcommittee on Investigations. *Threats to U.S. Networks: Oversight of Chinese Government-Owned Carriers.* Washington, D.C.: Senate Committee on Homeland Security and Government Affairs, June 2020. *https://www.hsgac.senate.gov/wp-content/uploads/imo/media/doc/2020-06-09%20PSI%20Staff520Report%20-%20Threats%20to%20U.S.%20Communications%20Networks.pdf.*

dual-assigned to Team Telecom and programs like CFIUS, the latter of which often ended up receiving more time and attention).[86] Yet, Team Telecom has also, in many ways, made significant progress in tackling these challenges in recent years and since President Trump signed E.O. 13913 in 2020. It has seemingly spent more time focused on threats to submarine cables from the Chinese government, issued more public and plain-language justifications for its recommendations to the FCC on submarine cables, and worked with the FCC to develop new mechanisms to make the program more transparent to industry (*e.g.,* the new Standard Questions). The Senate's bipartisan staff report in 2020 digging into Team Telecom—and, at the time, particularly its failings—was a useful exercise to provide Congress with more information about the committee and to unearth problems and opportunities, but policies and practices have changed. To inform effective oversight, communication to the public about Team Telecom's role and the national security risks to submarine cables, and any future legislative action, Congress should formally request that the Justice Department (as Team Telecom chair), in conjunction with the Defense Department and in consultation with the FCC, author and provide a publicly shareable, unclassified report to Congress on major lessons learned in the design, administration, and threat analysis of its program since the Executive Order in 2020—and describing priority areas and national security risks for the next decade.[87]

The security and resilience of this network are critical to worldwide information flows, commerce, scientific research, military communications, and U.S. national security. Private-sector companies have long played a pivotal role in building and operating this network, and U.S. firms' ability to do so is vital to economic security, national security, and the US' ability to differentiate its Internet model from that of Beijing. Simultaneously, foreign actors, particularly the Chinese and Russian governments, pose serious threats to the global submarine cable network and the security of U.S. data flows—making Federal government entities like "Team Telecom" essential to protecting our national security, countering Chinese efforts to surveil U.S. subsea cables, and ensuring there is a specialized national security voice in discussions about this global Internet infrastructure.

Senator LUJÁN. Next, we will hear from Tim Donovan, President and CEO of the Competitive Carriers Association.

STATEMENT OF TIM DONOVAN, PRESIDENT AND CEO, COMPETITIVE CARRIERS ASSOCIATION

Mr. DONOVAN. Chairman Luján, Senator Moran, Ranking Member Cruz, members of the Subcommittee, thank you for the opportunity to testify about the importance of providing safe and secure connectivity for all Americans.

CCA represents communications providers ranging from small and rural, to regional and nationwide, as well as vendors and suppliers. Our members are often the only provider for portions of their service area, delivering lifesaving connectivity across rural America for their subscribers, as well as millions of Americans that roam onto their networks.

This hearing is timely as new details of compromised networks fill headlines daily. While work continues to analyze and secure networks, it is important to look at broader threat landscape and for Congress and Federal Government to take steps to promote safe and secure networks.

This includes fully funding the $3.8 billion shortfall needed to complete the Rip and Replace program, promoting work between communications providers and Federal partners with clear and unambiguous cybersecurity guidance, and beginning work now to take

[86] Ibid., 13.

[87] This report could, of course, be accompanied by a non-public annex and/or a classified annex provided solely to the appropriate Members.

steps in the 119th Congress to preserve and expand connectivity with a focus on security.

CCA thanks this committee for passing the legislation that created the reimbursement program. The program should have been completed this past July under the initial timeline, but significant amounts of covered equipment and services remain in place today because of insufficient funding.

The situation is dire. Rural providers are being forced to decide where to remove equipment but not replace it. Cutting off service, including for 911. These decommissioning decisions are permanent choices that are detrimental to service availability and even entire businesses.

These decisions are agonizing for our members because they live in the communities they serve, and impacts go beyond their customers. For example, five program participants that collectively serve fewer than 200,000 subscribers connected over 60 million Americans last year who roamed on to their networks because no other service was available. This equipment remains in service right now, including near military bases, airports, and other areas of strategic importance.

Further, because the equipment cannot be properly maintained or upgraded, every day that passes increases the risk of catastrophic network failures. Because it is illegal to procure new equipment and services from untrusted vendors, carriers with this equipment cannot properly patch and upgrade software to defend against emerging threats or even perform basic maintenance.

They cannot work with the manufacturers to identify problems or resolve issues. The Salt Typhoon can hack major operators, and there is a flashing red light for rip and replace networks that do not have the same resources. The national security risk also goes beyond the reimbursement program participants.

Because of the fundamentally interconnected nature of networks, a threat to one network is a threat to all. This is not a partisan issue, and it impacts Americans in red and blue states alike. Funding has bipartisan support in Congress and at the FCC.

I am encouraged by and deeply appreciative of recent legislative developments toward meeting this critical moment and providing the desperately needed funding in the pending NDAA. I want to thank new Senators, representatives, and staff, especially on this committee, for the steadfast work to arrive at this point.

CCA urges Congress to swiftly pass this important legislation and send it to the President for enactment. Beyond Rip and Replace, there are other ways Congress can bolster national security and remove barriers and uncertainty.

Our carriers truly need Federal partners in the fight with us, and they need access to information and resources required to stay ahead of the seemingly never-ending game of security whack-a-mole. Information sharing should facilitate collaboration not only between Federal partners and carriers, but also among carriers.

Policymakers must also take steps to ensure security requirements are clear and consistent across the Federal Government. Today, there are many different standards and requirements that carriers must consider with new layers constantly being added. We

need centralized authority and guidance. Small carriers face specific challenges.

Beyond having smaller teams with a potential lack of security clearances, many smaller carriers rely on their vendor partners for aspects of security hygiene, monitoring, and response. These carriers do not have the buying power to demand specific security procedures and rely on broader economies of scale and industry investment to support these efforts.

Finally, Federal policymakers should continue to encourage and invest in new solutions, including research, development, and growth of Open RAN technologies and continued support for trusted vendors.

There are other key policy issues Congress should prepare for consideration in the upcoming Congress that are necessary to preserve and expand connectivity, each with aspects impacted by security issues, including defending and reforming the Universal Service Fund, supporting permitting reform, and restoring FCC auction authority.

CCA is committed to working with all stakeholders to accomplish the challenging task of securing U.S. networks while maintaining communications services for millions in rural America. Thank you for the opportunity to testify, and I welcome any questions.

[The prepared statement of Mr. Donovan follows:]

PREPARED STATEMENT OF TIM DONOVAN, PRESIDENT AND CEO, COMPETITIVE CARRIERS ASSOCIATION

Chairman Luján, Ranking Member Thune, and Members of the Subcommittee, thank you for the opportunity to testify about the importance of providing safe and secure connectivity for all Americans.

Competitive Carriers Association (CCA) represents communications providers ranging from small, rural providers, serving fewer than 5,000 customers, to regional and nationwide providers serving millions, as well as vendors and suppliers throughout the communications ecosystem. Our members are often the only provider for hundreds or even thousands of square miles of their service areas, providing life-saving connectivity across large swaths of rural America—including in your home states of New Mexico and South Dakota—for their subscribers, as well as millions of Americans who roam onto their networks.

CCA and its members thank this Committee for its continued focus on security and expanding connectivity to all Americans. This hearing is timely as new details of compromised networks fill headlines daily. While work must continue to analyze and to secure networks related to the Salt Typhoon breach, it is important to look at the broader threat landscape and for Congress and the Federal government to take steps to promote safe and secure networks. This includes fully funding the $3.08 billion shortfall needed to complete the Secure and Trusted Communications Networks Reimbursement Program (STCNRP or Reimbursement Program)—often referred to as Rip & Replace—at the Federal Communications Commission (FCC), promoting work between communications providers and Federal partners with clear and unambiguous guidance, and beginning work now to take steps in the 119th Congress to preserve and expand connectivity with a focus on security.

I. CONGRESS MUST FULLY FUND THE "RIP & REPLACE" PROGRAM.

CCA thanks this Committee for passing the Secure and Trusted Communications Networks Act (STCNA), which, among other provisions, created the STCNRP. This important program is part of a yearslong effort to address concerns related to communications equipment and services deemed by Federal agencies, including the FCC, to pose a "national security threat to the integrity of communications networks or the communications supply chain," including the following benchmark steps:

- *August 13, 2018: 2019 NDAA* Section 889 enacted, limiting use of Federal funds for untrusted telecommunications equipment.

- *March 12, 2020:* The *Secure and Trusted Communications Networks Act of 2019* is signed into law after passing Congress with broad bipartisan support.
- *December 27, 2020:* Congress appropriates $1.9 billion to the FCC for the Secure and Trusted Communications Networks Reimbursement Program in the FY2021 *Consolidated Appropriations Act* with a priority for companies with under 2 million subscribers.
- *October 29, 2021:* FCC *opens the filing window* for applicants seeking support from the Reimbursement Program.
- *February 4, 2022:* FCC *notifies* Congress that they have received 181 original applications from 96 applicants requesting $5.6 billion and that current appropriations would not be sufficient to fully fund all approved applications.
  - STCNA requires the FCC to approve or deny applications within 90 days of submission but allows the FCC to extend that deadline by up to 45 days if additional time is needed to review. Exercising that option, the FCC extended the review deadline to *June 15, 2022.*
- *June 1, 2022:* FCC Chairwoman Rosenworcel *informs* Congress the FCC determined the gross cost estimate demand for the program was reduced to $5.3 billion and anticipated further reduction, but that appropriated funds will remain less than the demand from applicants. She notes three contributing factors:
  - The expansion of entities eligible for participation in the Program by the FY2021 Consolidated Appropriations Act;
  - Preliminary cost estimates of the Program did not consider the full range of costs that were ultimately reimbursable under law;
  - Providers reported increased costs since the program was funded due to supply chain issues, inflation, and project completion requirements by law.
- *June 15, 2022:* FCC Chairwoman Rosenworcel *updates* Congress on the FCC's progress reviewing "materially deficient" applications and allowing applicants to cure their submissions. She also announces that absent additional appropriations, the FCC will apply the prioritization scheme specified by Congress for allocation funding on a pro-rata basis.
- *July 15, 2022:* FCC Chairwoman Rosenworcel *informs* Congress that the FCC has completed its review of applications to the Reimbursement Program, and announces in a *Public Notice* the granted applications for reimbursement, the approved cost estimates, and the approved prorated allocations.
  - FCC Chairwoman Rosenworcel notes a shortfall of $3.08 billion to fully fund approved cost estimates.
  - Chairwoman Rosenworcel announces the Commission will prorate reimbursement funds equally to each eligible applicant that have 2 million customers or less. The pro-rata factor is approximately 39.5 percent.
- *July 17, 2023:* Applicants approved for funding support are required to have submitted at least one reimbursement claim, and are required to complete the permanent removal, replacement and disposal of Huawei/ZTE communications equipment and services from their networks within a year of initial distribution of reimbursement funds.

Since 2023, the FCC has continued to update Congress on the status of the program, yet it cannot be completed without sufficient funding. As Chairwoman Rosenworcel noted in her most recent update to Congress, "[t]he consequences of the continued lack of full funding for the Reimbursement Program are significant for our national security and rural communities."[1] To be clear, while the program should have been completed this past July under Congress's initial timeline from the STCNA, significant amounts of covered equipment and services remain in place today because of insufficient funding. The FCC has had to use authority provided by Congress to grant 139 extensions of time, including 118 "based in whole or in part on the funding shortfall." While necessary, these extensions mean that the process is prolonged with increasingly disruptive impacts on the participating carriers and customers they serve.

[1] Letter from Jessica Rosenworcel, Chair, Fed. Commc'ns Comm'n, to Hon. Steny H. Hoyer, Ranking Member, H. Comm. on Approps., Subcomm. on Fin. Servs. And Gen. Gov't (Nov. 26, 2024), https://docs.fcc.gov/public/attachments/DOC–407870A1.pdf.

A. Without full funding, many of your states will lose coverage; including for 9–1–1 and emergency services.

The situation is dire: rural telecommunications providers, especially in Western states, are being forced to decide where to remove equipment but not replace it, eliminating service both to their own subscribers as well as the tens of millions of Americans who roam onto their networks for connectivity, including for 9–1–1 and emergency services. For example, though five Reimbursement Program participants collectively serve under 200,000 subscribers, they connected over 60 million Americans last year who roamed onto their networks because no other service was available. These decommissioning decisions are permanent choices that are detrimental to service availability and even the feasibility of entire businesses. These decisions are agonizing for our Rip & Replace members because they live in the communities they serve. They know that if their network cannot carry a 9–1–1 call, it could be their neighbor, or someone from their own families, who is unable to access life-saving services. Eliminating service in an area does not only affect that carriers' customers, but anyone who would roam onto their network, as they are often the only wireless provider serving much of their market. Millions of Americans, particularly in rural areas and on Tribal Lands, could lose basic connectivity.

Without Congressional action, the lack of STCNRP funding is forcing rural carriers to go out of business. This is not hypothetical. Without more funding, in the coming months, you will see companies go out of business—disconnecting service and eliminating jobs in your home states. To further underscore the impacts across large swaths of the country, the following are examples of impacts from CCA members participating in the STCNRP:

- A Reimbursement Program participant will be forced to reduce its coverage area by over 67 percent (over 31,000 square miles) in Arizona and nearly 64 percent (over 26,000 square miles) in Nevada.
- That same carrier would have a nearly 90 percent reduction in service in Utah, and the impacted areas include key military and national security installations.
- A Reimbursement Program participant in New Mexico will lose 70.2 percent of its current coverage area (over 19,000 square miles) leaving customers unserved.
- A Reimbursement Program participant in Colorado will be forced to reduce its coverage area by 73.8 percent (13,766 square miles).
- A Reimbursement Program participant in Wyoming will be forced to reduce its coverage by over 80 percent (nearly 4,000 square miles).
- A Reimbursement Program participant in Montana will be forced to reduce its service by over 62 percent (over 1,500 square miles).
- A Reimbursement Program participant that serves the Navajo Nation will likely reduce coverage in that area by 20–40 percent.
- A Reimbursement Program participant covering 122,000 square miles in the Rocky Mountains is deciding what portions of its network to decommission because of the funding failure. Its coverage area will need to be reduced by over 70,000 square miles, eliminating the only coverage roamers have available. This coverage area includes 40 military installations, 32 of which are in areas that will not retain service without full funding, including a strategic missile base. Further, only 91 healthcare facilities out of 456 will remain covered, and only 415 schools or other educational facilities out of 1,897 will be able to retain coverage. Over half of this provider's approximately 40,000 subscribers will be affected, as well as the 13–14 million roamers that use the network each year.
- A Reimbursement Program participant in Western states that connects approximately 20 million annual roaming customers, in addition to its own customers, would see service degraded or lost.
- A Reimbursement Program participant serving a large rural area in the Upper Plains cannot transition to 5G because it does not have full funding to remove untrusted equipment. The network, and the communities it serves, will degrade over time and the area will go from served to unserved.
- A Reimbursement Program participant in the South faces financial obligations beyond its prorated funding and faces dire implications in the absence of full funding even if they do not rip and replace.

B. Without full funding, untrusted equipment remains in place, including in locations near military bases and other areas of strategic importance.

This funding shortfall not only threatens the success of the Reimbursement Program and connectivity in rural America, but it also seriously compromises national security. As stated above, untrusted equipment remains in service right now, including some near military bases, airports, and other areas of strategic importance. Further, because this equipment cannot be properly maintained or upgraded, every day that passes increases the risk of catastrophic network failures. Because it is illegal to procure new equipment *and services* from untrusted vendors, carriers with this equipment cannot properly patch and upgrade software to defend against emerging threats or even perform basic maintenance. They cannot work with the equipment manufacturers to identify problems or resolve issues. If Salt Typhoon can hack major operator networks, then there is a flashing red light for Rip & Replace networks that do not have those resources.

The national security risk also goes beyond the Reimbursement Program participants. Because of the fundamentally interconnected nature of networks, a threat to one network is a threat to all. This impacts not only network interconnections, peering, and traffic exchange between networks, but also consumer access. For example, a customer who roams onto a network with covered equipment or services, because no other connectivity is available, could have their device compromised. It has been over six years since Section 889 was enacted, and the status quo is critically unsustainable.

The inability of Reimbursement Program participants to complete their projects in our own backyards also undermines America's strength and leadership internationally. The United States has led the world in raising concerns regarding use of insecure communications equipment and services and has strongly urged Allies and other nations to remove covered equipment currently in use and prohibit future deployments. We must complete this process at home to maintain connectivity in many rural areas while addressing a national security mandate and demonstrating global leadership.

C. There are no other options for Rip & Replace carriers. Congress must provide $3.08 billion.

While FCC extensions of time have been necessary, there is little else the agency can do to support the STCNRP without additional funding. Additional time alone cannot provide the resources for work to continue. Indeed, 72 percent of the status updates filed on October 7, 2024 indicated that the lack of full funding continues to be an obstacle to completing the permanent removal, replacement, and disposal of the covered communications equipment and services in recipients' networks.[2] Fifty percent of the participants reported that they cannot complete the work required because of the funding shortfall.

This is not a partisan issue. It impacts Americans in red and blue states alike. Funding has bipartisan support in Congress and at the FCC. In addition to Chairwoman Rosenworcel's calls for necessary funding, Commissioner Carr has strongly called for Congress to close the funding gap, including in testimony earlier this year noting that:

As a government, we have taken the smart step of ordering the removal of this insecure and high-risk Equipment—gear that proliferated in rural networks near some of our military's most sensitive facilities—and we have said that we would compensate covered providers for the costs of removing and replacing that gear. We need to make good on that promise.[3]

D. Congress has an immediate opportunity to address this issue in the FY2025 NDAA.

I am encouraged by, and deeply appreciative of, recent legislative developments towards meeting this critical moment and providing the desperately needed funding. The Senate Amendment to H.R. 5009—WILD Act [Servicemember Quality of Life Improvement and National Defense Authorization Act for Fiscal Year 2025] (NDAA) includes provisions to increase the STCNRP authorization to the level needed to complete the program and allow the FCC to immediately access the funding nec-

---

[2] Letter from Jessica Rosenworcel, Chair, Fed. Commc'ns Comm'n, to Hon. Steny H. Hoyer, Ranking Member, H. Comm. on Approps., Subcomm. on Fin. Servs. And Gen. Gov't (Nov. 26, 2024), *https://docs.fcc.gov/public/attachments/DOC–407870A1.pdf.*

[3] *Budget Hearing—Fiscal Year 2025 Request for the Federal Communications Commission Before the H. Comm. on Approps. Subcomm. on Fin. Servs. And Gen. Gov't* (May 16, 2024) (testimony of Brendan Carr, Comm'ner, Fed. Commc'ns Comm'n).

essary. I thank the Senators, Representatives, and staff—including members, leadership, and staff on this Committee—for their steadfast work to arrive at this point. CCA supports this effort and urges Congress to swiftly pass this important legislation and send it to the President for enactment.

II. FEDERAL POLICYMAKERS SHOULD TAKE STEPS TO SUPPORT INDUSTRY SECURITY EFFORTS.

Congress should support efforts to increase collaboration between Federal agencies and carriers to bolster network security and to remove barriers and uncertainty. This includes updates to information sharing, clear and consistent security requirements, and a recognition of the unique challenges faced by smaller carriers, including limited resources.

All carriers must have clear and unambiguous guidance and information from the Federal government on network security. Obtaining this information can be particularly challenging for smaller and rural carriers, with limited resources and staff, that are unlikely to have in-house personnel, let alone teams of professionals, with appropriate and often necessary security clearances sitting alongside Federal partners on a day-to-day basis. Without better channels for information sharing, there can be times that, even when Federal partners want to help, assistance is minimal because the lack of clearances prohibits sharing anything other than unclassified/public information. For example, in the ongoing efforts surrounding Salt Typhoon, without sharing of intelligence, many carriers have late or limited indicators of compromise to go hunting for or understanding of how hackers got in, hampering the ability to respond and further secure their networks.

While lists of trusted or untrusted vendors for equipment and services are helpful, efforts must go further. These lists have primarily focused on network equipment and vendors, yet carriers may not have visibility deeper into supply chains to avoid chipsets, modules, or other devices that could create vulnerabilities. Information sharing efforts targeting small and rural carriers like the Communications Supply Chain Risk Information Partnership (C–SCRIP) at the National Telecommunications and Information Administration (NTIA) are helpful and should be expanded, including with appropriate resources to assist all carriers. Most small and rural carriers do not have the resources to participate in ongoing public/private initiatives on security such as the Department of Homeland Security's Cybersecurity & Infrastructure Security Agency (CISA) Communications Sector Coordinating Council. Our carriers truly need Federal partners in the fight with us, and they need access to the information and resources required for staying ahead of the seemingly never-ending game of security whack-a-mole.

Information sharing should facilitate collaboration not only between Federal partners and carriers, but also among carriers. This can create difficulties because our members report that they do not know which other carriers have had cybersecurity issues in part because, as one said:

> We aren't allowed to talk to others, even if we know something, we probably can't share it. This hinders communications and makes things really complicated. We don't know who we can talk to, or what we can talk about with carriers. Somehow, we all need to be brought up to the same level, all brought under the same tent, and be allowed to have open and honest discussions with the other carriers. We need to learn from each other. Right now, we can't do that. By doing things the way the government has, in some ways they have made things worse.

In addition to real-time information sharing, policymakers must take steps to ensure security requirements are clear and consistent across the Federal government. Today, there are many different standards and requirements that carriers must consider, with new layers constantly being added. These range from industry standards, for example, those from 3GPP and other international standards organizations, as well as various requirements or recommendations from the FCC, CISA, and the Department of Commerce's National Institute of Standards and Technology (NIST). Even if well-intended, the lack of coordination is a significant challenge to the implementation of successful cybersecurity plans. There can be major differences between requirements from CISA and what is required by an agency as part of specific programs administered by the FCC, NTIA, or the Treasury or Agriculture Departments. At least in terms of the Federal government, minimizing the agencies involved and synchronizing security-related requirements would foster clarity and consistency and also reduce the associated regulatory burdens so providers with limited resources can use those resource to actually improve their network security.

As breaches occur, it is important to balance alerting consumers and national security authorities with understanding and resolving threats, especially for carriers with limited staff and resources. Our members report significant problems with overly burdensome data breach reporting requirements. For example, the FCC's *Data Breach Order* undermines Congress's connectivity goals by unnecessarily and unlawfully imposing significant compliance costs on smaller carriers, most of which are small businesses that lack dedicated privacy teams and in-house attorneys to navigate the requirements that the FCC has stacked atop existing state and Federal data breach notification laws. In addition, the FCC proposed requiring broadband providers to develop and implement detailed risk management plans for Border Gateway Protocol (BGP) security. These requirements should account for the cumulative regulatory burdens on carriers. The same team or individual may be struggle with these requirements as well as other cybersecurity proposals related to Wireless Emergency Alerts (WEA), the 5G Fund, and CISA's upcoming Cyber Incident Reporting for Critical Infrastructures Act (CIRCIA) reporting framework because of lack of human and financial resources to keep up.

It would be helpful to have one set of centralized authority and directive on cyber hygiene. For example, CCA encouraged the FCC to coordinate with CISA and industry-driven efforts instead of independently regulating. CCA also encouraged CISA to synchronize its CIRCIA reporting with the FCC's reporting requirements as encouraged by Congress. Congress should ensure needed flexibility with government standards with capacity building for carriers, especially smaller ones. Using existing programs can also reduce costs and encourage broader participation.

Federal policymakers should also be aware of specific challenges faced by smaller carriers. Beyond having smaller teams with a potential lack of security clearances, many smaller carriers rely on their vendor partners for aspects of security hygiene, monitoring, and response. Smaller carriers do not have the buying power or scale to demand specific security procedures. They rely on broader economies of scale and industry investment to support these efforts instead of costly bespoke equipment and services.

Finally, Federal policymakers should continue to encourage and invest in new solutions, including research, development, and growth of Open RAN technologies and continued support for trusted vendors. This investment will not only support network security domestically but will also have international impacts that advance American leadership. Today, a large portion of the world's communications networks rely on equipment from untrusted vendors, raising significant security concerns. CCA believes that continued growth of Open RAN can provide an important alternative by enabling a multi-vendor ecosystem that decreases the dependence on untrusted vendors while promoting competition and innovation. However, policymakers should not mandate technologies—if new technologies deliver on their promise, they will compete and succeed in the marketplace. CCA also supports continued partnerships like that between CCA member Cape and the U.S. Government to support strategic communications services to address concerns around security vulnerabilities.

III. IMPORTANT CONSIDERATIONS FOR THE 119TH CONGRESS.

There are several key policy issues Congress should prepare for consideration in the upcoming 119th Congress that are necessary to preserve and expand connectivity, each with aspects impacted by security issues.

A. Universal Service Fund (USF) Reform and Litigation.

I commend you; your staffs; those of Sens. Klobuchar, Peters, Moran, and Capito; and their House Energy & Commerce Committee counterparts for your diligent efforts to create a bipartisan working group for reforming the USF. All CCA members have an interest in ensuring that all Americans have access to the latest broadband services, especially those in rural and high-cost areas. CCA appreciates Congress's support for bipartisan policies that foster sufficient and predictable USF support and that advance the universal service goals of Section 254 of the Communications Act, as amended.

The job of universal service is not complete—there are still areas where coverage will continue to need to be filled in and deployed to meet the overall objectives of ubiquitous voice and broadband services. Even where deployments have occurred, ongoing support for operating expenses—including maintaining an appropriate security posture—demand support from USF to continue to provide service. Most rural carriers operate on extraordinarily thin margins, so threats to USF hurt their ability to upgrade their cybersecurity infrastructure. Failure to update and direct USF programs to preserve and to expand ubiquitous connectivity will lead to continued

consolidation of smaller carriers and carriers serving rural America, reducing coverage in areas uneconomical to serve absent support.

Especially considering the subject of today's hearing, Congress should ensure that resources are available to promote secure networks, especially for smaller carriers serving rural areas. USF reform could be an opportunity to promote cybersecurity best practices. In addition to considering USF eligibility for more carriers and areas, funding for cybersecurity compliance could be part of an operational expenditure fund or part of an existing fund.

Further, recognizing the importance of security, the FCC should consider alternatives to awarding USF support through reverse auctions. These create a race-to-the-bottom where cuts to security may be necessary to access support. Indeed, a previous reverse auction for the Mobility Fund Phase I drove the deployment of significant amounts of equipment now subject to the STCNRP, because those vendors made their equipment and services available at the lowest cost.

The USF is also under threat in the courts. The Supreme Court granted certiorari in a case that could destroy the USF. The litigation questions the fundamental delegation of authority for the USF from Congress to the FCC, and from the FCC to the Universal Service Administrative Company (USAC). The FCC and CCA, among others, are fighting to protect the USF from these attacks. We appreciate the leadership from several Members of Congress, including on this Committee, in previously supporting USF in court against litigation threats by submitting an amicus brief, on bicameral, bipartisan basis, supporting the FCC's defense of the USF in the Fifth Circuit. If the USF is undermined by this litigation, it could have disastrous impacts on broadband deployment in the United States. Although CCA maintains that Section 254 provides more than enough authority for the FCC to administer the USF, Congress could provide additional clarity to protect the USF from future, spurious litigation attempts and should be prepared to act quickly if a court decision undermines the USF.

B. Permitting Reform.

The ability to site, build, and upgrade network equipment is also important for reinforcing network security. CCA members often face unique environmental and geographic challenges that complicate infrastructure work, and increased costs associated with permitting can take up resources that could otherwise be dedicated to enhancing security. Siting reform is critical to overcome major potential barriers to broadband deployment. In the next Congress, CCA encourages common-sense historic and environmental preservation reforms, improved siting standards, and greater CCA member access to Federal lands. CCA also strongly believes that meaningful broadband infrastructure reform need not pit carriers against Federal agencies, states and municipalities. Congress should consider programs and legislation that incentivize state and local governments to facilitate deployment, including through appropriately staffing review offices.

C. Spectrum Auction Reauthorization.

Access to additional spectrum allows carriers to continue to improve coverage, capacity, and upgrade to the latest—and often most secure—equipment and technologies. I echo calls from many on this Committee to reinstate the FCC's general spectrum auction authority. Congress should also facilitate, improve, and maximize public/private collaboration and interagency cooperation in Federal spectrum management and continue to support providing carriers of all sizes with meaningful opportunities to bid on and win spectrum at auction.

* * * * *

Strengthening our communications networks to ensure that all consumers have access to the latest fixed and mobile broadband services is critical to our national security, disaster preparedness and response, and economic growth. To that end, Congress must immediately fill the $3.08 billion funding gap for the Rip & Replace Program. CCA is committed to working with all stakeholders to accomplish the challenging task of securing U.S. networks while maintaining communications services for millions of consumers in rural America. Thank you for the opportunity to testify at this important hearing, and I welcome any questions.

Senator LUJÁN. Thank you. Senator Moran, you are recognized for our next introduction.

Senator MORAN. Mr. Chairman, I would like to welcome and thank Dr. James Mulvenon for joining us today at this hearing.

Mister—Dr. Mulvenon is an international expert on Chinese cyber warfare, on espionage, and military issues.

A Chinese linguist by training, he holds a B.A. from the Chinese Studies from the University of Michigan and a Ph.D. in political science from UCLA. I appreciate his willingness to share his insights and expertise with the Committee. Thank you.

Senator LUJÁN. Dr. Mulvenon, you are recognized, sir.

STATEMENT OF JAMES MULVENON, PH.D., CHIEF INTELLIGENCE OFFICER, PAMIR CONSULTING

Mr. MULVENON. Subcommittee Chairman Luján, Ranking Member Moran, and Ranking Member Cruz, thank you for inviting me here today. As Senator Moran said in his introduction, I am a Chinese linguist.

I always start with that because it was so damn hard, and it took so long, and it destroyed my eyesight. But I have spent the last 30 years here in D.C. building teams of cleared linguists analysts supporting the Department of Defense, and the Intelligence Community, and Federal law enforcement.

And the through line through all of that has been a focus on Chinese cyber and technology issues, which we have been looking at since the mid 1990s. Having looked at all of those attacks over the years, I will say that the Salt Typhoon intrusions are the most serious intrusion against a U.S. telecommunications networks that I have seen in my career and raises a number of troubling strategic and operational and legal issues that I think fall under the purview of this committee to consider.

I would like to make three quick points. The first is the United States clearly is still in a very deep cyber deterrence hole with respect to China, and the whole appears to only be getting deeper.

It is clear from recent events that China, and frankly for that measure Moscow and Tehran, don't feel like they have found America's pain point yet when it comes to cyber, in terms of an expected imposed cost or expected actions on the part of the U.S. Government. According to people in this field, deterrence basically comes in two forms, deterrence through denial and deterrence through punishment.

The problem with cyber warfare and with networks is deterrence through denial is almost impossible because of the nature of the network itself. The offense only has to find one way to get in. The defender has to find every way to keep them out.

That really only leaves deterrence through punishment, which is through response. Whether in the cyber realm or in other elements of U.S. national power, responding to the intrusion or the attack in a way that changes the attacker's calculus about doing it again.

I will say in the first Trump Administration, the promulgation of NSPN 13 went a long way to lowering the thresholds for authorization of offensive action and also a bias toward action. And I expect that in the incoming Administration, we are likely to see a similar new bias toward offense as a way of pushing back.

The second concern has to do with the operational implications for Federal wiretapping and collection by Salt Typhoon. According to public reports, the Chinese gained access to the systems used by

the carriers to comply with CALEA and with FISA Section 702 for wiretapping.

And as the Committee is familiar, Section 105 of CALEA maintains that the carriers have to and maintain the security and integrity of those collection requests, which have clearly been violated in this case. It is important historically to note that this is not the first time that we have had this concern about China.

In fact, in 2009, the so-called Google Aurora Campaign by Chinese hackers also breached a number of these wiretapping compliance databases. So while this isn't the first time that this has happened, it is certainly a pattern.

And they certainly, again, from a deterrence failure perspective, don't see any prohibition against doing this because of the lack of reaction the first time. Public reports also suggested the Chinese intruders used a vulnerability in the existing infrastructure hardware that cannot be remediated and would require a generational upgrade of equipment, costing billions of dollars.

I think that CALEA, as well as these infrastructure upgrade concerns, should be a primary focus of the Committee's oversight and regulatory activity. And I would only point out that the FCC's recent announcement of their draft declaratory ruling that would require communications service providers to submit an annual certification to the FCC attesting that they have created, updated, and implemented a cybersecurity risk management plan does not seem to me to be proactive enough given the seriousness of the intrusion.

And then finally, I would go against my Irish heritage and try and find something optimistic to talk about within this context, which is that the Rip and Replace of the vulnerable hardware exposed by Salt Typhoon could in fact be a huge boon for U.S. telecommunications equipment manufacturers that frankly have struggled over the last decade because of Huawei and ZTE, and that this massive overhaul would, in fact be exactly the kind of reshoring and kind of U.S. industrial planning and modernization that frankly we have been trying to achieve over the last five or six years in our rebalanced relationship with the Chinese economy. Thank you. I look forward to your questions.

[The prepared statement of Mr. Mulvenon follows:]

PREPARED STATEMENT OF JAMES MULVENON, PH.D., CHIEF INTELLIGENCE OFFICER, PAMIR CONSULTING

Introduction and Main Points

Chairman Cantwell, Ranking Member Cruz, and distinguished members, thank you for inviting me to testify today.

I have been researching Chinese cyber operations since the mid 1990s. The SALT TYPHOON cyber campaign by PRC state actors is the most serious telecommunications compromise I have seen in my career, raising a range of strategic and operational issues that fall under the jurisdiction of this Committee.

The Strategic Cyber Deterrence "Hole" is Getting Deeper

- The United States is currently in a deep *deterrence "hole"* with respect to China.
- Neither Beijing (nor Moscow or Tehran for that matter) believe that they have found America's "pain point" regarding cyber intrusions or attacks, further emboldening them to conduct deeper and more dangerous penetrations.
- Much as we would like, we can't simply declare today that we have a credible cyber deterrent; it must be recognized by others as credible.
- Deterrence comes in at least two distinct forms, deterrence by punishment and deterrence by denial.

- Cyber deterrence through denial is primarily based on computer network defense, but it is cost-prohibitive, as cyber offense, which only needs to find one way in, is demonstrably cheaper than cyber defense, which must prevent every avenue of entry. Given the nature of the network, deterrence through denial therefore seems to be extremely difficult.
- Deterrence through punishment, by contrast, is primarily an offensive game, based on the threat of credible and painful retaliation for adversary attacks; in other words, imposing costs. In the cyber realm, deterrence by punishment theoretically offers better chances of success, especially against adversaries that have well-developed cyber infrastructure.
- Some progress was made in the first Trump Administration, particularly its promulgation of NSPM–13 "United States Cyber Operations Policy," which clearly articulated a "bias for action" and for the first time lowered the threshold for authorization of offensive cyber operations by delegating "well-defined authorities to the Secretary of Defense to conduct time-sensitive military operations in cyberspace."
- The current dynamic with China in cyberspace will not change unless a similar, and hopefully even more forward-leaning policy like NSPM–13 is enacted in the new administration.

The Operational Concerns about Federal Wiretapping and Collection are Gravely Serious

- According to public reports, the Chinese intruders gained access to the systems used by the carriers to comply with wiretapping and FISA Section 702 requirements, potentially exposing the targets of U.S. law enforcement and intelligence collection and undermining related counterintelligence operations.
- This is not the first time Chinese intruders have penetrated these types of systems. Public reports asserted that China's Operation Aurora campaign in 2009 against Google also breached their FISA Section 702 systems.
- Public reports suggest that the Chinese intruders used a vulnerability in the existing infrastructure hardware that cannot be remediated and would require a generational upgrade of equipment costing billions of dollars.
- The CALEA (Communications Assistance for Law Enforcement Act) law, especially Section 105 "Systems Security and Integrity," provides ample basis for the Committee to mandate the carriers provide a detailed remediation plan for the vulnerability.
- The recent FCC announcement citing Section 105 as the basis for a Declaratory Ruling that "would require communications service providers to submit an annual certification to the FCC attesting that they have created, updated, and implemented a cybersecurity risk management plan" is not nearly proactive enough.

The "Rip and Replace" of the Vulnerable Hardware Could Be a Huge Boon for Domestic Telecommunications Equipment Manufacturing

- American telecommunications equipment manufacturers like Cisco and Juniper have struggled for decades to meet the challenge from unfairly subsidized competitors like Huawei and ZTE.
- A massive overhaul of the U.S. core infrastructure, restricted to trusted Western equipment manufacturers, would be a huge boost to domestic manufacturing.

Senator LUJÁN. Appreciate that very much. Ranking Member Cruz—Senator Cruz will be recognized for his opening statement.

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

Senator CRUZ. Thank you, Mr. Chairman, for convening this hearing. And thank you for the witnesses for being here today. Cyber attacks from state sponsored hackers represent a grave threat. These attacks strike at the health of our economy, undermine the functioning of our Government and security, and cost our Nation billions of dollars.

State-backed hackers, especially those from the People's Republic of China, Russia, and Iran, are well-funded, highly sophisticated, and relentless in their exploits. No company could hold such a state aggressor at bay indefinitely once it is determined to attack. These attacks have become all too frequent.

The latest one, the so-called Salt Typhoon, was a group of hackers reportedly linked to China's Ministry of State security, who embedded in our telecommunications infrastructure and remained undetected, monitoring America's communications networks.

Based on public information, these Chinese hackers reportedly used backdoor channels to access sensitive government information about the integrity of their Chinese spy network operating in the United States.

These hackers also accessed American citizens' unencrypted texts, audio calls, and potentially e-mails from around the country, and specifically targeted our Nation's leaders, including President-Elect Trump and Vice President-Elect Vance. There is still much unknown about the Salt Typhoon attack and details continue to emerge.

What is clear is that it was a significant cybersecurity breach with far reaching implications for both the U.S. Government and the public. This incident underscores the persistent and malicious interference by the Chinese Communist Party, a belligerent state actor with a long history of exploiting cyber and telecom avenues to harm U.S. interests.

This attack from a state actor against our Nation's infrastructure will not be the last. We must plug any vulnerabilities in communications networks. We already have in place a regime of cybersecurity authorities across multiple Government agencies.

Now is the time to review and align these so they work robustly and efficiently to ensure that our Nation's cybersecurity is as strong as it can be. This, however, is only a start. For too long, the Biden-Harris Administration has tolerated cyberattacks from the People's Republic of China and others, while using these as a pretext to expand inefficient and redundant Government regulations of, at best, dubious efficacy.

In the wake of this attack, we may hear more Pavlovian advocacy in this vein today. In fact, just last week, the Biden FCC announced a declaratory ruling and proposed rulemaking to impose "a modern framework to help companies."

The press release is quite short on details, but this seems to be a bandaid at best and a concealment of a serious blind spot at worst. I have my doubts over whether an annual certification is the right solution, as well as questions about the FCC's technical expertise and legal authority on this matter.

The FCC should not be using the waning days of this Administration to rush into regulatory expansion. Rather, the agency should be assisting cyber and national security experts of the Executive Branch to gather and disseminate the information in the public that the public and policymakers will need to fully address the issue in the next Administration.

As I have noted before, the Federal Government has a poor track record of protecting against cyber attacks, and we should be cautious about placing too much faith in more regulation and reporting

requirements to protect us. Redundant regulations and reporting requirements stifle investment and can weaken incentives to promote secure communications networks and to cooperate with Federal authorities.

In addition to plugging any holes, we should look at coordinating the cybersecurity tools we already have in place at DHS, at the Department of Justice, and elsewhere. Where these conflict or overlap, I believe we should streamline and remove any chinks in the armor. But rather than finger pointing and punishment, we should be working constructively in asking what incentive structures could be implemented to make our cybersecurity defenses as strong as possible.

Finally, the Biden-Harris Administration's lack of an effective response to the PRC's brazenness only emboldens our adversaries to push the boundaries further. One of my Senate colleagues called this "the worst telecom hack in our Nation's history." If we continue the current Administration's approach of weakness and dubious knee jerk self-regulation, we may have to reply to that colleague, yes, until the next one. Thank you.

Senator LUJÁN. Thank you, Senator. I will now recognize myself for five minutes for questions. Now, the providers that the Competitive Carriers Association represents are the smallest, most rural providers across the country.

Thousands of Americans, but thousands of the most vital community institutions. As I stated earlier, schools, library, hospitals, community centers, even our 9-1–1 systems. Mr. Donovan, when there is a vulnerability at one place in one provider's network, how does that affect the rest of the network and the customers that rely on it?

Mr. DONOVAN. Thank you for the question. Because the interconnected nature, a vulnerability of one truly is a vulnerability for all. If the network is breached, they can use that position to look at interconnection points, to monitor traffic patterns, to test out different attacks, and to use that as a launching point to attack other networks.

It is a major problem there. It also includes data roaming where customers may roam on to another network and then back on to their home network. These are some significant problems, and so we do need to remove the vulnerability threats for all carriers.

Senator LUJÁN. I appreciate that. Mr. Sherman, can you put the map displayed behind me into context. How do weak security standards in the construction of an undersea cable out in San Francisco or New York can impact institutions in New Mexico and the data that they protect?

Mr. SHERMAN. Well, first you hit the nail on the head, right. We have these cables taking all kinds of data into and out of the country. So whether you are in Texas, or in New York, or New Mexico, or anywhere else, right, these cables are really central. I think the key two words are supply chain, right.

Because we could worry about, for example, Huawei supplying the actual physical component, right, of the cable. We could worry about a bad actor repairing a cable and messing with it right when it's pulled up from the bottom of the ocean.

And so the key is to make sure that across each part of the supply chain, we have the right standards in place, companies are following best practices, and we have groups like Team Telecom saying here are the extra national security risks we have to watch.

Senator LUJÁN. Well, I want to thank you both for those responses. Now, our networks are highly interconnected, and I appreciate the emphasis that both you placed on that. A vulnerability at any point impacts all of us, and that is why it is important that we use tools at our disposal to fight attempts by foreign threat actors to find ways into our network.

Now, as I said in my opening statement, I am very concerned by the Salt Typhoon hacks and am dedicated to getting to the bottom of how it happened and preventing an intrusion of this magnitude from ever happening again.

On December 3, the FBI, CISA, and international partners released a guide on what cybersecurity practices telecommunication companies should have in place to resist attacks like Salt Typhoon.

Mr. Sherman, reviewing this list, is this brand new information? And are these novel recommendations that the largest companies would have—would not have heard before the U.S. national security agencies?

Mr. SHERMAN. Certainly not. And as my fellow witness noted, maybe that is different, right, for a smaller carrier or a medium-sized business. But nothing in there like use encryption, use multi-factor, you know, don't do a weak password, right, that is not news to a large carrier, right.

That is not news to a large company. So I think the real problem and underscores, as you are saying, is that this guidance is not new, yet companies are still not implementing these basics to try and raise the floor of cybersecurity practices.

Senator LUJÁN. So just to make sure that I understand, Mr. Sherman, most of the practices that the FBI and CISA are recommending are the things that large companies would know that they should already be doing?

Mr. SHERMAN. That is my interpretation, yes.

Senator LUJÁN. Doctor Mulvenon, yes or no, are there things companies could do today to strengthen their networks and resist cyber attacks in the future?

Mr. MULVENON. Yes, there are, Senator. I would only point out that the CISA guidance that you are citing, if you read between the lines, if you have read a lot of these, do more monitoring, you know, review your best practices list.

It doesn't have any specific remediations that you have seen and other guidance where there is—where you can actually fix the vulnerability. Previous guidance from the Five Eyes partners and the FBI and NSA have actually provided the specific patches that would allow you to fix the vulnerability.

The fact that they only call for monitoring and for better encryption and better multi-factor, actually if you read between those lines now you understand that the vulnerability is not fixable. That it is a hardware vulnerability that requires a generational equipment shift. And so, I think that that was one of the most important things that could be revealed here. Now, defense is, of course, always very good.

But 15 years ago, the Department of Defense finally came to the conclusion that said simply concentrating on perimeter defense, buying a better firewall, you know, using VPNs and things along those lines was actually not going to be effective because of the advantage that the offense has in cyber warfare and in cyber espionage.

Again, as I said before, they only have to find one way to get in. You have to find every way to stop them. As a result, the Department of Defense began implementing what they called defense in depth, which began with a very wise assumption, which is we should assume that all of the hardware and software in our infrastructure is either compromised or potentially compromised, but we need to nonetheless operate.

And they began using a lot of very sophisticated techniques like VPNs and secure virtual machines and other things. So it didn't matter if the physical box in the rack was compromised because you could nonetheless operate securely within the machine. But again, it was based on the assumption that in this modern day, you can't ever believe that you don't have compromised hardware and software.

So my only point is there is a limit to defense, and that is why deterrence through punishment really is the only thing that we have left to us because we cannot do deterrence through denial, to deny them access to the target that they are going after.

Senator LUJÁN. I appreciate your answer. So should companies save money and not do any cyber security?

Mr. MULVENON. No, sir. In fact——

Senator LUJÁN. Well just so that I am clear.

Mr. MULVENON. No, no, no. I understand——

Senator LUJÁN. I am going to move on because I don't want us to lose track that these investments are critically important.

Mr. MULVENON. Yes.

Senator LUJÁN. And they should not be ignored. I very much understand using multiple tools.

Mr. MULVENON. Right.

Senator LUJÁN. But having a hardened system for water, electricity, for someone that you purchase a package from, and it delivers at the point, you know, from A to B, are absolutely necessary. I just don't want to lose sight of that.

Now, Dr. Lewis, you noted in your testimony that while major banks spend 6 to 12 percent of their IT budgets on cybersecurity, major telecommunication company providers spend only 3 to 5 percent.

What do you believe is the reason for the discrepancy and how do these companies need to—where do these companies—and how should these companies be investing more?

Mr. LEWIS. Thank you. The first answer, of course, is that banks have more money and so they can spend more. Second answer is the telecom companies are in one of those generational changes as they move to 5G. They are spending a lot on new infrastructure, and they have a different market.

I mean, if your cell phone doesn't work, you switch carriers. So the margin for error is much smaller. So the telcos try hard, but they are just in a worse competitive position than the banks when

it comes to this. I should note I talked to a senior executive at one of the big banks, and he said, look, there is really no difference.

We are an Internet company now. So what the banks could do, the telcos could do. And perhaps to Senator Cruz's point, one of the reasons people believe the banks do better is they are more closely regulated by the financial authorities.

Senator LUJÁN. Appreciate that, sir. Senator Moran, you are recognized for your questions.

Senator MORAN. I will yield to——

Senator LUJÁN. Senator Cruz, you are recognized.

Senator CRUZ. Thank you, Mr. Chairman. Thank you, Senator Moran. Dr. Mulvenon, let's start with you. You state in your testimony that, "the United States is currently in a deep deterrence hole with respect to China."

Based on what you know about Salt Typhoon, as well as your extended knowledge of other state-based attacks on U.S. networks more broadly, is the problem we are facing one of insufficient regulation of domestic companies, or are there broader issues at play?

Mr. MULVENON. I really do believe, Senator, that it has to do with the strategic dynamic between Washington and Beijing, and that the carriers are really collateral damage in the discussion. It really has to do with a basic breakdown of deterrence stability that we have with the Chinese on a whole range of strategic topics, including space, nuclear weapons, and cyber.

And it really has to do with the issue that the Chinese, at least in cyber, don't actually believe that they found our pain point yet because they haven't elicited a response from us that would suggest that they found our pain point.

Senator CRUZ. So what would provide meaningful deterrence?

Mr. MULVENON. Well, meaningful deterrence can really only be achieved through imposing costs rather than simply building better defenses, which as I have tried to point out, is more difficult.

To Senator Luján's comment, however, I would say that the most powerful weapon in the U.S. Government's arsenal is not the Trident D5 nuclear missile on the Ohio class submarine. It is actually the Federal acquisition regulations.

Because to the extent to which the Federal acquisition regulations combine with better NIST standards for telecoms security, the U.S. Government is one of the largest consumers of telecommunications equipment in the United States, and through the Federal acquisition regulation, could simply raise the floor on the cybersecurity quality of the hardware going into the infrastructure.

Senator CRUZ. So should the Federal Government do that? And what precisely would that look like?

Mr. MULVENON. It has been going on for the last couple of years but going on very slowly. NIST has been very slowly raising the standard. And I would only highlight as a defense contractor that the defense industrial base is held to a much higher standard than non-defense contractors in the United States.

And we actually have to adhere to a much higher level of cybersecurity standard for our networks. And the way that the U.S. Government, in fact, enforces that higher level of standard is through the Defense Federal Acquisition Regulations. In other

words, if we want to stay in business, we have got to fix the cybersecurity.

But in terms of our dynamic with Beijing, that is really beyond the purview of the companies for the same reason you said in your opening statement, which is no commercial company is able to withstand the dedicated activity of a state cyber actor.

And that is really cyber deterrence comes down to a response policy by Cyber Command and the other elements of the U.S. Government in terms of imposing costs on the Chinese side such that it changes their calculus of the expected value of future attacks and intrusions.

Senator CRUZ. So, Dr. Lewis, you state in your testimony that countering China requires, quote, "a sustained, direct, and more forceful effort to disincentivize the Chinese." In your judgment, what can a future Trump Administration do to curb the incentives of the Chinese to engage in these types of deeply troubling behaviors?

Mr. LEWIS. Thank you, Senator. I am hopeful that the incoming Administration will do this, but you need a two part strategy. First, you need to engage with the Chinese regularly the way we had arms control talks with the Soviets on nuclear weapons. You need to start by telling the Chinese, this is unacceptable. You have gone too far. And if you don't stop, we are going to take action.

Now, they aren't going to stop, right. That is just—why would they believe us? So the next step is to actually do something. And this would be where Cyber Command or NSA probably needs to develop a menu of responses.

Not the top end, but something a little lower down, probably going after their attack infrastructure in cyberspace and then go back to the Chinese and say, we weren't kidding. Now, do you want to talk?

The Chinese aren't that interested in making a deal with us. I was there in September, and they basically said, you are on a downhill path. Why should we deal with you now? So I think the first step is to engage, warn them, and then take action.

Senator CRUZ. Dr. Mulvenon, you also state in your testimony that the FCC's recent announcement of plans to require communication providers to submit certification that they have implemented a cybersecurity risk management plan is "not nearly proactive enough." Are you concerned that the FCC might be so focused on doing something that it risks creating policies that merely appear effective without addressing the core of the problem?

Mr. MULVENON. Well, to be fair, it could have been worse. They could have called for a blue ribbon commission. But the FCC has direct regulatory oversight particularly over CALEA compliance. And in the past, when CALEA was expanded to include broadband and VoIP, those were led by orders from FCC.

So what I expected to see in their press release was a specific discussion of CALEA compliance, and wiretapping compliance, and certification from the carriers that they were engaged in fixing the problem right now.

Not some airy, fairy sort of annual certification, but that they were actually going to submit something within 90 days that actually described how they were going to actually remediate the spe-

cific vulnerability that caused Salt Typhoon in the first place, and I was surprised to not see it.

Senator CRUZ. So a final question to anyone on the panel who wishes to answer it. What should the American people know about Salt Typhoon, about what happened, and about the security of their communications?

Mr. DONOVAN. Senator, I will share that Americans should know that we—our communications network has been attacked. That carriers are doing their best to provide service. There are things that consumers can do.

RCS, Rich Communication Services for text messages that is encrypted end to end. If you use those services, then there is ways that even if somebody is watching the network, they cannot see what the traffic is.

There are steps that consumers can also take to increase their security, and our carriers are trying to work to educate them on those while we are also working to kick the attackers out of the networks.

Mr. LEWIS. Thank you, Senator. I guess the first thing I would say is that they should know that we are losing, right. That we are not on the winning side of the scoreboard here in the telecommunications and cyber espionage battle.

The second thing they need to know is their services that they depend on, whether it is delivery from company, or the phone, or the electricity are all at risk and are all potentially being held hostage by a hostile foreign power. That makes me nervous.

Senator CRUZ. Thank you.

Senator LUJÁN. Thank you very much, Senator Cruz. Senator Hickenlooper, you are recognized.

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

Senator HICKENLOOPER. Thank you, Mr. Chair. Thank you to you for coming here. We know how busy you are as well. This hearing today is obviously very timely. Salt Typhoon, as we have been discussing, pretty much everyone, is one of the most devastating cyber attacks in the country's history.

It is a sobering reminder for all of us of how critical it is to make sure that our infrastructure is resilient to all types of threats from all types of adversaries. Certain threats like relying on equipment manufactured in China like Huawei or ZTE, it has been known for years. This technology leaves Americans vulnerable to spying.

The data being stolen, marketed. When it was first created in 2019, the FCC's Rip and Replace program was designed to remove suspect Chinese network equipment from wide swaths of the U.S. networks.

But the program is currently impacted by a $3 billion shortfall, leaving wireless networks vulnerable to espionage, disruption, forms of terrorism. There are thousands of wireless towers, often in rural areas, with dangerous equipment still hanging from them to this day.

And behind me, you are going to see the—just how devastating Rip and Replace program's lack of funding is to Colorado, Nebraska, Wyoming, and to a lesser extent to many other states.

Many of these are rural carriers, small businesses that have not been reimbursed for the costs of replacing this equipment for multiple years.

We are delighted that the bipartisan fiscal bill of 2025 National Defense Authorization Act will finally include a solution to fully fund the Rip and Replace program. The success of Rip and Replace will ensure wireless communications across rural America can continue without disruption or interruption.

I am grateful to both Republicans and Democrats in this bipartisan effort, and the FCC who worked with us, to achieve this goal to protect the impacted communities. Let me now—let me ask a couple of questions.

Mr. Lewis, when NTIA hosted the inaugural International Open RAN symposium this year in Golden, Colorado, I am forced to mention—it is a short drive from the NTIA's Institute for Telecommunication Sciences in Boulder.

The symposium brought together experts from over 20 countries to advance security and reliability, to make sure we have the successful adoption of Open RAN technology. Mr. Lewis, how would you open—and how would open and interoperable technologies like Open RAN help enhance the supply chain and address security concerns that have impacted the traditional networks?

Mr. LEWIS. Thank you, Senator. One of the things that happened over the last 20 years is that all of the American telecom companies were driven out of business, largely because of Huawei's advantages from the mothership. Open RAN has the opportunity to change that, and that is a real plus. It will not immediately guarantee better security. It will change the security problem.

Open RAN is more like the Internet than the traditional telecom stack. That means it will have the same cybersecurity problems we know the Internet faces, which are different. But on the whole by getting China out of our supply chain, by finding ways to create new technologies, I think we will be better off. So that is the promise of Open RAN. Just a final thing.

I used to—I meet with a lot of phone companies, and I used to ask them, what do you think of Open RAN? And until this year, all of them said, we are not going to use it. It is not reliable. That started to change.

Senator HICKENLOOPER. Good. Mr. Sherman, the Office of National Cyber Director published a request for information last year to continue harmonizing the various cybersecurity regulations across the entire Federal Government.

Their stakeholders, including telecom companies, they heard that regulations should be flexible and voluntary so that companies can innovate and respond to evolving, sophisticated threats. In addition to innovating, we should be doing more to improve our cyber basics, including adopting well-known best practices, you know, patching devices, making sure that we have—improving the access controls.

Had these been in place across our critical infrastructure, we could have prevented many recent cyber attacks that compromised both our customers and our national security. Mr. Chairman, to continue improving our cyber defenses, how should we determine the right scope of mandatory cyber security?

And where should the Federal Government stick to the flexible, voluntary compliance? What they obviously prefer but it is not always in the best interest of the country.

Mr. SHERMAN. Yes, I think two things, right. One, as you said, is scoping which systems are we talking about, right. And for years we have identified what those critical infrastructure systems are, water treatment, energy.

Obviously, today we are talking about telecommunications, subsea cables. So I think, as you are saying, the first part is which are the sectors, everything could be attacked, but where are the sectors where attacks, breaches, compromises are the most damaging for the American people and for national security.

The second piece, as you said, is what are those basics? So certainly telling a small carrier, I am sure, to do 7,000 things is not useful or productive, right. But large companies that still don't have multi-factor authentication, that is a terrible security practice, right. So we need to identify what are those basics.

You mentioned some of them, encryption and others. Make sure that for those critical infrastructure sectors, organizations, right, they are aware of what to do and they are actually doing it.

Senator HICKENLOOPER. Yes. And that is the required part. I agree. All right. I yield back. Thank you. Thank you.

Senator LUJÁN. Senator Moran, you are recognized for your questions.

Senator MORAN. Chairman, thank you. Maybe this is to Dr. Lewis. Let me start there. So the information that China gathers from this most recent episode and the information they can continue to gather, what is its value to China?

Mr. LEWIS. Thank you, Senator. That is a great question. It is worth bearing in mind that the Chinese government is paranoid and composed entirely of control freaks. So some of the information they steal, it is not clear why they take it.

The intellectual property that lets them design new products, like in the telecom sector, that makes sense. Traditional political, military espionage, you know what our war plans are, what our capabilities are, that makes sense.

But some of the personal data they take really doesn't make sense. Now they do it at home because they are afraid of their own population, but they do it us too. The downside to this is we don't want to wake up one day and find out that the Chinese have figured out how to use the personal data they have been collecting on Americans. Heavens knows they are trying to figure out what the benefit could be.

Senator MORAN. Is there a benefit just of distraction, expense? United States is taking its eye off other balls while we address this issue?

Mr. LEWIS. I don't think so. I think it is a crucial part and I think my—all my fellows would agree with me. It is a crucial part of China's plan to overcome the United States.

Senator MORAN. That is useful for Americans to hear too, what you just said. And our unwillingness to respond in deterrence, looking the other way in a sense, is it expensive, lack of will?

It seems to me that we have learned in other cold wars that you respond to your adversary's actions, and you respond in a way that diminishes those actions in the future.

I appreciated your suggestion that there be negotiations or conversations that precede that, but if we are going to have any chance of success in combating these continual attacks, it has got to be a dramatic and real consequence to China, right?

Mr. LEWIS. No, that is absolutely correct. The Chinese—part of it, and I think my colleagues would agree, part of deterrence is you have to be credible. You have to make credible threats. And since probably about 2010, other countries have concluded that our threats aren't credible.

Senator MORAN. And are there other countries where the threat is responded to or the actions are responded to, and there is a consequence unless—who else besides the United States is in the crosshairs of China?

Mr. LEWIS. All NATO members, Japan, Korea, Singapore, the Philippines.

Senator MORAN. Do all of them do it better than we do?

Mr. LEWIS. They are in the crosshairs of the Chinese. None of them do it in part because they are looking to us for a signal. They are looking for us to lead.

Senator MORAN. Mr. Mulvenon, something you want to say—add to that?

Mr. MULVENON. No. What I would say is that historically, when I have spoken with previous Administrations about response options, the caution has always been the situation is asymmetrical, the domain is asymmetrical. The United States is asymmetrically vulnerable because we are a more digital wired society, therefore we have more to lose. Therefore, we shouldn't respond.

My response to that has always been, but over time, the Chinese economy, the Chinese population, key elements of the Chinese digital infrastructure have, in fact, become much more modernized. And I would argue that we have achieved a relative level of symmetry where that asymmetry argument really doesn't hold any water for me anymore.

To be honest, I have over the years burned my own hole in the ozone layer driving up to central Maryland trying to talk to people about ranges of response options, even when we had very clear understanding of who had done it and why, and even with a discussion about the whole range of U.S. national power, not simply tit for tat in cyber.

And as I pointed out, during the first Trump Administration, the lowering of the authorization threshold under NSPN 13 actually resulted in greater activity, response activity. And one thing I would highlight, for instance, as a success was the attack against the Internet Research Agency in St. Petersburg, which we knew had been responsible for some level of election interference.

And there is a school of thought that said there was less election interference originating from that type of organization in the subsequent election because we hit imposed cost on the Internet Research Agency.

Senator MORAN. Do we have the capability of responding?

Mr. MULVENON. We do have the capability of responding across a whole variety of measures, including cyber. And so it isn't a capabilities discussion. It is absolutely a political will and national command authority decisionmaking discussion.

Senator MORAN. And finally, would we know if we responded? I have often wondered if we have responded to Chinese attacks, cyber attacks on the United States, and China would never report that we had responded to those attacks.

Mr. MULVENON. Well, to be honest, sir, I don't think that that's the metric of success. In many ways, if we wanted—if we want the Chinese to de-escalate, something that they see and understand the consequences of but doesn't create a public situation where they feel reputational shame where they then have to respond again, probably is the best outcome.

Senator MORAN. You are right. You took that differently than I had intended. My point was that I would feel better if we are responding as compared to waiting, but we just didn't know that we had responded because the Chinese never made an issue of it. I just wanted to make sure that there is not a fact out there that I don't know or that we don't know about something we are doing.

Mr. MULVENON. Yes. I would turn the logic upside down and say deductively, again in an open hearing, deductively you could conclude from the increasing severity of the Chinese intrusions and attacks that we have not in fact previously imposed costs on them that has changed their cost benefit calculations.

Senator MORAN. Thank you for reminding a member of the U.S. Senate about logic.

Mr. MULVENON. No, sir.

[Laughter.]

Senator LUJÁN. Senator Peters, you are recognized.

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

Senator PETERS. Thank you, Mr. Chairman. And I want to thank all of our witnesses for being here. You know, each of your testimonies touched on the threat posed by our—to our national security and to our rural broadband by the Chinese telecommunication firms Huawei and ZTE.

And that is why I was proud to have joined many others in successfully fighting for funding to close the Rip and Replace shortfall in this year's National Defense Authorization Act, which we expect to become law in just a matter of a few weeks here. As I have said before, we shouldn't make rural communities choose between being fully connected and having their connections compromised by our adversaries.

This is actually particularly big news back in Michigan, and specifically for Northern Michigan University, which provides Internet to 7,400 students and over 16,000 families in the Upper Peninsula. And for the first time in years, they are going to now be able to upgrade and expand their service.

So, Mr. Donovan, my question is for you, sir. How significant is this funding for a provider like Northern Michigan University? And how do networks like theirs in the Upper Peninsula, a very rural

area, work to drive more activity around rural broadband that otherwise would probably simply not even be feasible?

Mr. DONOVAN. Thank you, Senator. And thank you for your support and push to get this program funded over the years.

And I join you in my optimism that it will get across the goal line in the coming weeks and just really appreciate all your efforts on that. It is absolutely essential for these companies. They have been frozen for the last five years, unable to patch, unable to upgrade, unable to buy spare parts.

This allows them to complete the Rip and Replace build and then move forward. The effect is life changing in communities like the areas that they serve because simply no one else is going to go there. The economy is being what they are of the sparse populations and the terrain that they serve, it is incredibly hard to make a business case to build it out. They are doing it because it is part of their mission to connect their community.

And I want to make clear also that let's not confuse small operators with being unsophisticated. These are operating state-of-the-art networks that are doing this. The biggest challenge is the information asymmetry that they have where you get a guidance of, you know, update your passwords, have these right things in place, but it is not actionable.

We need a little bit more of look here, go do this. Give the carriers something so that when the intelligence community is aware of threats, that the small carriers and all carriers can take the steps that are necessary with clear guidance.

Senator PETERS. Yes. Very good. Mr. Lewis, one of my top priorities as a member of this committee, as well as Chair of Homeland Security and Government Affairs, is protecting American consumers and companies from the national security and economic threat posed by Chinese connected vehicles on our roads.

That is why I pushed the Commerce Department to publish its proposed rule to block the import and sale of Chinese controlled connected vehicles here in the United States. And even if they were manufactured in companies—in countries like Mexico. Mr. Lewis, you have raised concerns in the past about the Chinese government's goal of using dominance in connected and automated vehicle technology to exploit the national security of our country.

So, sir, could you please discuss the national security risk associated with Chinese infiltration and control of the data sharing infrastructure modern vehicles operate, and the importance of U.S. leadership in innovation in this space if we hope to prevent these vulnerabilities from occurring?

Mr. LEWIS. Thank you, Senator. And thanks for your work on this, because it is an issue that is often ignored. But we all know, or we all should know that by now your car is a rolling computer, and that most cars, certainly those built in the last few years, connect to the telecommunications network through a module.

The biggest makers of those modules are Chinese. It is a worrisome problem for the carmakers because if you stop buying from those Chinese companies, you won't be able to have a connected car. And I have talked with both European and American car manufacturers about the dilemmas of moving this out and what can they do. Well, first of all, they know where you are, right. The car

is transmitting a signal. It gives away your location. You can think of scenarios where that location data would be useful.

Second, it gives you the ability to perhaps interfere with the performance of the car. We don't want to go all Hollywood and have people turning cars off in mid-flight or whatever, but it is a risk that your performance could be interfered with in a crisis, for example. Again, you can think of scenarios. So we have found ourselves in a situation not just in this but with others where we went for the lowest cost supplier.

We thought the Chinese were going to be friends. They are embedded throughout our infrastructure, and it will be hard to get them out. Cars are a leading example of this, though, because the modules that come from China, the updates, the patching, all of that creates opportunity for mischief.

Senator PETERS. Thank you. Thank you, Mr. Chairman.

Senator LUJÁN. Senator Budd, you are recognized for your questions.

STATEMENT OF HON. TED BUDD,
U.S. SENATOR FROM NORTH CAROLINA

Senator BUDD. Thank you, Mr. Chairman. I appreciate you holding this hearing. And I thank the panel. This is truly fascinating. You know, public reporting around the Salt Typhoon hack is deeply concerning and speaks to the massive scale of Chinese efforts to infiltrate America's telecommunications infrastructure.

Today's testimony referenced the mismatch between the scope of the threat and the ability to harden networks, incredibly deter malign state actors like China from trying again. China's heavy subsidies and commercial espionage for Huawei and ZTE have helped make them global leaders in deployed networks.

I am pleased to see that the National Defense Authorization Act, which my colleague mentioned just a moment ago, that included funding to finally rip—complete the Rip and Replace of this compromised technology in U.S. networks. So, Dr. Mulvenon, what else could the U.S. be doing to combat the global dominance of Chinese hardware providers?

Mr. MULVENON. So the thing is, as we discussed Open RAN earlier, there are a number of interesting dynamics, particularly in 5G. When we decided to adopt a plurilateral strategy where we decided to work with our OECD allies in Europe and Japan and South Korea, we confronted a number of dilemmas.

One is that even if we don't buy Huawei equipment, that because of the—Huawei's involvement in the standard setting for 5G, that they actually get 40 percent of the royalties for the patents from 5G.

So even companies—even non-Huawei companies that sell 5G equipment, Huawei is still financially benefiting under the 3GPP standard setting process. Open RAM gave us an opportunity to get out of that trap and in fact be the basis for cooperation among OECD partners in an open source way that would not get bogged down in particular royalties and particular patents.

It was also important in that case to break down any antitrust barriers that might exist between, for instance, Nokia and Ericsson in Europe, and Juniper and Cisco in the United States that would

prevent them from working together to actually build a coherent end-to-end handset to base station to servers offering of an alternative to 5G for—as an alternative to Huawei and ZTE for the global South, for Africa, for South America, for Southeast Asia. Because for a long time there was no Western company that actually offered an end-to-end offering that could compete with Huawei's.

And so the things that we were doing in Open RAN, the things we were doing in those plurilateral frameworks, I think strengthened our ability to not only push back against Huawei's global dominance, which had national security implications, but it also allowed us to strengthen our own companies to be able to compete on a relatively level playing field.

Senator BUDD. You know, 5G has been talked about for years from here to the dinner table but we are only recently hearing, at least in these settings, about Open RAN. Why the disconnect there?

Mr. MULVENON. Well, I mean, the carriers were right for a number of years that Open RAN wasn't as robust to be able to handle tier one level traffic as the current standards were. But that is why we invested so much money in Open RAN was to help it catch up so that in fact the carriers wouldn't resist that by saying it is actually going to reduce our performance in terms of providing telecommunication service.

So Open RAN had a lot of work to do, but I would argue and agreeing with Dr. Lewis that in fact Open RAN is much more mature and robust right now and is a credible alternative for the carriers. There are a lot of benefits to going to open source, by the way, as opposed to a closed source patent and royalty environment in which clearly Huawei is financially benefiting.

Senator BUDD. Thank you. Mr. Donovan, I wanted to briefly ask you, you mentioned that it is difficult for smaller providers to navigate these complex cybersecurity requirements from all these different agencies that sometimes they overlap, sometimes they don't align with each other. Should this committee look at addressing streamlined cybersecurity requirements, and how could we encourage private sector investment in cybersecurity?

Mr. DONOVAN. Yes, sir. That certainly would help by having some coordinated response and making sure that you are taking information collection regulations requirements that are already in place and using those as much to build on them into the cyber instead of creating new frameworks that make it even more challenging for smaller operators in particular to navigate.

Senator BUDD. Much appreciated. Thank you.

Senator LUJÁN. Senator Welch, you are recognized for your questions.

STATEMENT OF HON. PETER WELCH,
U.S. SENATOR FROM VERMONT

Senator WELCH. Thank you very much, Mr. Chairman. I want to thank all the witnesses. It is very helpful. You know, there are a couple of things that come to mind as I am listening. Obviously, if China infiltrates, there are national security risks, there is an infrastructure risk, there is company security risk, and then potentially individuals.

Mr. Lewis, you said that there is not any—you don't know why, or China doesn't even know why they might try to get individual consumer information or citizen information. Are they—is there evidence that they are absolutely—they are trying to do that specifically?

Mr. LEWIS. Yes. Thank you, Senator. Unfortunately, there is.

Senator WELCH. So why would they want somebody's information in Norwich, Vermont, let's say? And what information is it that they would be going after?

Mr. LEWIS. Well, you could improve their intelligence analysis. You could better identify targets for some sort of covert action.

Senator WELCH. I don't get that. I mean, that sounds like it is specific. I mean, if you randomly get somebody like you throw a dart at the old phone book and you get a name, you come up with some information, how is that going to help you do anything?

Mr. LEWIS. Because the technology allows it. Because the same way that Amazon or Google can track tens of millions of people and say this is what they want for Christmas, this is what they want for, you know, in their stocking. That is something that the Chinese are able to do. So they are looking for political benefit. They are looking for——

Senator WELCH. All right. So, I mean, so how do we deal with this? There is always going to be an effort to infiltrate, right, by adversaries. And China is very aggressive, and you have talked about that. But what is the best way to deal with that and who bears the burden? I mean, the big telecom companies are the ones that have the systems in place.

Mr. LEWIS. Thank you——

Senator WELCH. As opposed to a small individual consumer.

Mr. LEWIS. I think one of the things that we have all said is that this requires a national response to change Chinese behavior. A phone company going to China and saying, please stop. They will just laugh.

Senator WELCH. Well, that is the deny and deterrence that you were talking about. I get that. So there would be a national response if we are going to try to punish China or another adversary by infecting their systems. But what is the deterrence—what's the deny? I mean, who is responsible to set up a denial system?

Mr. LEWIS. Well, there are a couple of things you could do. And this Administration has made some progress, and it is probable that the next Administration will continue it. Here is a good example.

When this last transition occurred, there was a company called SolarWinds that was hacked. One of the targets now is go for the server—the third party service providers, because you hack once, and you get hundreds of targets. SolarWinds had a password for their updater. It was SolarWinds 1, 2, 3, right.

That is not going to stifle, I mean, the Chinese or the Russians for very long. You had the OPM hack where 17 million Americans, including I think some of us on this panel, had our information——

Senator WELCH. Let me go to Mr. Sherman. I was going to—yes, you and then Mr. Mulvenon.

Mr. SHERMAN. Yes, I think it is two things, right. As we are saying, we have to identify where a company is not following best practices. How do we require to raise the floor?

Again, I don't think we should be writing 8,000, you know, bullet points down and putting it in a law that doesn't change, but we can't keep doing this voluntary business anymore where companies don't have any requirements in critical infrastructure sectors. And some they do, right. But where they don't, we can't do this voluntary thing anymore.

Senator WELCH. So how do we hold them accountable and how do we impose that obligation?

Mr. SHERMAN. Yes. Well, as one of my fellow witnesses mentioned, the Federal contracting is a huge way of getting that language in. You can do ongoing audits in ways that are—right, there are tons of technology now, innovative stuff from the private sector to do ongoing auditing anyway.

Lots of companies do this. So it is not like you are adding on some massive cost necessarily to go in as the Government or somebody and take a look at what those metrics are looking like.

Senator WELCH. But the burden would be on those companies to do that?

Mr. SHERMAN. To improve the baseline, absolutely.

Senator WELCH. Mr. Mulvenon, you were going to—looked like you wanted to answer this too, but before you do, one of the huge concerns I have is the things that Mr. Donovan is talking about. I am from Vermont.

Rural carrier—you know, it is small and there is no way our small companies can bear the regulatory burdens that might be associated with best practices for national security. They just can't do it. And the bottom line then is that people who need access to the Internet won't have it. So, and maybe you can address that Mr. Mulvenon.

Mr. MULVENON. I agree with you, Senator. In fact, what we have said from the beginning is even the large carriers, even the tier ones, are not technically capable of withstanding the determined efforts of a state-based cyber actor. And so that shouldn't be the standard.

I would push back a little bit on the idea of why the Chinese are gathering this information. The OPM hack, which stole the personal information of everyone in the U.S. Government at the time who had a security clearance, combined with the CareFirst Blue Cross, Blue Shield hack, the Anthem hack, the Experian financial data hack, based on what I do for a living, if I had that information about an adversary, I would have a highly precise and detailed understanding that would allow me to do a range of targeting of those individuals.

The amount of data that Americans have out in the wild that could then be put together in ways that could be used for recruitment, for disruption of what they are doing. And so if you have all of that data to begin with and then you have a Salt Typhoon, we are knowing already all of the personal information necessary to then drill into the tier one providers customer records to be able to identify who then you want to—you want to actually listen to

the phone calls of and be able to listen to the voice-mails of, that is exactly the intelligence sequence that you would need——

Senator WELCH. To be able to do that. So basically, it adds up.

Mr. MULVENON. Absolutely.

Senator WELCH. I yield back. Thank you.

Mr. LEWIS. Can I add one thing, Senator?

Senator WELCH. Sure.

Mr. LEWIS. One of the reasons I think we are all frustrated is that we actually know what to do now. And so between NSA, Australian Signals Directorate, other partners, we have identified the minimal number of steps that will reduce the effectiveness of most cyber attacks by 80 to 90 percent. There is something called known Exploitable Vulnerabilities Program that some of the private companies do. We know how to lower the threat considerably; we just aren't doing it.

Senator LUJÁN. Thank you, Senator. Senator Blackburn, Senator Blackburn, you are recognized for your questions.

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

Senator BLACKBURN. Thank you so much. And thank you all for being here for the hearing. I appreciate it. Mr. Mulvenon, I want to come to you. And let's talk a little bit about what you refer to as the deterrence hole regarding China, noting that deterrence can involve denial and hardening networks or it can involve punishment, which really relies on that retaliation from credible threats.

So have you talked about deterrence by punishment may be being more effective, but we are looking at an increase in these threats and attacks, and you all just touched on that with Senator Welch. So as we look at a new Administration coming in, talk to me a little bit about lessons learned.

And you are just saying we know how to do this and that is why it is frustrating. So drill down on that. What can we look at with a cyber deterrence posture? What opportunities would be there for cyber diplomacy and offensive capabilities, and things that would actually discourage our adversaries from trying to carry out the attacks in the first place?

Mr. MULVENON. Thank you, Senator. I want to be clear that obviously we should do everything we can on the defensive side to bolster deterrence through denial by not making it easy for the adversary to get in the network.

The key issue that I often run into when talking to people about this is a belief that there is a silver bullet out there, there is a technology, there is a U.S. vendor that has a piece of hardware or a piece of software that is the answer and therefore there are going to be no more intrusions.

But unfortunately, the nature of the cyber domain is such that the offense is always outpacing the defense. So my point is, deterrence through denial is impossible to be the only solution. It has to be paired with deterrence through punishment. We have done a lot of deterrence through denial, through equipment upgrades and software upgrades.

Deterrence through punishment into the case of China is not something that we have pursued. We have done it on a limited

basis with the Russians. We have done it with lesser powers. We have seen real impact from it. But it is, as you suggest, Senator, a range of things. First and foremost is a declaratory policy, a declaratory policy that draws a line that you can defend.

Now, often our declaratory policy in cyber is something pretty anodyne along the lines of the U.S. Government reserves the right at a time and place of its own choosing to respond to a cyber attack against a U.S. target with the full measure of U.S. national power. It is not that we haven't said it out loud that is the problem.

It is that we haven't backed it up. And what that means is when we have attacks like the attack against Sony, the attack against GitHub, the attack, you know, Volt, Flax, and Salt Typhoon, the world is awaiting understanding what our response is going to be and whether we are going to impose costs in any potential realm.

What we know doesn't work is naming and shaming. We know that, you know, blasting the operators and putting them out on an Interpol red notice does not do anything. We know that talking to them about it alone doesn't do anything.

One area where we did have some—frankly, some very positive results was when the Obama Administration put out an Executive Order ascribing cyber sanctions to Chinese state-owned enterprise executives and others that financially benefited from Chinese commercial cyber espionage. Because we were touching people that were actually directly connected to the leadership.

Senator BLACKBURN. Right.

Mr. MULVENON. I am a big follow the money guy in that sense. But at the end of the day, there are things we can do in this symmetrical domain where we can actually signal to the Chinese in cyber that we are holding capabilities that they have at risk.

We can do it in a gray way that is not publicly visible so that they don't feel that international reputational shame, feel like they have to respond in order to defend national dignity. But they nonetheless will get the message that, in fact, there will be costs in the future if they do something like that again.

Senator BLACKBURN. Right. Thank you. Mr. Sherman, I have a question for you dealing with the undersea cables and the way the U.S. is relying on foreign repair ships to go in. And of course, we are concerned about the Chinese vessels that are dragging anchors to cut these cables.

And I want—and I will let you submit this since I am running out of time, but I would like to get what you think about investing in a subsea cable repair, and what we should be doing there in order to make certain that we are protecting the undersea cables? But since I am out of time, let's submit that one for the record. Thank you all.

Senator LUJÁN. Thank you, Senator Blackburn. Senator Markey, you are recognized for questions.

STATEMENT OF HON. EDWARD MARKEY, U.S. SENATOR FROM MASSACHUSETTS

Senator MARKEY. Thank you, Mr. Chairman. And thank you so much for having this incredibly important hearing. In 1994, when the House debated the Communications Assistance for Law En-

forcement Act, or CALEA, I was the Chairman of Telecommunications in the House of Representatives.

I think Mr. Donovan remembers that. And I took to the House floor to discuss the importance of safeguarding the constitutional and privacy rights of the public in that debate on the House floor. I also pushed on the House floor for clear, comprehensive cybersecurity standards, recognizing that a back door into our telecom networks would create an enticing target for hackers, domestically and internationally.

30 years later, those privacy risks have become abundantly clear with the Salt Typhoon hack, which Chinese hackers reportedly exploited that back door to spy on Americans' phone calls. This hack appears to be the most disastrous and impactful telecommunications hack in our Nation's history.

As our witnesses and my colleagues have said today, we urgently need to enhance our cybersecurity defenses to ensure a hack of this nature never happens again. Mr. Lewis, you talk in your written testimony about how the FCC should use Section 105 of CALEA to secure our telecommunication systems. Can you elaborate on what the Commission should do under this authority?

Mr. LEWIS. Thank you, Senator. As you well know from chairing the Committee that drafted CALEA, it had cybersecurity provisions in it, and perhaps they haven't been lived up to as much as we would like.

Senator MARKEY. And I would have been the one putting those provisions in at that time. So they have not been used, is that what you are saying?

Mr. LEWIS. They are being used incompletely, partially. We could do a better job. That is a good starting point. FCC and other parts of the new Administration will need to figure out what to do next on supply chain, on Federal acquisition regulations. But CALEA is a good place to start for the FCC.

Senator MARKEY. And why do you think they never acted, the FCC, over the years?

Mr. LEWIS. Well, some of it is there is a presumption that the companies are doing the right thing. And in many cases, they were. What we have is a very dynamic, well-resourced opponent.

Senator MARKEY. The opponent is?

Mr. LEWIS. China.

Senator MARKEY. Right. But we also have a well-resourced telecommunications industry.

Mr. LEWIS. Not in comparison, unfortunately, Senator. The Chinese are willing to spend money that the telcos could only dream of to get into their systems. So it is a dynamic battle and what might have worked five years ago doesn't work now.

Senator MARKEY. And, well, obviously what the Chinese had five years ago wasn't the same as what the Chinese have today. So it is a constant game of spy versus spy. It is like Mad magazine, right. And if one side stops spending and the other side gains the advantage. So there obviously has to be some additional spending, which, you know, takes place and if it is not the companies——

Mr. LEWIS. Well, the oversight part is important too, because if you look at the rules in CALEA, written so many years ago, they are actually adequate, right. They are written in a way that they

could be implemented. Who is making sure that someone is following them? And that is where some of the things that the FCC has proposed now for annual reporting probably is useful.

Senator MARKEY. No, I appreciate that. You know, interestingly, four years ago, as soon as Trump came in, the telecom companies wanted to have a Congressional Repeal Act, repeal of the privacy laws that had just been passed by the Federal Communications Commission and all of the Republicans came out and voted to repeal all the privacy laws that were on the books at the behest of the telecommunications companies, which passed. We have nothing right now.

And so I think it is more complex, to be honest with you. I think the telecom companies could have done a lot more, but they don't want to do anything on children's privacy or on—or even these security upgrades.

You just have to spend the money. You are in that business. You just have to accept that that is your—that is part of network reliability. So I think the hack does deserve attention, immediate action, and I am glad the Commission has begun the process to require telecom providers to secure their networks and urge the Agency to use the full scope of its authority to protect our communications system.

It is not just a vulnerability that comes from the Chinese, but it can come from any other place in the world as well. And ultimately, the private sector just has to have a responsibility to upgrade to protect. That is the cost of doing business. It is just the way it is. And the same thing is true, by the way for network climate resilience.

You know, we just really need to improve the resilience of against climate of our telecommunications system. So just if you could yes or no to each of our witnesses, do you agree that we must invest additional resources to protect our communications networks against climate change and natural disasters, yes or no?

Mr. LEWIS. It is sort of a no brainer, but I will say yes.

Senator MARKEY. OK, good. Mr. Sherman.

Mr. SHERMAN. Yes.

Mr. DONOVAN. Yes.

Mr. MULVENON. Yes.

Senator MARKEY. No, thank you. It is coming and there is nothing that is going to stop it. You know, climate deniers are not dealing with the reality of this right. And it can hit North Carolina. It can cause—unbelievable. You know the number in—from the two storms, Milton and Helene, total damage to the United States, $300 billion in two weeks—$300 billion. And that is just a preview of coming atrocities.

And it can wipe out telecommunication systems. It can wipe out anything in its path. And it is just kind of—these are baby storms compared to what is going to happen in five or ten more years if we don't deal with climate change. Our whole defense budget is $800 billion. That was $300 billion in two weeks. And anything and everything in its path just got completely and totally wiped out.

So, Mr. Chairman, I can't tell you how grateful I am for this hearing. And you are saying, Dr. Lewis, they are going to use that inherent authority that we built into the 1994 law to finally, you

know. So I am very grateful for that. And you want to add something, Mr. Donovan? I am being indulged by the Chairman right now. Yes.

Mr. DONOVAN. I would just add that part of that—of the funding necessary in other another program that you know well, with Universal Service Fund, that is simply put, we are under attack on USF in the courts right now, and that creates uncertainty that could strip away the funding that allows these companies to even exist, let alone invest in their cybersecurity.

Senator MARKEY. No, I get it. Thank you. I appreciate it. Thank you, Mr. Chairman.

Senator LUJÁN. Thank you, Senator. Senator Rosen, you are recognized for your questions.

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

Senator ROSEN. Well, thank you, Chairman Luján and Ranking Member Moran. This hearing, like everyone said, it is so incredibly important. This is an issue that is fundamental to our national security. And I want to thank all of our witnesses for your work, for being here. And as everyone has been so worried or worried about zero trust right, because many cybersecurity practices, they span over sectors.

Implementing multi-factor authentication, mandatory training on recognizing threats and not just once a year for a half hour, really trying to reinforce cyber hygiene, data minimization. It is really important, being sure that we talk about that zero trust architecture where verification is required at every major point of access. And historically, our telephone networks were built assuming that only those with authorized access would be able to get into certain pieces of the network.

But of course, we know it is no longer the case. So, Mr. Donovan, I am going to ask you a little bit of a two part question. What dynamics have prevented the telecom industry, especially small providers, from building networks with zero trust approach?

And what could Congress and Federal agencies do to ensure providers, big and small, are empowered to prioritize security in their network? And I am going to ask Mr. Sherman if you have anything to add.

Mr. DONOVAN. Well, thank you for the question. You know, there is a couple of different buckets. One for the carriers that are going through the Rip and Replace process. There has been the lack of funding to complete that and to remove this untrusted equipment from their networks.

But for all carriers and to continue what I was mentioning a little bit before that it has been the lack of the Universal Service Fund to maintain, to continue, to allow operating expenses to include cyber.

The margins are extraordinarily tight, and we need to have that support to maintain telecommunications service in rural America. Just like why the program was created. To the latter point, it really is—it is full on information sharing so that we have an all Government approach to help carriers respond to some of these attacks

and get ahead of them. Cyber is a scale game and so we need everyone working together on this.

Senator ROSEN. Thank you. Mr. Sherman, do you have anything to add?

Mr. SHERMAN. Just two things. One, as we have heard, right, we are not going to stop hacking. That is not going to go away. But we should not be making it easy for people to get into systems.

So those baselines, again, are important, and making some of them mandatory are important. The second piece, as we have also been talking about, I think is know your vendor, know your supplier. It is way too easy, right. These systems are far too interconnected, whether it is subsea cables, mobile telecom networks, health care, whatever, right.

It is way too interconnected with too many companies, too many parts made in too many different places that if you are not aware of where those parts are made, have they been tested, who owns it, that is a huge vulnerability space. So, you know, again, we have analogies in other sectors for KYC and banking and other areas. We should be taking those principles and frameworks and applying them to these technology issues.

Senator ROSEN. Yes, I couldn't agree more. I actually wrote a little software system—many years ago, and so I know a little bit about this.

But I want to talk about the funding piece because this is so important to all of us, and you talked about the Universal Service Fund and others, but we think about the E-Rate program and how do we allow schools and libraries to use funding for cybersecurity. And we know that they have received $5 billion in requests over the first year.

We think about how we expand some of those things on the E-Rate program. So to all of the witnesses, I know I am moving on to something a little different. Are there other Federal telecom programs that we could expand eligible expenses to cyber security? Is it worth establishing a specific program for telecom cyber security?

Because in my opinion, if simply adding cybersecurity requirements, is that really enough? So, Mr. Donovan, we will start with you. Should we expand or should we try to create an overarching system that everyone can use?

Mr. DONOVAN. Senator, I think you touched on a really important piece of this, that it is one thing to tell an industry, you need to do more, you need to do this, you need to provide us reports.

But if there isn't—aren't the resources available for those carriers, no matter the best of their intentions, they simply cannot do that. As Senator Welch touched on before, you will drive these companies out of business. We need to make sure that we are resourcing them to address these threats.

Senator ROSEN. Anyone else have anything to add in my last few seconds, thinking about maybe setting some templates that certainly some of our smaller carriers can use that would make them less vulnerable to——

Mr. LEWIS. There is something we could add, Senator, and it is a good question. We talked about it a little earlier before you joined us, but the Federal Government is actually the largest single con-

sumer of IT products and services in the United States and one of the biggest in the world.

So changing the Federal acquisition regulations to require more secure hardware, more secure software, more secure services would benefit everyone, including some of these smaller institutions that we have been talking about.

It is nice because you don't have to choose to sell to the Government, but we think that it would create incentives for people to improve their products without adding to the budget woes.

Senator ROSEN. Well, thank you. And Mr. Chairman, this hearing overall has been so incredibly helpful. I appreciate it and thank you again.

Senator LUJÁN. Senator Rosen, thank you very much. Senator Klobuchar, you are recognized for your questions.

STATEMENT OF HON. AMY KLOBUCHAR,
U.S. SENATOR FROM MINNESOTA

Senator KLOBUCHAR. Thank you. Thank you, Mr. Chairman, and thank you for this hearing. I am sorry, I had the Capitol Police Chief before us today in the Rules Committee or I would be there in person.

I am the Co-Chair of the Next Generation 9–1–1 Caucus, and our focus is on ensuring that our emergency communications are secure. Ransomware attacks have taken down 9–1–1 systems. As the witnesses know, in August, a cyber attack caused outages to the 9–1–1 system in Austin, Texas.

And in 2018, Baltimore's 9–1–1 dispatch system had to be shut down because of hackers. And of course, many, many other things have been warded off because of good work at the Federal, state, and local levels.

Mr. Donovan, in your view, what can Congress do to ensure the resiliency of our emergency response systems in the face of a cyber threat, especially in rural areas?

Mr. DONOVAN. Thank you for the question, Senator. I think this is a continuation that these networks are interconnected. The telecommunications services help power emergency services, 9–1–1.

As we talked about earlier in the hearing, even—our automobiles going on. And so, it is shoring up those vulnerabilities across the entire ecosystem will earn benefits on an emergency services and 9–1–1.

Senator KLOBUCHAR. Thank you. Mr. Lewis, I believe the public and private sector have to work together whenever possible on this. We know oftentimes the private sector are on the first line of defense. They pick things up as like the Chinese—recent Chinese hack with Microsoft.

Can you speak to the importance of the Federal Government and private sector working together to improve cybersecurity, especially for small businesses that have fewer resources than the big ones? We can't have a situation where small businesses get pushed out, shoved away because you don't have the cybersecurity to protect things.

And so, we are going to need a combined effort on this front. Your testimony notes telecom companies could be investing more in

acquiring cybersecurity talent and expanding security teams. Could you talk about this?

Mr. LEWIS. Certainly. Thank you, Senator. One of the changes in the last decade or so has been the shift for spending on research and development, on creating new technology on innovation from the Government agencies to the private sector, to some of the big tech companies, to some of the startups.

So the private sector is where the action is on this. And one way to take advantage of that for smaller companies and for smaller institutions is to think about where they can use what are called cloud services. Cloud services is basically you access the resource over the internet, but somebody else is responsible for managing it, for updating it, for making sure it is secure.

So for a lot of things, I think moving to greater use of the cloud would be the answer, something the Federal Government has been sort of slow at doing. But I think the emphasis of the private sector in R&D, the use of private sector cloud providers, the benefits of the Federal acquisition regulations, emphasizing cybersecurity, that is a good way to partner with the private sector.

Senator KLOBUCHAR. Very good. Mr. Sherman, AI has great potential to improve our infrastructure, but as we all know, it also has new risks. And we have to make sure that our infrastructure is staying ahead of foreign adversaries. And that means we have to have our AI protections in place.

I have worked on this extensively on the democracy front, but I have also worked on it extensively as the member of this committee, the Commerce Committee, with Senator Thune. Senator Thune and I have introduced legislation that passed through the Committee to set up guardrails for the riskiest non-defense applications of AI.

Our bill would ensure AI systems used to manage our critical infrastructure undergo rigorous testing and scrutiny before it gets deployed in the real world. Mr. Sherman, do you agree that transparency in how we train commercially available models can lead to safer, more secure, and more reliable AI systems?

And for instance, if a power grid wants to use AI to improve efficiency, under our bill, a vendor providing the AI system would have to comply with rigorous testing and evaluation before offering the product to, say, utility companies. Since that is clearly a high risk area. We have seen attempts before AI on our power grids. So please comment on this area. Thanks.

Mr. SHERMAN. Yes, I think that is essential. And as you noted, there are several components to this, including every piece that goes into an AI application, right, the training data, testing data, the model weights, the cloud systems that are used to deploy it, right. It is essential to ensure all of that secure.

And as you are getting at from a computer science perspective, a lot of these systems are still black boxes, right. We put in A, we get B out, and we can't tell you what happened in the middle.

So as much transparency as possible is good for safety reasons. It is good for ethical reasons. It is also good for security reasons because, you know, if you are trying to fix it, right, you need to understand it first.

Senator KLOBUCHAR. Very good. All right. Well, thank you, everyone. And thank you, Mr. Chair.

Senator LUJÁN. Senator Klobuchar, thank you very much. Senator Sullivan, you are recognized for questions.

STATEMENT OF HON. DAN SULLIVAN,
U.S. SENATOR FROM ALASKA

Senator SULLIVAN. Thank you, Mr. Chairman. And I appreciate the witnesses' testimony today. It is a really important topic. And let me give you a little bit of my kind of thinking. And I know we have already talked about deterrence, but I really think we need to go into that a lot more. Mister, or Dr. Mulvenon I hopefully I am pronouncing that right. Was I close? OK.

[Laughter.]

Senator SULLIVAN. I got A for—B plus for trying. You have a lot of really good background on China. So I am going to ask this question of you first, but then I will open up to really any of the witnesses, and it goes to this issue of deterrence. And let me just give you a little background without revealing any, you know, classified information.

But like pretty much every Senator here, right before the elections, when we had a top secret briefing with the DNI and the NSA and everything—it was all about the election interference that our adversaries were undertaking, China, Russia, Iran primarily. So really trying to screw with our elections.

Now, I would like to say the Chinese say, you think Taiwan's a core interest of yours? You are going after American democracy by coming in when your dictators would never have the guts to stand for election. Like this is a core interest of ours. There is nothing more important than American elections and democracies.

And yet these countries feel very free to go after, try to disrupt our elections when they again, would never have the guts to do it. Then we got this Salt Typhoon briefing. Breathtaking, I would say. Not in a good way but shocking just how exposed we are and still are.

Think that is not saying anything that is classified. But here is the thing, in all these briefings I was kind of like, you know, we have our NSA and everybody else doing all their good work and these are great Americans, but it is all about defense. Here is how we prevent the Chinese and Russians from going after election interference. We play defense. And then on the Salt Typhoon, it is pure defense.

Here is what we are doing on defense. So a number of us, myself included, this is Democrats, Republicans, we are like, well, what about offense? What about offense? Like, what the hell, what about deterrence? So I have a bill I am getting ready to introduce with Senator Warren—you want to talk about how bipartisan that is. She's a liberal Democrat and I am not.

But after the election interference briefing, our bill is essentially saying, hey, if you are an authoritarian regime and you are undertaking major efforts to undermine American elections, we are going to come at you. These—the U.S. Government, all of it, intel agencies, you name it, we are going to come, and we are going to present to your people not misinformation, but just information.

I mean, let's face it, half the Chinese Communist Party leadership is corrupt as hell. Xi Jinping's sister is a billionaire. I wonder how that happened. Putin is the richest guy in the world. OK, when their people get to know that they are going to get very upset. Now, they can't know that now because of the Chinese firewall, the great Chinese firewall.

You know, we have ways to get around that. We are confident. So what I want to ask you guys all about, especially you, Dr. M, why aren't we going on offense? And doesn't that help? And don't you think if we go quietly, covertly, overtly to the Chinese leadership and say, man, we have got so much—not misinformation like you are doing in our elections.

We got the real scoop on how all you guys are rich, you rip off your people, you steal from your government. Xi Jinping's sister is a billionaire. We are going to let everything—we are going to let 1.3 billion Chinese know that. And we are going to do the same thing to you, Putin. I think he is worth $90 billion, all stolen.

We probably even know where the Swiss bank accounts are where he steals his money. Let's let the Russian people know about that. I think that will be a deterrence. I think the Chinese and the Russians are so scared of their own people. But why are we doing that?

And by the way, every U.S. Senator in these classified briefings is asking our top people, why aren't we doing that? Come on, we are a very powerful nation. We can go on offense here and bring some real deterrence.

So I want to do that, but you are a Chinese expert. What do you think the Chinese will think if we are publishing how rich all the Communist Party leaders are and how much they have stolen from their people?

Mr. MULVENON. Senator, you and I are kindred spirits. If I had a nickel for every time in a U.S. Government meeting I raised this point and proposed a set of nefarious actions, we would be having this meeting on my private Caribbean island. And we would have those——

[Laughter.]

Senator SULLIVAN. They don't need to be——

Mr. MULVENON. We would cut the top of the pineapple off an——

Senator SULLIVAN. I always say like it doesn't need to be misinfo—for the Chinese and Russian, they put stuff in our elections. It is all baloney. You should see the stuff that we are briefed on that they were doing about candidates, Democrats—how bad—it is all lies. We are not going to lie at all.

We are just going to let them know, your leaders are ripping you off and here are the Swiss bank accounts, and we will let them know. And let the Chinese and Russian people know that. Maybe we will get regime change out of that. Who the hell knows, but it will—I think they will be scared to death. And we can do that, and we never do it. Why don't we do that?

Mr. MULVENON. Senator, there are two things you have raised that that I—you know, Amen from the chorus. One is the United States does have a pretty spotty record of trying to engage in deception and lying. Our open society, our free press militate against us telling lies abroad. The most powerful thing——

Senator SULLIVAN. Again, I am not talking about——

Mr. MULVENON. No, no, I understand. The most powerful thing I have ever seen in our information operations is when we simply tell the truth.

Senator SULLIVAN. Yes.

Mr. MULVENON. And the power of that. And I would only highlight this data point. The two pieces of information that caused the Chinese Politburo Standing Committee to leap higher and be angrier and exact more revenge than any other were the articles by David Barboza and Mike Forsyth in Bloomberg and the *New York Times* about the personal billions of Politburo Standing Committee members and their families. Nothing has caused a reaction within Zhongnanhai like the publishing of those two articles.

Senator SULLIVAN. And why is that?

Mr. MULVENON. That is because they are absolutely concerned about the visible hypocrisy of carrying out an anti-corruption campaign and claiming that the party is the source of all truth and wisdom and that there is a purity to the party when in fact their own relatives are enriching themselves using their personal connections.

Senator SULLIVAN. Yes. So why don't we go to them overtly or covertly and say, look, you are messing with our elections.

Mr. MULVENON. Yes.

Senator SULLIVAN. Our elections, right. Again, you think Taiwan is a core interest? You are messing with American elections. You keep doing this, we are going to let every one of your 1.3 billion citizens know how corrupt and rich all of you are.

Mr. MULVENON. Yes.

Senator SULLIVAN. Why don't we do that? And what do you think they would do if we did that?

Mr. MULVENON. It would cause a tremendous amount of instability within the leadership, which frankly is not as a predicate to regime change.

Even as a predicate to the Chinese people making different choices about who they want to rule them and the system in which that ruling is happening, this is the most powerful informational weapon we have, is to simply hold up a mirror and say this is exactly what we know is going on in your system.

And oh, by the way, almost all of that information is knowable through open sources and does not run into some sort of intelligence equities, issue related to sources and methods.

Senator SULLIVAN. And you think it would have—start to have a deterrent effect? Maybe next time they think about messing with our elections, you think they would think twice like, I am not sure I want every Chinese person to know how rich Xi Jinping's family is.

Mr. MULVENON. I have long argued that this is one of the most interesting and potentially effective wedge things we could do, yes.

Senator SULLIVAN. Good. OK. Anyone else have a view in terms of letting—like I will give you another example. You saw Navalny, who Putin ended up killing. They put that video out on Putin's, you know, rich mansions on the Black Sea, I think, or the Baltic. And, you know, had like a hundred million views and got Putin's attention. He's very nervous about that.

Mr. LEWIS. So in 2016, I was advising parts of the Federal Government on how to respond to Russian election interference. And at the time, they said, here is a menu of things we are going to do.

Number one on the list was we would like Vladimir Putin's Botox injections schedule. And I said, this is the best we can do? We are gun shy, so it needs support from the Senate and from others to make us be less gun shy. The leaking the money, you don't have to do covert ops. You don't have to do anything. Just tell. That has been wildly effective. But we have to be a little less gun shy.

Senator SULLIVAN. Anyone else have a view on this? Deterrence, deterrence. We are a big country. We can go to people and say, hey, you want to keep doing this, we are going to bring you a lot of pain.

Mr. SHERMAN. Yes. And being much more of a Russia specialist. Of course, you mentioned, you know, Putin. Fair amount of corruption there, right. Funny how, you know, amateur judo wrestlers become billionaires when they happen to tussle with——

Senator SULLIVAN. One of the richest guys in the world.

Mr. SHERMAN.—when they are teenagers. But I think, as you are saying and others have mentioned, that's an example where we can also take action to interrupt operations, right. And folks mentioned, OK, we have this nine to five, you know, troll farm where people come in and clock in and clock out and post lies, as you said about Americans and members of both parties.

OK, there has been all this reporting, right, about, you know, the U.S. We went in and we shut down some of those farms and we knocked some of those servers offline. And did that stop them from getting back up? Definitely not. But like you said——

Senator SULLIVAN. I mean, I think that is good, but it is all defense. I mean, that is all defense, you knock out the troll farms.

Mr. DONOVAN. Yes. Right, defensive but more of that proactive action of saying, OK, if you are going to set up this infrastructure in this building to run these campaigns, can we actually get in there and shut that down?

Senator SULLIVAN. Yes. Anyone else—any other thoughts?

Mr. LEWIS. Senator, it is also internationally around the world, efforts are already underway on shutting down the influence and power of Huawei and ZTE. But that is why it is also so important that we finish the job here in our backyard, that we have that credibility on the world stage.

Senator SULLIVAN. 100 percent. I agree with that. Well, Mr. Chairman, thank you. I do think there is a lot of bipartisan agreement in the Senate that we need to be a little bit more offensive-minded and that we up to deterrence levels with these authoritarian regimes who are scared to death of their own people.

And if we just let their people know, boy, look at how your leading Politburo Chinese members who talk about corruption, they are all as rich as can be. I wonder how they got that? They stole it from their people. Let's let the Chinese know that and then tell them, quit messing with us or we will keep doing this, and your people will be rioting in the streets before you know it. Thank you.

Senator LUJÁN. Thank you, Senator Sullivan. Mr. Sherman, we didn't get a chance to talk about Team Telecom, and I wanted to ask you a question about existing structures that the Federal Gov-

ernment established to help ensure companies make investments to keep their network safe.

We heard from Dr. Lewis about the list that everyone knows that people should be doing, but others are not. You recommended in your testimony that Congress consider statutorily authorizing Team Telecom, which is currently operating on the authority of Executive Order 13913, which President Trump signed in 2020. Can you talk to us a little bit about that and explain about Team Telecom here?

Mr. SHERMAN. Certainly, Senator. So in the mid 90s, right, the FCC said, OK, we have a complex national security threat environment. Obviously, telecoms are a core target. We need to have a group of experts and other agencies talking to the Commission about what those threats are.

So informally, for years it was known as Team Telecom. This is NTIA. This is the Defense Department. This is DOJ advising the FCC on critical national security issues, including to subsea cables. So for years, this operated informally, bipartisan supported. It was renewed every Administration. And in 2020, as you noted, President Trump formally made it an interagency committee.

President Biden has kept that in place. So also say it plays a central role, and I am happy to talk more about that, in identifying equipment that needs to be taken out of networks from China. In looking at subsea cable plans to connect the U.S. to China and elsewhere. But I think the core analogy is that we have other areas where we have these national security programs, right.

We have CFIUS, the Committee on Foreign Investment in the U.S. Same thing. It was Executive Order, Executive authority. Once Congress put that into law, that was meaningful for authorities, for budget, for transparency. Still getting there with CFIUS, but that was a core moment in cementing that in the Government.

So I think statutorily authorizing Team Telecom would enable that oversight, would enable those proper authorities.

Senator LUJÁN. I appreciate that. And Mr. Sherman, one thing that I think it is important to note for those that are not as familiar with the acronym soup that we often speak with when it comes to telecom policy, that Team Telecom, they get to work when it touches a foreign entity as opposed to domestic.

And it is my understanding that outside of the FCC or others with these authorities, there is not a domestic facing group that gets kicked into gear like Team Telecom, which is all these Federal agencies, including the Department of Justice, to get to work. Is that correct?

Mr. SHERMAN. Well, right. So one, as you rightly noted, Team Telecom is restricted to three main areas, right, including things like is this a foreign carrier or is this a subsea cable that would connect to, as some companies tried to do a few years ago that got blocked, to Hong Kong.

But the second piece, as you said, I am not—others maybe can speak to this. I am not familiar with a similar committee interagency set up to kind of look at security risk to the domestic infrastructure, but part of that is just a function of Team Telecom, right.

The focus is and in some ways should remain on China, on Russia, on Iran, North Korea, and not—you know, they don't go into domestic companies that don't have that international touch point.

Senator LUJÁN. Appreciate that. And you know, one thing, Dr. Mulvenon, that I appreciate is that clarification that both tools are needed. I certainly agree with that as well. And I appreciate that it feels like every one of the experts today expressed that in one form or another.

So I just want to recognize and thank you all. I also agree with the lack of direction that could have been included from the FCC, which was published after there was a briefing to Members of Congress. It should have come before. And I think there is so much more that could be done in partnership with these entities.

And as we work in a bipartisan way, which I believe we will, there is a lot of interest in this space, given that President Trump is the person that signed that Executive Order associating with Team Telecom and looking at what tools could be strengthened in America. Contracting, simple agreements.

If you want to do business with the U.S. Government, these are the kind of safety tools that you need to be including to limit, to reduce the threats that exist. I have been concerned about the lack of trusted foundries that the United States now holds. This is a vulnerability that we have, not in the jurisdiction necessarily of this committee, but we should be having this conversation robustly across tools.

You know, when families have to worry about the baby monitor that they purchased to keep an eye on a loved one or who might be jumping into that to only do ill will, the threats that exist to the most vulnerable amongst us. It is not always someone that is barreling down the door of your home anymore that is going to take all of your financial holdings.

It is someone that sneaks in through a text, or through an e-mail, or through some other way that gets access to everything and then, poof, it is gone. I say all of that because I don't believe that this burden that we have been talking about today with this hack should fall on the backs of the American people.

The education that is being put forward to the American people as to what they could be doing to keep themselves a little safer, it is acronym soup. You know, we started telling them to do this or do that or use this tool or that tool. Well, if most people knew how to do it, I think they would be. I often describe it—it is the same thing as what we had to remind all of ourselves during COVID to wash our hands.

Simple hygiene during COVID to keep ourselves healthy and strong. Simple hygiene when it comes to using the Internet, all of these tools. Not clicking on things we don't know about, all the rest. But, you know, encryption, you go out and talk to folks on the street about encryption and two factor authentication and ask them who is doing it and what is going on. Where do get some responses? There is also going to be a lot of folks that want to know how to use these things.

So I hope that in the way that Senator Kennedy of Louisiana often reminds us, we need to speak to each other in a way that we can understand. And we can pretend to understand what all these

acronyms are. A lot of folks don't, including those that are experts in these fields.

I still remember when I became a public utility commissioner, the book that was given to me on telecom acronyms. It was heavy and the print was very small. My eyes worked back then, and I still needed reading glasses to be able to get through that dictionary, if you will. So I hope that we can work together in these spaces to be able to get this work done. I think this was an excellent conversation.

I appreciate what was shared by all of our colleagues today. Maybe my final question to the final—to the panel as I close this hearing is yes or no, is there more that needs to be done to protect our networks? Dr. Lewis.

Mr. LEWIS. That is not a fair question because it is so obviously yes.

Senator LUJÁN. Appreciate that, sir.

Mr. SHERMAN. He can answer for the group. Yes.

Mr. DONOVAN. Yes. And since you went on the acronyms, make it so that all companies of all sizes can understand it. We need—that the paint by numbers approach for what we have to do to operate this. Don't just assume general guidance is going to be good enough. But yes.

Senator LUJÁN. Mr. Donovan, I want to repeat what you just said. Make it so that the companies doing the work can understand it. I am talking about people on the street, my mom, my neighbors, nephews and nieces.

So let's talk about the importance of putting this together in a way that we can understand it and that those that are responsible can implement it. I appreciate that very much. I would just like to put that exclamation point on that. Dr. Mulvenon.

Mr. MULVENON. Yes. And Volt, Flax, and Salt Typhoon are just the latest harbinger of the consequences of not doing what you are saying.

Senator LUJÁN. What an important reminder. I appreciate that as well. Now, in my closing remarks, as we wrap up today, I just want to enter a few items into the record.

The report published by the FBI, CISA, and other Federal partners titled, "Enhanced Visibility and Hardening Guidance for Communication Infrastructure, Laying Out Best Practices to Defend Our Communication Systems."

And a blog post from T-Mobile providing an update to their customers in light of the Salt Typhoon attacks. Without objection.

[The information referred to follows:]

ENHANCED VISIBILITY AND HARDENING GUIDANCE FOR COMMUNICATIONS INFRASTRUCTURE

Publish Date: December 04, 2024

Related topics: Cybersecurity Best Practices, Critical Infrastructure Security and Resilience, Cyber Threats and Advisories

Introduction

The Cybersecurity and Infrastructure Security Agency (CISA), National Security Agency (NSA), Federal Bureau of Investigation (FBI), Australian Signals Directorate's (ASD's) Australian Cyber Security Centre (ACSC), Canadian Cyber Security Centre (CCCS), and New Zealand's National Cyber Security Centre (NCSC–NZ) warn that People's Republic of China (PRC)-affiliated threat actors compromised

networks of major global telecommunications providers to conduct a *broad and significant cyber espionage campaign.* The authoring agencies are releasing this guide to highlight this threat and provide network engineers and defenders of communications infrastructure with best practices to strengthen their visibility and harden their network devices against successful exploitation carried out by PRC-affiliated and other malicious cyber actors. Although tailored to network defenders and engineers of communications infrastructure, this guide may also apply to organizations with on-premises enterprise equipment. The authoring agencies encourage telecommunications and other critical infrastructure organizations to apply the best practices in this guide.

As of this release date, identified exploitations or compromises associated with these threat actors' activity align with existing weaknesses associated with victim infrastructure; no novel activity has been observed. Patching vulnerable devices and services, as well as generally securing environments, will reduce opportunities for intrusion and mitigate the actors' activity.

Strengthening Visibility

In the context of this guide, visibility refers to organizations' abilities to monitor, detect, and understand activity within their networks. High visibility means having detailed insight into network traffic, user activity, and data flow, allowing network defenders to quickly identify threats, anomalous behavior, and vulnerabilities. Visibility is critical for network engineers and defenders, particularly when identifying and responding to incidents.

Monitoring

Network Engineers

- Closely scrutinize and investigate any configuration modifications or alterations to network devices such as switches, routers, and firewalls outside of the change management process. Implement comprehensive alerting mechanisms to detect unauthorized changes to the network, including unusual route updates, enabled weak protocols, and configuration changes (*i.e.,* changes to users and Access Control Lists [ACLs]).
  - Store configurations centrally and push to devices. Do not allow devices to be the trusted source of truth for their configuration. Monitor configuration and, if feasible, test and override on a frequent basis.
- Implement a strong network flow monitoring solution. This solution should allow for network flow data exporters and the associated collectors to be strategically centered around key ingress and egress locations that provide visibility into inter-customer traffic.
- If feasible, limit exposure of management traffic to the Internet. Only allow management via a limited and enforced network path, ideally only directly from dedicated administrative workstations.
- Monitor user and service account logins for anomalies that could indicate potential malicious activity. Validate all accounts and disable inactive accounts to reduce the attack surface. Monitor logins occurring internally and externally from the management environment.
- Implement secure, centralized logging with the ability to analyze and correlate large amounts of data from different sources. Encrypt any logging traffic destined for a remote destination via IPsec, TLS, or any other available encrypted transport options. Additionally, store copies of logs off-site to ensure they cannot be modified or deleted. Enable logging and auditing on devices and ensure logs can be offloaded from the device.
  - If possible, implement a Security Information and Event Management (SIEM) tool to analyze and correlate logs and alerts from the routers for rapid identification of security incidents.
  - Ensure logging takes place at all levels of the environment, network operating system, application, and software levels, as it pertains to network devices.
  - Establish a baseline of normal network behavior and define rules on security appliances to alert on abnormal behavior.
- Ensure the inventory of devices and firmware in the environment are up to date to enable effective visibility and monitoring.

Network Defenders

- Implement a monitoring and network management capability that, at a minimum, enforces configuration management, automates routine administrative

functions, and alerts on changes detected within the environment, such as connections and user and account activity.

- Establish understanding of the architecture of infrastructure and production enclaves, as well as where the two environments meet or are segregated. Map and understand boundary and ingress/egress points of the network management enclave.
- Understand which assets should be forward facing and remove those that should not be forward facing. Closely monitor all devices that accept external connections from outside the corporate network and investigate any configurations that do not comply with known good configurations, such as open ports, services, or unexpected Generic Routing Encapsulation (GRE) or IPsec tunnel usage. Threat actors have been observed taking advantage of external-facing vulnerable services and features; therefore, proper visibility of network and security operations is vital.
- If appropriate, implement a packet capture capability as part of the broader visibility effort for the enterprise. Determine capture location(s) and retention policies based on organizational demands.

Hardening Systems and Devices

Hardening device and network architecture is a defense-in-depth strategy. Reducing vulnerabilities, improving secure configuration habits, and following best practices limit potential entry points for PRC-affiliated and other cyber threats.

Protocols and Management Processes

Network Engineers

- Use an out-of-band management network that is physically separate from the operational data flow network. Ensure that management of network infrastructure devices can only come from the out-of-band management network. In addition, confirm that the out-of-band management network does not allow lateral management connections between devices to prevent lateral movement in the case that one device becomes compromised. Ensure device management is physically isolated from the customer and production networks. When properly implemented, out-of-band management can mitigate many threat actor tactics, techniques, and procedures (TTPs).
- Implement a strict, default-deny ACL strategy to control inbound and egressing traffic. Ensure all denied traffic is logged. For maximum depth, implement on separate devices from those implementing other security controls.
- Employ strong network segmentation via the use of router ACLs, stateful packet inspection, firewall capabilities, and demilitarized zone (DMZ) constructs. Separation via virtual local area networks (VLANs) and, if possible, private VLANs (PVLAN) will provide additional granular logical separation. This should be done as part of a broader defense-in-depth approach that protects and isolates different device groups.
  - Place externally facing services, such as Domain Name System (DNS), web servers, and mail servers, in a DMZ to provide segmentation from the internal LAN and backend resources.
  - Additionally, as a general strategy, put devices with similar purposes in the same VLAN. For example, place all user workstations from a certain team in one VLAN, while putting another team with different functions in a separate VLAN.
  - Do not manage devices from the internet. Only allow device management from trusted devices on trusted networks. Use dedicated administrative workstations (DAWs) connected to dedicated management zones.
- Harden and secure virtual private network (VPN) gateways by limiting external exposure, if possible, and limiting the port exposure to what is minimally required (for example udp/500, udp/4500 and protocol type 50 (ESP)). Ensure all VPNs are configured to only use strong cryptography for key exchange, authentication, and encryption. [1]
  - Disable unused VPN features and cryptographic algorithms to prevent exploitable weaknesses.
- Ensure that traffic is end-to-end encrypted to the maximum extent possible.
- As a management policy, control access to device Virtual Teletype (VTY) lines with an ACL to restrict inbound lateral movement connections.

- Additionally, disable outbound connections to mitigate against lateral movement. Monitor for changes as adversaries can modify this configuration on compromised devices to allow outbound connections.

- Ensure all authentication, authorization, and accounting (AAA) logging is securely sent to a centralized logging server with modern confidentiality, integrity, and authentication (CIA) protections.
- If using Simple Network Management Protocol (SNMP), ensure only SNMP v3 with encryption and authentication is used, along with ACL protections against unnecessary public exposure. Ensure configuration with the most secure cryptographic options supported by the hardware.
- Disable all unnecessary discovery protocols, such as Cisco Discovery Protocol (CDP) or Link Layer Discovery Protocol (LLDP). If they are required, only enable on the necessary interfaces.
- Ensure Transport Layer Security (TLS) v1.3 is used on any TLS-capable protocols to secure data in transit over a network. [2] Ensure TLS is configured to only use strong cryptographic cipher suites. [3]
  - Use Public Key Infrastructure (PKI)-based certificates instead of self-signed certificates.
  - Implement a robust process to renew certificates before they expire.
- Disable Internet Protocol (IP) source routing.
- Disable Secure Shell (SSH) version 1. Ensure only SSH version 2.0 is used with the following cryptographic considerations [2]. For more information on acceptable algorithms, see NSA's *Network Infrastructure Security Guide.*
  - Configure with minimally a 3072-bit RSA key.
  - Configure with minimally a 4096 Diffie-Hellman key size (group 16).
- When possible, apply secure authentication to protocols and services which allow it, such as Network Time Protocol (NTP), Terminal Access Controller Access-Control System (TACACS+), Open Shortest Path First (OSPF), Border Gateway Protocol (BGP), and Hot Standby Router Protocol (HSRP). Similarly, disable any unauthenticated management protocols or functions, such as Cisco Smart Install.
- Use secure cryptographic building blocks when building VPNs such as [3]:
  - Key Exchange:
    - Diffie-Hellman Group 15 with 3072-bit Modular Exponential (MODP)
    - Diffie-Hellman Group 16 with 4096-bit Modular Exponential (MODP)
    - Diffie-Hellman Group 20 with 384-bit Elliptic Curve Group (ECP)
  - Encryption: AES–256
  - Hashing: SHA–384 or SHA–512
- Ensure that no default passwords are used.
  - Change all default passwords on first use.
  - Ensure no passwords are reset back to the default.
- Confirm the integrity of the software image in use by using a trusted hashing calculation utility, if available.
  - If a utility is unavailable, calculate a hash of the software image on a trusted administration workstation and compare against the vendor's published hashes on an authenticated site as a trusted source of truth. This may require engaging the device's maintenance contract to access source of truth hash values. For additional security, copy the image to a forensic workstation and calculate the hash value to compare against the vendor's published hashes.

Network Defenders

- Disable any unnecessary, unused, exploitable, or plaintext services and protocols, such as Telnet, File Transfer Protocol (FTP), Trivial FTP (TFTP), SSH v1, Hypertext Transfer Protocol (HTTP) servers, and SNMP v1/v2c. Ensure any required internet-exposed services are adequately protected by ACLs and are fully patched.
- Conduct port-scanning and scanning of known internet-facing infrastructure to ensure no additional services are accessible across the network or from the internet. Remove unnecessary internet-facing infrastructure, monitor necessary internet-facing infrastructure, and continuously validate the architecture.

- Routers with an active shell environment—even if they have not been tampered with—have significantly more listeners running at the operating system (OS) level compared to the software level.

Network defenders and network engineers should ensure close collaboration and open communication to accomplish the following:

- Ensure all networking configurations are stored, tracked, and regularly audited for compliance with security policies and best practices.
  - Whenever networking configurations are transmitted for storage, tracking, and troubleshooting, confirm that they are sent using encrypted protocols. Additionally, be sure they are not attached to plaintext e-mails or sent via FTP or TFTP.
- Monitor for vendor end-of-life (EOL) announcements for hardware devices, operating system versions, and software, and upgrade as soon as possible.
- Implement a change management system that anticipates both routine and emergency patching. Continuously monitor for vendor vulnerability and patch announcements and ensure patches are applied in a timely manner. Ensure use of vendor recommended version of the operating system for the features and capabilities required.
  - Test and validate patches as part of the change and patch management processes.
- As part of a broader password policy, store passwords with secure hashing algorithms. Passwords should meet complexity requirements and should be stored using one-way hashing algorithms or, if available, unique keys. Follow *National Institute of Standards and Technologies guidelines* when creating password policies.
- Require *phishing-resistant multi-factor authentication (MFA)* for all accounts that access company systems, networks, and applications, including sensitive administrative access to routers. MFA should use a combination of credentials and a phishing-resistant secondary verification method, such as hardware-based PKI or FIDO authentication, to ensure secure access and prevent unauthorized entry.
- As part of a broader identity and access management policy, use local accounts only for emergencies and change the passwords after each use. Verify that each use was authorized and expected. For everyday management of network infrastructure, use a centralized AAA server that supports multi-factor authentication requirements; however, ensure the AAA server is not linked to the primary corporate identity store.
- Limit session token durations and require users to reauthenticate when the session expires. Conduct audits to determine the standard session duration for each role to implement session expirations.
- Implement a Role-Based Access Control (RBAC) strategy that assigns users to a specific role with defined and inherited permissions to better control and manage what users can do.
- Remove any unnecessary accounts and periodically review accounts to verify that they continue to be needed. Apply the principle of least privilege to make sure accounts only have the minimum permissions necessary to complete their tasks. Additionally, continuously monitor accounts in use.

Cisco-Specific Guidance

Organizations in the communications sector should be aware that the authoring agencies have observed Cisco-specific features often being targeted by, and associated with, these PRC cyber threat actors' activity. To address the risk of exploitation by these specific threat actors, the authoring agencies urge organizations to apply the following hardening best practices to all Cisco operating systems. For additional information, see Cisco's *IOS XE Hardening Guide* and *Guide to Securing NX–OS Software Devices.*

- Disable Cisco's Smart Install service using no vstack.
- If not required, disable the guestshell access using guestshell disable for those versions which support the guestshell service.
- Disable all non-encrypted web management capabilities. If web management is required, configure servers in compliance with vendor recommended security settings and software images.

- Always disable the underlying non-encrypted web server using no ip http server. If web management is not required, disable all of the underlying web servers using no ip http server and no ip http secure-server.
- Disable telnet and ensure it is not available on any of the VTY lines by configuring all VTY stanzas with transport input ssh and transport output none.
- To securely store passwords on Cisco devices, organizations should:
  - Use Type-8 passwords when possible.
  - Avoid use of deprecated hashing or password types when storing passwords, such as Type-5 or Type-7.
  - If supported, secure the TACACS+ key as a Type-6 encrypted password.

Incident Reporting

- *U.S. organizations:* If suspicious activity is identified, contact your local FBI *field office* or the FBI's *Internet Crime Complaint Center (IC3).* Cyber incidents can also be reported to CISA by calling 1–844-Say-CISA (1–844–729–2472), e-mailing *report@cisa.dhs.gov,* or reporting online at *cisa.gov/report.* For NSA client requirements or general cybersecurity inquiries, contact *Cybersecurity_Requests@nsa.gov.*
- *Australian organizations:* Visit cyber.gov.au or call 1300 292 371 (1300 CYBER 1) to report cybersecurity incidents and access alerts and advisories.
- *Canadian organizations:* Report incidents by e-mailing CCCS at *contact @cyber.gc.ca.*
- *New Zealand organizations:* Report cyber security incidents to *incidents @ncsc.govt.nz* or call 04 498 7654.

Secure by Design

The authoring agencies urge software manufacturers to incorporate secure by design principles into their software development lifecycle to strengthen the security posture of their customers. Software manufacturers should prioritize secure by design configurations to eliminate the need for customer implementation of hardening guidelines. Additionally, customers should demand that the software they purchase is secure by design. For more information on secure by design, see CISA's *Secure by Design* webpage. Customers should refer to CISA's *Secure by Demand* guidance for additional product security considerations.

Resources

- CISA: *Cross-Sector Cybersecurity Performance Goals*
- *Joint Guide: Best Practices for Event Logging and Threat Detection*
- NSA: *Network Infrastructure Security Guide*
- NSA, CISA, and FBI: *People's Republic of China State-Sponsored Cyber Actors Exploit Network Providers and Devices*
- NSA: *Hardening Network Devices*
- NSA: *Performing Out-of-Band Network Management*
- NSA: *Cisco Password Types: Best Practices*
- NSA: *Cisco Smart Install Protocol Misuse*
- CCCS: *Cryptographic Algorithms for UNCLASSIFIED, PROTECED A, and PROTECTED B Information—ITSP.40.111*
- NIST: *Special Publication 800–52: Guidelines for the Selection, Configuration, and Use of Transport Layer Security (TLS) Implementations*
- NIST: *Special Publication 800–77: Guide to IPsec VPNs*

References

1. CCCS: *Guidance on Securely Configuring Network Protocols*
2. NSA: *Network Infrastructure Security Guide*
3. CNSS: *Committee on National Security Systems Policy (CNSSP)-15*

Disclaimer

The authoring agencies do not endorse any commercial entity, product, company, or service, including any entities, products, or services linked within this document. Any reference to specific commercial entities, products, processes, or services by service mark, trademark, manufacturer, or otherwise, does not constitute or imply endorsement, recommendation, or favoring by the authoring agencies. Additionally, the information in this document is provided "as-is" and without warranties or representations of any kind. The users of this information shall have no recourse

against the authoring parties for any loss, liability, damage or cost that may be suffered or incurred at any time arising from the use of information in this document, including but not limited to loss of data or interruption of business.

Acknowledgements

Cisco and Google Cloud Security contributed to this guidance.

Version History

December 3, 2024: Initial version.

AN UPDATE ON RECENT CYBERATTACKS TARGETING THE U.S. WIRELESS COMPANIES

By Jeff Simon, Chief Security Officer, November 27, 2024

Like the entire telecommunications industry, T-Mobile has been closely monitoring ongoing reports about a series of highly coordinated cyberattacks by bad actors known as "Salt Typhoon" that are reported to be linked to Chinese state-sponsored operations. Many reports claim these bad actors have gained access to some providers' customer information over an extended period of time—phone calls, text messages, and other sensitive information, particularly from government officials. This is not the case at T-Mobile. To clear up some misleading media reports, here is what we're currently seeing, much of which we believe is different from what is being seen by other providers.

- Within the last few weeks, we detected attempts to infiltrate our systems by bad actors. This originated from a wireline provider's network that was connected to ours.
- We see no instances of prior attempts like this.
- Our defenses protected our sensitive customer information, prevented any disruption of our services, and stopped the attack from advancing. Bad actors had no access to sensitive customer data (including calls, voice-mails or texts).
- We quickly severed connectivity to the provider's network as we believe it was—and may still be—compromised.
- We do not see these or other attackers in our systems at this time.
- We cannot definitively identify the attacker's identity, whether Salt Typhoon or another similar group, but we have reported our findings to the government for assessment.

Simply put, our defenses worked as designed—from our layered network design to robust monitoring and partnerships with third-party cyber security experts and a prompt response—to prevent the attackers from advancing and, importantly, stopped them from accessing sensitive customer information. Other providers may be seeing different outcomes.

We have shared what we've learned with industry and government leaders as we collectively work to combat these large-scale, sophisticated national threats. Last week, I had the opportunity to join a meeting at the White House with other leaders to discuss how we're mitigating these threats. As we all have a mutual goal to protect American consumers, we felt it was important to communicate more about what we've seen with providers who may still be fighting these adversaries.

Prevention of Cyber Attacks

No system is immune to cybersecurity attacks. Technology companies and wireless providers like ours experience hundreds and sometimes thousands of attempted attacks of various degrees every day, so my team and I must stay vigilant. We work each day to stay ahead of what's to come, constantly adjusting our approach as bad actors adjust theirs.

Following some incidents we experienced a few years back, we set out to undertake a cybersecurity major transformation, making a massive investment in our program and focusing on enhancing four key areas:

- Layered defenses that more effectively deter attacks, essentially a series of gates that are increasingly difficult to pass
- Proactive and more robust monitoring to detect unusual activity
- Rapid response capabilities to quickly shut down activity and mitigate impact
- Constant vigilance to stay ahead of evolving threats, promptly detect suspicious activity, and rapidly respond

As we know that attackers will not stop and neither will we, so we've gone even further, investing in new enhancements and bolstering measures we already had in place such as:

- MFA or multi-factor authentication for our entire workforce; requiring FIDO2 (external devices that enable passwordless logins) where possible. MFA requires users to provide multiple forms of verification to access an account, helping prevent unauthorized access through phishing.
- Separation of our systems and networks to hinder a bad actor's ability to move beyond the initial system that they may have compromised.
- Comprehensive logging and monitoring to rapidly alarm on and track unauthorized activity.
- Accelerated patching and hardening of systems to address any security vulnerabilities.
- More security tools to ensure laptops, servers, and network devices are connecting to approved trusted sources
- Constant testing of our systems and advanced attacker simulations to identify security weaknesses, and offering rewards for finding potential security vulnerabilities in our systems

Also, it's important to mention that T-Mobile's modern and advanced telecommunications infrastructure provides additional security advantages. Our wireless network built on standalone 5G technology offers advanced device authentication, enhanced encryption, and improved privacy protections. It tends to be newer and has more security capabilities versus older 4G systems. (You can check out more on the benefits of 5G standalone technology *here.*) Additionally, T-Mobile has minimal operations in wireline networks (*e.g.,* cable, copper, or bulk fiber) and provides service almost exclusively within the U.S. This simplifies the management and security of our systems. Our consumer fiber offerings are also separate isolated networks from our wireless network infrastructure.

These are just a few examples of what we're building and supporting but our work is never done. Cybersecurity is a journey not a destination.

Our Commitment

As an industry and country, we are now seeing activity from the most sophisticated cyber criminals we've ever faced, and as such, we can't make any promises with absolute certainty. But I can tell you that our commitment to our customers is clear: T-Mobile will work tirelessly to keep customer information secure, safeguarding our network, responding swiftly to threats, and investing in security. We are humbled by the trust our customers place in us, and we do not take this responsibility lightly.

Senator LUJÁN. Now, it is clear that when we talk about these threat actors infiltrating our networks and accessing sensitive data through our national security, we are not talking about something that is theoretical. It is happening. This is before us. We are talking about the current state of affairs across all of these networks.

And it is also clear that there are things we can do today to make our systems safer. Rip and Replace, I am optimistic that there is now support and language in the House version of the National Defense Authorization Act.

We need to keep that in place. The telecommunication companies that were affected by Salt Typhoon must do full accounting of their network security practices to ensure they are taking every single box that the FBI, CISA, and others, as Dr. Lewis shared with us today—I mean, every one of you pointed out what we could be doing better.

Get that done before you come back and talk to us. I know they are listening today. We have someone taking notes from this hearing. Get that done because at least this member is going to ask you if you have done it.

And we might do it in a hearing. We might do it in private. We will probably do it in both. It is vital that companies are making the investments necessary to provide the support against these latest attacks. Last, Federal authorities must do more to keep our networks safe.

Going forward, I look forward to working with my colleagues in this room and everyone that has expertise in this space that cares about keeping the American people safe. Last, as my last hearing in this Congress, as the Chair of this subcommittee, I just want to say thank you to all of the staff that provided support, all the journalists, some that are still here covering this today, that are sharing this information with the American people.

It makes a big difference when we are talking about something so complex, but that is part of our daily lives. Together, we passed the single largest investment in broadband infrastructure in our Nation's history and stood up a successful broadband affordability program.

I am pleased to see that there's support for Rip and Replace. We still have work to do when it comes to the Affordable Connectivity Program. 90 million people across America not being able to afford the internet, when they have a hard connection, is a problem. The promise of AI being able to provide a tutor to every young person in America that needs one is only as good if they can get that connectivity.

We have got to get this one done. To Ranking Member Thune, I also wanted to thank him and his team for being such a strong partner. His availability and willingness to work together to be able to work in a bipartisan fashion is something so very much appreciated.

I congratulate him with his new leadership responsibilities and look forward to working with him in that space as well. And then last, the Universal Service Fund. What a strong working group, bicameral, bipartisan.

Came up with strong reforms and ideas. I certainly hope that that work is something that we will see more in the future, that product that actually gets to the President for signature because this is desperately needed.

A program that whose contribution factor from people that still have, here is another acronym, POTS, plain old telephone service. That is the old phone that you have in your house that is dependent on a copper connection that still runs to, you know, some little piece of equipment you see when you are driving out of your driveway or on the road, that old service.

Some people still use that to make long distance phone calls, even though everyone that has a mobile phone can do it for no additional cost. If you are making those long distance calls from your plain old telephone, 30 percent cost factor is contributing to the United Service Universal Service Fund.

It is just not sustainable. We have to modernize. We have to be smart about this. We have to make sure it works or this next generation of tools that we have. I also want to thank Chair Cantwell, Maria, for her leadership in this committee as the Chair of the full committee and for always making these priorities her priorities as well.

To Ranking Member Cruz, I look forward to working with him in the next Congress to move the needle forward on this and so many other areas. And to the members of the Committee who I really got a chance to learn from, find commonality with challenges that exist in my state and in their states with where and how we can work together.

I also want to recognize Betsy, who is we still with us here today, learning from her and getting a chance to work with her in this incredible role. Thank you for your expertise and be willing to work here. Eric, I want to thank you.

I want to thank Matthew. There is a few staff that are no longer on the Committee, but John, Shawn, Christie, Mary, and Harsha. I also want to recognize Ariel, who was and is part of Senator Cruz's team for the work that she has done.

Alex, on Senator Thune's, he has been incredible. His willingness to work together, plan together, find commonalities where we can. Agreeably disagree where we must. That is appreciated as well.

Stephanie and Jeff, thank you for keeping this place running and informing us who is next by making sure you keep this place running the way that it should. They are clerks on the Committee.

And then my staff, Jeff, Hakon, Shelby, Sophia, who is here with me as well, DeeDee, Carla, and Sarah for their expertise. It is—this comes with so many responsibilities and you need experts to help you through this.

Now, with that, I will close this hearing. Should members have additional questions for the witnesses for the record, I ask that they submit them to the Committee by December 20, and witnesses will have until January 13 to respond. Thank you, everyone, so very much.

[Whereupon, at 4:45 p.m., the hearing was adjourned.]

A P P E N D I X

RESPONSE TO WRITTEN QUESTIONS SUBMITTED BY HON. TED CRUZ TO JAMES ANDREW LEWIS

Cybersecurity and the Regulatory State

The long history of state-backed cyberattacks, particularly from the People's Republic of China, will surely not be the last. Cybersecurity is of critical importance. However, the Federal government has a poor track record of protecting against cyberattacks, and we should be cautious about placing too much faith in more regulation or reporting requirements.

Question 1. Are there ways to incentivize the adoption of better cybersecurity in the telecommunications sectors rather than reaching for the regulatory stick? For example, could we use regulatory or liability protections to align incentives and get companies to better protect their systems?

Answer. More than a decade ago, Senators McCain, Leiberman and Collins held hearings on cyber security legislation. Ultimately, after interventions by business groups, the Senate rejected a regulatory approach in favor of a voluntary approach. At that time (2010), not rushing into regulation was the right decision since the U.S. could not define what regulations were necessary to reduce the risk of being hacked or which agency should be responsible (there was universal agreement that DHS was not capable of this). Faith that regulation could be avoided without degrading security was misplaced, however, and the result has been years of damaging hacks by opponent using the most basic techniques because of failures to take rudimentary precautions. The sector-specific approach adopted in 2012 and the work on defining basic cyber hygiene since then have changed this

Regulation is essential and well regulated sectors do better at cybersecurity than unregulated sectors or, in the case of the FCC, sectors that are weakly regulated. The counter to this is the Eureopan Union, where over-regulation has killed economic growth and digital innovation. Too much regulation or badly designed regulation creates economic damage; the absence of regulation harms national security. The issue whether Congress and the Federal government can design regulations that balance national security and economic growth and there are examples of success, such as TSA's work on cybersecurity after the Colonial Pipelines hack.

Overregulation is a serious risk, but this risk can be managed by relying on self-certification, accompanied by proof of the assertion of compliance that is then made public. This approach reduces the compliance burden without compromising performance and creates incentives for companies to improve their cybersecurity posture.

Question 2. What are the risks of overregulating the telecom sector in response to cyber incidents like "Salt Typhoon"?

Answer. Badly designed regulation imposes costs without providing security benefits. The chief risk facing the telecom sector is that their need for capital to build out 5G networks means they will need to choose between modernization and expending the financial resources to pay for better cybersecurity. One precedent could come from the Universal Service Fund. Another could be creating tax incentives for more spending cybersecurity. Both of these actions require Congressional action. Funding needs to be provided on a recurring basis.

Question 3. How can Congress support knowledge and threat-sharing across sectors to improve collective resilience against cyber threats?

Answer. Knowledge sharing by itself is worthless. Companies, especially small- and medium sized companies, lack the resources and incentives to act on the information. Confining Federal action to telling someone that their shop is in a bad neighborhood and they should watch out for criminals is an abdication of responsibility. Information sharing has to be tied to a regulatory structure that includes promulgation of best practices, oversight and monitoring, and penalties for non-compliance.

Deterring Nation-state attacks

During the hearing there was much discussion about the persistent nature of state-backed cyberattacks and the apparent increase in the brazenness of these attacks. Indeed, one witness called this latest attack, "the most serious intrusion against U.S. telecommunications networks that I have seen." A recurring theme throughout the hearing was the lack of effective deterrence against nation-backed cyberattacks.

Question 1. How can we most effectively deter nation-state attacks in the cyber domain?

Answer. Deterrence has failed entirely in cyberspace and the pursuit of deterrence has had a crippling effect on U.S. strategy and performance in international security. It condemns the U.S. to a reactive and passive posture which opponents easily exploit. U.S. deterrent threats are not credible. To restore credibility requires first abandoning the idea that opponents can be deterred and replacing it was the idea that the imposition of consequences on opponents that go beyond complaints or feeble sanctions will chance their calculations of the benefit of continued intrusions.

The steps needed for this are to first define a menu of effective consequences, communicate this to opponents (who will not believe the U.S. will take action) saying the U.S. will take action if they continue to hack, act, and then offer dialogue with opponents on what changes in their behavior we would like to see. This will take several cycles of warning, response, and negotiation and does not come without risk, but the alternative is to continue to be a victim.

RESPONSE TO WRITTEN QUESTIONS SUBMITTED BY HON. MARSHA BLACKBURN TO JAMES ANDREW LEWIS

Question 1. You've suggested that the U.S. response to Chinese cyber espionage has been overly restrained and advocate for measures such as targeting China's leadership, disrupting their cyber operations, or imposing harsher sanctions. What concrete actions could the U.S. prioritize to deter further cyber aggression from China?

Answer. Changing China's behavior will be difficult. The first steps are to engage them, warn them, and after they ignore the first warning (almost inevitable, after years of U.S. inactivity), take action that creates tangible effect. We will need to repeat this cycle for some period of time as the Chinese do not believe the U.S. will respond seriously. Tangible effects could include actions like leaking information on the covert wealth of the leadership (in the past, this has prompted a major reaction from the Chinese), disrupting the support infrastructure of Chinese hackers in China and outside, and taking more vigorous counter-intellignce actions (such as arrests or expulsions) in partnership with allies. An overly legalistic approach used by the U.S. is regarded by the Chinese (and other opponents) as a symptom of timidity. The goal is not deterrence but engagement to change behavior.

Question 2. How should Congress approach harmonizing cybersecurity regulations to ensure clarity, reduce compliance burdens, and enhance overall effectiveness? Are there specific frameworks or models you would recommend?

Answer. Regulatory harmonization is a task for the next National Cyber Director, since only the White House has the ability to direct multiple agencies to take action. DHS/CISA cannot do this as it lacks authority over other agencies. Congress should task the new Director to review all existing regulations to harmonize them and eliminate overlap. This is not a one-time exercise but something that Congress should mandate as an annual review. A good place to start is with the Director's confirmation hearing

Question 3. What broader structural or policy changes should be considered to enhance the Federal government's ability to respond to large-scale cyber threats effectively?

Answer. A broad approach would have the U.S. engage in a sustained, senior-level dialogue with China to change their behavior (and this will entail undertaking measures of "active defense"), develop regulatory standards to ensure minimum best practices are being observed (currently they are not in many companies), and build a common approach with other countries based on the multinational Counter Ransomware Initiative as a foundation

RESPONSE TO WRITTEN QUESTIONS SUBMITTED BY HON. ERIC SCHMITT TO
JAMES ANDREW LEWIS

Dr. James Lewis, Senior Vice President, Pritzker Chair, and Director of the Strategic Technologies Program, Center for Strategic and International Studies, Alexandria, VA

Question 1. Subsea cables are essential to global connectivity and cooperating with international allies is vital to ensuring their security. For example, Japan is a key partner in securing subsea cable infrastructure, especially given the strategic security challenges in the Indo-Pacific region and its role as a trusted supplier and ally. Australia has also been supportive of these trusted network initiatives. How do you view the importance of U.S. collaborations with allies like Japan and Australia in addressing these security risks, and what key areas should we prioritize to protect subsea cable infrastructure, especially in the event of a kinetic war with an adversary in the Indo-Pacific region?

Answer. Undersea cables are inherently indefensible, but several steps could reduce vulnerability. A first step would be to ensure a minimal degree of redundancy for vital communications. by building a more robust undersea cable infrastructure based on multiple cable systems and using satellites (which are inherently limited in capacity but much less vulnerable). Another steps is to increase repair capacity. A third step is to take legal action against ship owners and by intercepting and detaining ships suspected of disrupting undersea cables. This will require an increased degree of monitoring. If current laws are interpreted to preclude such actions, the laws should be changed.

The chief dilemma here is that undersea cable resilience requires doing more than the market alone would justify for both capacity and repair. The additional effort may require either incentives (possibly using tax breaks) or additional government spending to build a degree of redundancy. The additional cost is unfortunate, but required by the current international situation.

RESPONSE TO WRITTEN QUESTIONS SUBMITTED BY HON. TED CRUZ TO
JUSTIN SHERMAN

Cybersecurity and the Regulatory State

The long history of state-backed cyberattacks, particularly from the People's Republic of China, will surely not be the last. Cybersecurity is of critical importance. However, the Federal government has a poor track record of protecting against cyberattacks, and we should be cautious about placing too much faith in more regulation or reporting requirements.

Question 1. Are there ways to incentivize the adoption of better cybersecurity in the telecommunications sectors rather than reaching for the regulatory stick? For example, could we use regulatory or liability protections to align incentives and get companies to better protect their systems?

Answer. There is a considerable, ongoing debate about software cybersecurity liability and whether it would be an effective mechanism to ensure that companies with adequate investments in reasonable security can keep doing business, enhancing their security continually over time, while companies that fail to invest in reasonably adequate cybersecurity practices are penalized for their failures—and incentivized to do better going forward. Congress should consider this debate and the various proposals at hand. In areas that are particularly sensitive for public safety and national security, however, it is of the utmost importance for the United States to defend against serious, persistent threats—such as from the Chinese government—without expecting that all companies will make the adequate security investments themselves (*e.g.,* to protect Americans' data, to protect their own supply chains, to defend against Chinese state efforts to steal U.S. technology, etc.) without regulatory requirements or incentives.

Question 2. What are the risks of overregulating the telecom sector in response to cyber incidents like "Salt Typhoon"?

Answer. The challenge with cybersecurity—as with many other issues that are about risk—is finding balance. Because is impossible to prevent all incidents, one of the central questions for Congress right now should be identifying that right balance between not erroneously expecting all companies to be able to prevent all incidents all the time (and regulating against that) and recognizing that company under-investments in security and highly sophisticated threats (including from Beijing and Moscow) require the United States to raise the cybersecurity floor.

Question 3. How can Congress support knowledge and threat-sharing across sectors to improve collective resilience against cyber threats?

Answer. Congress should continue to work to ensure that companies sharing threat data with others in their sectors are able to do so quickly, effectively, and without undue fear of negative consequences from sharing that threat data, including with competitors. An ongoing challenge, on which I am happy to speak with your office further, is navigating public-private cyber threat-sharing in light of the sheer scale and scope of China's efforts to hack into American systems. The U.S. government sharing threat information with a small group of targeted companies is one thing, but it's another issue entirely when the number of potential companies, nonprofits, universities, individuals, and others targeted by a sophisticated threat actor such as the Chinese government is potentially endless (from the gaming and entertainment sectors to defense, tech, health, and more).

Deterring Nation-state attacks

During the hearing there was much discussion about the persistent nature of state-backed cyberattacks and the apparent increase in the brazenness of these attacks. Indeed, one witness called this latest attack, "the most serious intrusion against [] U.S. telecommunications networks that I have seen." A recurring theme throughout the hearing was the lack of effective deterrence against nation-backed cyberattacks.

Question 1. How can we most effectively deter nation-state attacks in the cyber domain?

Answer. As fellow witnesses noted in the hearing, there is a view that the United States can pursue deterrence by denial (such as by trying to deny a foreign adversary the ability to get into a particular network) or deterrence by punishment (such as by imposing economic costs on specific individuals and companies perpetrating cyber operations against the United States). In the former case, we should work to raise the cybersecurity floor as much as possible. While no company can guarantee that a foreign nation-state will never get into their networks, there are plenty of companies that could certainly make those intrusions less easy for the foreign nation-state—such as by implementing basic cybersecurity best-practices such as multi-factor authentication, robust encryption, strong access controls, continuous monitoring, supply chain due diligence, and other measures that are implemented by the companies with top security programs. In the latter case, it is probably long overdue to recognize that indictments of foreign nation-state hackers (while perhaps useful to document attacks, show an ability to attribute operations, etc.) is by and large not a serious cost, not going to result in their arrests, and not going to deter a persistent foreign threat actor such as the Chinese or Russian governments from continuing business-as-usual the next day. As was covered in the hearing, Congress could therefore consider what other measures—from sanctions to disruptive attacks like what was reported with U.S. Cyber Command and Russian operatives in 2018[1]—could disrupt and degrade ongoing nation-state operations against the United States. Additionally, it would help in future Congressional hearings, inquiries, and other efforts to continue to identify areas where foreign nation-states, such as Beijing, can easily infiltrate global tech supply chains and U.S. tech supply chains—and what can proactively be done about it.

RESPONSE TO WRITTEN QUESTIONS SUBMITTED BY HON. MARSHA BLACKBURN TO JUSTIN SHERMAN

Question 1. Your testimony highlights the strategic importance and vulnerabilities of undersea cables, including the risks of espionage or sabotage. For example, there have been reports of Chinese vessels allegedly dragging anchors to sever cables. Given that the U.S. relies heavily on foreign repair ships, what are the national security implications of this dependency? Should the U.S. invest in enhancing its own subsea cable repair capabilities, and if so, how?

Answer. It is critical that the United States, as a country, has the capacity to repair submarine cables even if other countries' repair ships are occupied by different incidents or priorities. The same goes for U.S. allies and partners. There is a risk that cables in critical areas could be intentionally damaged, and if this happens in

---

[1] Ellen Nakashima, "U.S. Cyber Command operation disrupted Internet access of Russian troll factory on day of 2018 midterms," *The Washington Post,* February 27, 2019, *https://www.washingtonpost.com/world/national-security/us-cyber-command-operation-disrupted-internet-access-of-russian-troll-factory-on-day-of-2018-midterms/2019/02/26/1827fc9e-36d6–11e9-af5b-b51b7ff322e9_*story.html.

a way that adversely impacts the United States, we need ships at the ready to respond without delay and to full effect. Even if damage is unintentional, cables could still need to be repaired quickly and in dangerous conditions (*e.g.,* what happened in the Red Sea with the Houthis), likewise necessitating the capacity to repair ships. Congress did important work in this area a couple of years ago in standing up and funding the Cable Ship Security Program. It may be important, in light of growing risks from China and Russia in particular, to reevaluate that program and if more funding or additional structures may be needed.

Question 2. When it comes to deterring cyber aggression by Russia, what strategies would you recommend to strengthen the U.S. posture and prevent future incidents?

Answer. Nobody is going to stop Russia (or China) from attempting to break into U.S. networks. But, as you note Senator, the United States can work to strengthen its cybersecurity posture and consider more options to potentially disrupt operations and shape how foreign threat actors design and execute their operations and attacks. In the former case, many companies still lack basic cybersecurity best-practices (like multi-factor authentication or strong access controls), and this remains a serious national security problem with critical infrastructure like our water treatment facilities and our electrical grids. As we have seen over and over, the nature of supply chains today means the weakest link in the chain can make the whole chain vulnerable. In the SolarWinds espionage campaign, for example, Russian government hackers targeted one weak company in the supply chain to get into a considerable range of other targets that otherwise had much higher security—but the weak link in the chain got them in.[2] So, ensuring cybersecurity best-practices across all industries and bolstering supply chain security is paramount. In the latter case, other witnesses noted in the hearing already that the United States and its allies and partners can have conversations about ways to better impose costs on foreign adversaries such as Russia—and ensuring that the United States is doing everything it can to shape Russia's cyber behavior. I have written at length on Russia's cyber ecosystem specifically and am happy to follow up further on this subject.

Question 3. What broader structural or policy changes should be considered to enhance the Federal government's ability to respond to large-scale cyber threats effectively?

Answer. Many new U.S. laws and regulations contain cybersecurity incident reporting requirements—which are important for notifying victims, alerting companies to potential compromise somewhere along their supply chain, creating data about incidents over time, informing the U.S. government of relevant problems, and more. But incident reporting in and of itself does not stop incidents in the first place, if those insights are not used in actionable ways—and if there are inadequate investments in overall security. Congress should consider requiring (in some ways) and heavily incentivizing (in other ways) stronger cybersecurity baselines for critical infrastructure sectors. It should similarly consider robust security requirements for all companies handling personal data (like Americans' geolocation data and genetic data, of high interest to actors like the Chinese government) as well as companies with proprietary information (like semiconductor designs, cybersecurity threat data, or source code for critical systems).

Question 4. How should Congress approach harmonizing cybersecurity regulations to ensure clarity, reduce compliance burdens, and enhance overall effectiveness? Are there specific frameworks or models you would recommend?

Answer. While some companies may advocate for a single Federal law over many state laws so they can push for a weaker overall baseline, it is also true that it's untenable for many companies—especially small-and medium-sized businesses that may be sophisticated but deal with smaller budgets and talent pools—to comply with highly complicated patchworks of overlapping laws, which are most navigable with large budgets and countless attorneys on hand. Simultaneously, as noted repeatedly in the hearing, considerable gaps remain in the U.S. cybersecurity regulatory landscape. I fully agree this is a serious policy issue. To better harmonize laws and regulations, Congress should start by looking at which areas of patchwork regulations are creating the highest costs to businesses and are creating the highest risk to the public and the country. These two categories may or may not overlap, but they will begin to give a better sense of which cybersecurity regulatory patchwork problems are highest-priority to address first.

---

[2] See, *e.g.,* Saheed Oladimeji and Sean Michael Kerner, "SolarWinds hack explained: Everything you need to know," Tech Target, November 3, 2023, *https://www.techtarget.com/whatis/feature/SolarWinds-hack-explained-Everything-you-need-to-know.*

RESPONSE TO WRITTEN QUESTIONS SUBMITTED BY HON. ERIC SCHMITT TO JUSTIN SHERMAN

Mr. Justin Sherman, Founder and CEO, Global Cyber Strategies, and Nonresident Senior Fellow, Atlantic Council, Washington, DC

Question 1. Can you talk about the value the CCP sees in controlling the global subsea cable architecture? And why is it important we work with our international partnerships as an avenue to shut out HMN Tech (Huawei Marine Networks)?

Answer. Submarine cables carry 99 percent of the world's intercontinental Internet traffic, are a potential surveillance goldmine, and play an even more important role in global telecommunications and Internet networks with the explosive growth of cloud services and AI/ML applications. There are many reasons for the Chinese government to want to have a role in shaping that network, from potentially compromising specific access points to spy on Internet traffic moving around the world, to viewing the construction of cables as a component of its Belt and Road Initiative and efforts to build infrastructure in countries around the world. Thankfully, U.S. efforts on HMN Tech are mostly a success story; the company has lost a large amount of market share in recent years. The problem is—to underscore your point, Senator, and as I noted in my oral and written testimony—that HMN Tech is hardly the only problematic Chinese company involved in the subsea cable supply chain. Others already present reason for concern and demand attention from Congress. I am happy to follow up further with your office on this subject.

Question 2. In terms of ensuring trusted vendors are laying these subsea cables and not China, are there immediate things the U.S. can do, potentially through permitting or procurement practices, that lighten the burden for trusted vendors to get their projects built from America to other parts of the world?

Answer. Yes. There is an important role for U.S. capacity-building in making sure that communications networks around the world are built in secure and resilient ways, whether the threats in question be a ship dragging an anchor and necessitating a repair, or a Russian government ship capable of going underwater and deliberately sabotaging a subsea cable. Working with allies and partners will further help promote awareness about the risks of using Chinese suppliers. The U.S. government should also be clear in its messaging about trusted vendors for the cable supply chain that its focus is on national security—such as encouraging other countries to avoid Chinese government repair ships that may be involved in espionage or supply chain compromise—and not engage in messaging that easily creates a perception overseas that the United States is attempting to use that security justification for purely economic reasons.

Question 3. President Trump, during his first administration, issued a critically important Executive Order formalizing the Team Telecom process. The President recognized the need to assess applications in a timely manner given the significant importance of subsea cables. During the Biden Administration, I'm told the timeline for processing applications has increased from 90 days to up to an unfathomable 3 years. This is unacceptable at a time when we are experiencing a significant need for increased capacity on our networks in light of AI and IoT—and perhaps more important is the global competition we are in to defeat China. While our applications wait for approval, China and Huawei are deploying cables at lightning speed and we are ceding the field. What can we do to restore timeliness to the process as President Trump envisioned?

Answer. This was indeed a critical executive order that recognized an essential program for U.S. national security. While I am not specifically familiar with the latest numbers on Team Telecom's application processing times, it is certainly important that programs like Team Telecom have the right processes, talent, and resources to be able to process applications on reasonably quick, fairly consistent, and transparent timelines. This is important for industry to have some level of transparency into, and to be able to expect some level of consistency from, such processes. It is also important for the U.S. government to be able to keep pace with Internet infrastructure development and with national security threats from foreign actors, such as the Chinese government. In my oral and written testimony, I noted that the Senate's 2020 bipartisan report on Team Telecom was viewed as an important and illuminating effort that informed thinking around President Trump's executive order as well as subsequent Congressional oversight and governing efforts. For what we can do now on the problem set, I would reiterate my recommendation that Congress initiate a lessons-learned report from Team Telecom to provide Congress and the public with major lessons learned in the design, administration, and threat analysis of its program since the 2020 E.O.—and describing priority areas and national security risks for the next decade.

RESPONSE TO WRITTEN QUESTIONS SUBMITTED BY HON. TED CRUZ TO TIM DONOVAN

Cybersecurity and the Regulatory State

The long history of state-backed cyberattacks, particularly from the People's Republic of China, will surely not be the last. Cybersecurity is of critical importance. However, the Federal government has a poor track record of protecting against cyberattacks, and we should be cautious about placing too much faith in more regulation or reporting requirements.

Question 1. Are there ways to incentivize the adoption of better cybersecurity in the telecommunications sectors rather than reaching for the regulatory stick? For example, could we use regulatory or liability protections to align incentives and get companies to better protect their systems?

Answer. CCA supports incentives, especially for smaller carriers and companies working to protect against cyberattacks, as opposed to additional regulations and potentially punitive enforcement actions. Additional regulation and regulatory penalties can take resources away from actually improving cybersecurity. CCA encourages policymakers to consider additional capacity building initiatives, flexible safe harbors, and Federal support mechanisms for smaller telecommunications providers to help them bolster cybersecurity where it is needed most.

Question 2. What are the risks of overregulating the telecom sector in response to cyber incidents like "Salt Typhoon"?

Answer. The burden smaller carriers face seeking to comply with the evolving security regulations from multiple Federal agencies, however well-intended, can quickly become overwhelmingly burdensome and potentially ineffective while diverting resources away from effectively responding to or avoiding cyber incidents. Minimizing the Federal agencies involved and synchronizing security-related requirements can reduce the associated regulatory burdens so providers with limited resources can use those resources to actually improve their network security.

Question 3. How can Congress support knowledge and threat-sharing across sectors to improve collective resilience against cyber threats?

Answer. For smaller and rural companies with fewer resources, security clearances, and technical expertise than larger, nationwide companies, the timely sharing of critical information and making sure it is actionable is critically important. Congressional efforts to lower the bar to participating in public/private information sharing activities, both within sectors and among sectors of the economy, could be helpful. This could include actions such as facilitating as-needed discussions for providers without security clearances, including one-day read-ins, increasing capacity building efforts, and more effectively centralizing Federal jurisdiction over cybersecurity issues. For the telecommunications sector, information sharing efforts targeting small and rural carriers like the Communications Supply Chain Risk Information Partnership (C-SCRIP) at the National Telecommunications and Information Administration (NTIA) are helpful and should be expanded, including appropriate resources to assist all carriers. Most small and rural carriers do not have the resources to participate in ongoing public/private initiatives on security such as the Department of Homeland Security's Cybersecurity & Infrastructure Security Agency (CISA) Communications Sector Coordinating Council. These carriers truly need engaged Federal partners, and they need access to the information and resources required for staying ahead of the seemingly never-ending game of security whack-a-mole.

Deterring Nation-state attacks

During the hearing there was much discussion about the persistent nature of state-backed cyberattacks and the apparent increase in the brazenness of these attacks. Indeed, one witness called this latest attack, "the most serious intrusion against [] U.S. telecommunications networks that I have seen." A recurring theme throughout the hearing was the lack of effective deterrence against nation-backed cyberattacks.

Question 1. How can we most effectively deter nation-state attacks in the cyber domain?

Answer. As network operators, CCA members play an important role of network defense as part of our Nation's cybersecurity policies, but cannot replace the overall strategy, posture, and roles of various Federal agencies. Carriers must have the resources and guidance from Federal partners to effectively secure their networks and continually upgrade, update, and patch their networks to support deterrence.

RESPONSE TO WRITTEN QUESTIONS SUBMITTED BY HON. MARSHA BLACKBURN TO TIM DONOVAN

Question 1. What unique challenges do small carriers face in meeting existing cybersecurity requirements, and how can policymakers address these issues without compromising security?

Answer. Smaller carriers often face challenges accessing actionable cybersecurity threat information from Federal partners and limited resources compared to nationwide carriers. For example, threat and incident information sharing from Federal agencies does not always incorporate smaller carriers at a level where they can either be proactive or mitigate a response with necessary precision. Further, smaller carriers generally lack staff with sufficient security clearances to participate meaningfully in cybersecurity-related information sharing. Smaller carriers also face challenges in terms of human and financial resources needed to ensure cybersecurity. Finally, smaller carriers face challenges in successfully balancing reporting requirements and resolving security issues given scarce resources. As breaches occur, it is important to balance alerting consumers and national security authorities with understanding and resolving threats. Policymakers can help address these issues through increased information sharing and providing additional resources and capacity building to smaller carriers to help bolster cybersecurity across the Nation.

Question 2. What broader structural or policy changes should be considered to enhance the Federal government's ability to respond to large-scale cyber threats effectively?

Answer. Policymakers could enhance the Federal government's ability to response to cyber threats by emphasizing the use of one centralized authority for cybersecurity in the United States. This would help focus attention and response activities, would facilitate clear and unambiguous guidance, and would also be more efficient in terms of resources. For example, CCA has encouraged the FCC to coordinate with CISA and industry-driven efforts instead of independently regulating. CCA has also encouraged CISA to synchronize its Cyber Incident Reporting for Critical Infrastructure Act (CIRCIA) reporting with the FCC's reporting requirements as encouraged by Congress.

Question 3. How should Congress approach harmonizing cybersecurity regulations to ensure clarity, reduce compliance burdens, and enhance overall effectiveness? Are there specific frameworks or models you would recommend?

Answer. In addition to the recommendations above, CCA encourages Congress to support efforts to increase collaboration between Federal agencies and industry to bolster network security and to remove barriers and uncertainty. This includes updates to information sharing, clear and consistent security requirements, increased participation in information-sharing by smaller companies, and a recognition of the unique challenges faced by smaller carriers, including limited resources.

RESPONSE TO WRITTEN QUESTIONS SUBMITTED BY HON. ERIC SCHMITT TO TIM DONOVAN

Question 1. I have sent letters to DHS and DoD regarding their efforts to identify and address the root issues that led to this extensive cyberattack. If China can penetrate our telecommunications networks for espionage, do you think their access could allow them to shut down cellular service for affected carriers? Could you discuss China's interest in exploiting vulnerabilities discovered by Salt Typhoon to launch an offensive cyber operation? Is this something we should be concerned about?

Answer. CCA members are very concerned about cyberattack capabilities that could potentially disrupt communications, including cellular services. CCA members rely on Federal partners to secure networks, including to address potential geopolitical motivations for exploitation. These attacks are not unique to telecommunications networks and policies to address concerns should take into consideration the myriad industries and services potentially vulnerable to attacks.

Question 2. Others at the hearing spoke about different network architectures that best protect against acts like Salt Typhoon. Let me ask you a hypothetical—If we are starting over and it is day one, how would you construct a secure network or what technology would you put in place to build the best network?

Answer. All carriers seek to have the resources and capabilities to source the most advanced equipment, updates, and services from the trusted vendors, as well as human and financial resources to implement cutting-edge best practices, continually monitor cybersecurity issues, and participate in public/private information sharing activities. This is not reality, however, and any network can become increasingly

vulnerable to attack as hackers test systems for potential intrusions like Salt Typhoon. One way to support secure networks and technologies going forward is to ensure predictable and sufficient support through the Universal Service Fund to preserve and expand connectivity with a focus on security.

Question 3. In my most recent letter to DoD,[1] I called on the Pentagon to establish stronger minimum cybersecurity requirements for contracted carriers. Do you believe enhanced minimum cybersecurity requirements would help mitigate attacks like Salt Typhoon? Are there any recommendations you can provide regarding ways to verify that enhanced minimum cybersecurity requirements are being upheld by contracted carriers?

Answer. Due to the interconnected nature of networks, a vulnerability anywhere in our Nation's networks is a potential vulnerability for all carriers. Security requirements should be actionable for all carriers, and Federal programs and contracts must ensure sufficient resources are available to prioritize security.

Question 4 a). Throughout your testimony and your exchange with my colleagues during the hearing, you stated that the challenges of defending against cyberattacks are insurmountable because defense requires protecting every part of the network. In contrast, an offensive cyberattack only needs to exploit a single vulnerability to gain access. You suggested that, no matter how much we spend or regulate, we may never fully protect ourselves from state actors like Salt Typhoon. In your professional opinion, what could effective deterrence in cyberspace look like?

Answer. All CCA members work diligently every day to ensure that their networks are safe for their customers, using the best information available. Defending networks is a critical part of deterrence and should be prioritized with support and guidance for carriers from Federal partners as part of our Nation's overall deterrence strategies.

Question 4 b). You also mentioned that Russia, China, and Iran may not have reached America's "pain point" in cyberattacks, largely because the Biden Administration's expected response has not been clear to our adversaries. In cyber strategy, there are only two options to protect your networks: deterrence through denial—an issue I have raised with the DoD—and deterrence through punishment. What does a well-balanced deterrence strategy based on both punishment and denial look like? How far off are we currently on the appropriate mix of denial and punishment? Additionally, what responses do you believe would be adequate for an incident like Salt Typhoon where the PRC targeted civilian infrastructure?

Answer. As network operators, CCA members play an important role of network defense as part of our Nation's cybersecurity policies, but cannot replace the overall strategy, posture, and roles of the Department of Defense and other Federal agencies.

○

[1] *https://www.schmitt.senate.gov/media/press-releases/following-devastating-salt-typhoon-hack-schmitt-and-wyden-call-on-pentagon-to-aggressively-prioritize-telecom-security-in-wake-of-historic-salt-typhoon-attack/*