GLOBAL NETWORKS AT RISK: SECURING THE FUTURE OF COMMUNICATIONS INFRASTRUCTURE

HEARING

BEFORE THE

SUBCOMMITTEE ON COMMUNICATIONS AND TECHNOLOGY

OF THE

COMMITTEE ON ENERGY AND COMMERCE

HOUSE OF REPRESENTATIVES

ONE HUNDRED NINETEENTH CONGRESS

FIRST SESSION

APRIL 30, 2025

Serial No. 119–17

Published for the use of the Committee on Energy and Commerce

govinfo.gov/committee/house-energy
energycommerce.house.gov

U.S. GOVERNMENT PUBLISHING OFFICE

60–348 PDF WASHINGTON : 2025

COMMITTEE ON ENERGY AND COMMERCE

BRETT GUTHRIE, Kentucky
Chairman

ROBERT E. LATTA, Ohio
H. MORGAN GRIFFITH, Virginia
GUS M. BILIRAKIS, Florida
RICHARD HUDSON, North Carolina
EARL L. "BUDDY" CARTER, Georgia
GARY J. PALMER, Alabama
NEAL P. DUNN, Florida
DAN CRENSHAW, Texas
JOHN JOYCE, Pennsylvania, *Vice Chairman*
RANDY K. WEBER, SR., TEXAS
RICK W. ALLEN, Georgia
TROY BALDERSON, Ohio
RUSS FULCHER, Idaho
AUGUST PFLUGER, Texas
DIANA HARSHBARGER, Tennessee
MARIANNETTE MILLER-MEEKS, Iowa
KAT CAMMACK, Florida
JAY OBERNOLTE, California
JOHN JAMES, Michigan
CLIFF BENTZ, Oregon
ERIN HOUCHIN, Indiana
RUSSELL FRY, South Carolina
LAUREL M. LEE, Florida
NICHOLAS A. LANGWORTHY, New York
THOMAS H. KEAN, JR., New Jersey
MICHAEL A. RULLI, Ohio
GABE EVANS, Colorado
CRAIG A. GOLDMAN, Texas
JULIE FEDORCHAK, North Dakota

FRANK PALLONE, JR., New Jersey
Ranking Member
DIANA DEGETTE, Colorado
JAN SCHAKOWSKY, Illinois
DORIS O. MATSUI, California
KATHY CASTOR, Florida
PAUL TONKO, New York
YVETTE D. CLARKE, New York
RAUL RUIZ, California
SCOTT H. PETERS, California
DEBBIE DINGELL, Michigan
MARC A. VEASEY, Texas
ROBIN L. KELLY, Illinois
NANETTE DIAZ BARRAGÁN, California
DARREN SOTO, Florida
KIM SCHRIER, Washington
LORI TRAHAN, Massachusetts
LIZZIE FLETCHER, Texas
ALEXANDRIA OCASIO-CORTEZ, New York
JAKE AUCHINCLOSS, Massachusetts
TROY A. CARTER, Louisiana
ROBERT MENENDEZ, New Jersey
KEVIN MULLIN, California
GREG LANDSMAN, Ohio
JENNIFER L. MCCLELLAN, Virginia

PROFESSIONAL STAFF

MEGAN JACKSON, *Staff Director*
SOPHIE KHANAHMADI, *Deputy Staff Director*
TIFFANY GUARASCIO, *Minority Staff Director*

SUBCOMMITTEE ON COMMUNICATIONS AND TECHNOLOGY

RICHARD HUDSON, North Carolina
Chairman

RICK W. ALLEN, Georgia, *Vice Chairman*
ROBERT E. LATTA, Ohio
GUS M. BILIRAKIS, Florida
EARL L. "BUDDY" CARTER, Georgia
NEAL P. DUNN, Florida
JOHN JOYCE, Pennsylvania
RUSS FULCHER, Idaho
AUGUST PFLUGER, Texas
KAT CAMMACK, Florida
JAY OBERNOLTE, California
ERIN HOUCHIN, Indiana
RUSSELL FRY, South Carolina
THOMAS H. KEAN, JR., New Jersey
CRAIG A. GOLDMAN, Texas
JULIE FEDORCHAK, North Dakota
BRETT GUTHRIE, Kentucky (ex officio)

DORIS O. MATSUI, California
Ranking Member
DARREN SOTO, Florida
YVETTE D. CLARKE, New York
RAUL RUIZ, California
SCOTT H. PETERS, California
DEBBIE DINGELL, Michigan
ROBIN L. KELLY, Illinois
NANETTE DIAZ BARRAGÁN, California
TROY A. CARTER, Louisiana
ROBERT MENENDEZ, New Jersey
GREG LANDSMAN, Ohio
JENNIFER L. MCCLELLAN, Virginia
KATHY CASTOR, Florida
FRANK PALLONE, JR., New Jersey *(ex officio)*

C O N T E N T S

GLOBAL NETWORKS AT RISK: SECURING THE FUTURE OF COMMUNICATIONS INFRASTRUCTURE

WEDNESDAY, APRIL 30, 2025

HOUSE OF REPRESENTATIVES,
SUBCOMMITTEE ON COMMUNICATIONS AND TECHNOLOGY,
COMMITTEE ON ENERGY AND COMMERCE,
Washington, DC.

The subcommittee met, pursuant to notice, at 10:05 a.m., in room 2322, Rayburn House Office Building, Hon. Richard Hudson (chairman of the subcommittee) presiding.

Members present: Representatives Hudson, Allen, Latta, Bilirakis, Carter of Georgia, Dunn, Joyce, Fulcher, Pfluger, Obernolte, Fry, Kean, Goldman, Fedorchak, Guthrie (ex officio), Matsui (subcommittee ranking member), Soto, Clarke, Peters, Dingell, Barragán, Carter of Louisiana, Menendez, Landsman, McClellan, Castor, and Pallone (ex officio).

Staff present: Sydney Greene, Director, Finance and Logistics; Kate Harper, Chief Counsel, Communications and Technology; Brittany Havens, Chief Counsel, Oversight and Investigations; Megan Jackson, Staff Director; John Lin, Senior Counsel, Communications and Technology; Sarah Meier, Counsel and Parliamentarian; Elaina Murphy, Professional Staff Member, Communications and Technology; Dylan Rogers, Professional Staff Member; Emma Schultheis, Clerk, Health; and Kaley Stidham, Press Assistant; Hannah Anton, Minority Policy Analyst; Keegan Cardman, Minority Staff Assistant; Parul Desai, Minority Chief Counsel, Communications and Technology; Tiffany Guarascio, Minority Staff Director; Dan Miller, Minority Professional Staff Member; Michael Scurato, Minority FCC Detailee; and Johanna Thomas, Minority Counsel.

Mr. HUDSON. The subcommittee will come to order.

The Chair recognizes himself for an opening statement.

OPENING STATEMENT OF HON. RICHARD HUDSON, A REPRESENTATIVE IN CONGRESS FROM THE STATE OF NORTH CAROLINA

Good morning. Welcome to today's subcommittee hearing on "Global Networks at Risk: Securing the Future of Communications Infrastructure." This topic has never been more pressing. The United States is home to the world's leading companies and innovators who are driving the development of cutting-edge technologies, like artificial intelligence, the Internet of Things, and

next-generation wireless technologies. These innovations are critical not just to our economy but the future of global connectivity.

Communications are also central to our national defense. This is a top of mind for me, especially as the Representative of Fort Bragg, home of the U.S. Army Special Forces and largest military base in the world. Connectivity and secure communication networks are vital to maintaining our defense capabilities and keeping our Nation safe.

Today, we rely on communications infrastructure in nearly every sector of our economy. As Americans become more connected, it is increasingly important the equipment we buy, the networks we rely on are secure, resilient, and protected from malicious actors.

Unfortunately, the security of these networks is under threat. The Chinese Communist Party, for example, has been investing heavily to develop unsecure communications equipment and export it around the world to assist in their espionage activities, including in the United States. The known vulnerabilities in many technologies produced by foreign adversaries pose a direct threat to the national security of the United States.

Last fall, we learned about Salt Typhoon, which may be the largest Chinese-backed telecommunications hack in our Nation's history. These hackers infiltrated U.S. telecommunications companies' networks impacting at least nine providers. This infiltration enabled the hackers to geolocate millions of individuals and record phone calls and impacted senior U.S. officials, including then-President-elect Trump and Vice President-elect Vance.

In addition to these vulnerabilities, there are an increasing number of physical attacks on communications infrastructure, such as undersea cables. These cables are responsible for carrying data traffic across oceans and are susceptible to damage by the elements and unintentional acts, such as anchors dragging along the sea floor. But they have also been intentionally sabotaged, and because of their physical location under the ocean, it can be difficult to monitor unauthorized access to these cables.

We must take decisive steps to address these threats. I was proud to support funding for the Secure and Trusted Communications Network Reimbursement Program, which will support the removal of the remaining Chinese equipment in our communications networks.

Another key aspect of securing our communications infrastructure is the review of foreign investments in U.S. networks. Team Telecom is an interagency working group that reviews foreign investments in certain communications applications that come before the FCC. Team Telecom assesses the national security risks, law enforcement, and other policy considerations that may be associated with such investments. While this process is important, applications often get bogged down by delays and bureaucratic hurdles. We must find ways to make sure the national security concerns are addressed without hindering deployment.

Satellite technology also plays an increasingly important role in our communications infrastructure. Satellites provide broadband services as well as mission-critical services to critical infrastructure companies and the Federal Government. Yet, the regulations gov-

erning the satellite operations have not kept pace with the growth in the industry.

Last Congress, this committee led bipartisan legislation to streamline regulatory processes for satellite operators, and the Federal Communications Commission adopted many of those reforms. But more work remains to provide clarity and more certainty in the licensing process to ensure the U.S. remains a leader in this sector as well.

We must meet these challenges head on. Innovation has provided untold benefits to Americans and to our economy. I look forward to hearing from the witnesses today about these issues.

[The prepared statement of Mr. Hudson follows:]

Opening Statement for Chairman Richard Hudson
Subcommittee on Communications and Technology
"Global Networks at Risk: Securing the Future of Communications Infrastructure"
Wednesday, April 30, 2025 at 10:00 AM

Introduction

Good morning, and welcome to today's subcommittee hearing on Global Networks at Risk: Securing the Future of Communications Infrastructure.

This topic has never been more pressing. The United States is home to the world's leading companies and innovators who are driving the development of cutting-edge technologies like artificial intelligence, the Internet of Things, and next-generation wireless technologies. These innovations are critical not just to our economy, but to the future of global connectivity.

Communications are also central to our national defense. This is top of mind for me, especially as the Representative for Fort Bragg — home to the U.S. Special Forces and the largest military base in the

world. Connectivity and secure communications networks are vital to maintaining our defense capabilities and keeping our nation safe.

Today, we rely on communications infrastructure in nearly every sector of our economy. As Americans become more connected, it is increasingly important the equipment we buy and the networks we rely on are secure, resilient, and protected from malicious actors.

Unfortunately, the security of these networks is under threat.

The Chinese Communist Party (CCP), for example, has been investing heavily to develop unsecure communications equipment and export it around the world to assist in their espionage activities, including in the United States. The known vulnerabilities in many technologies produced by foreign adversaries pose a direct threat to the national security of the United States.

Last fall, we learned about Salt Typhoon, which may be the largest Chinese-backed telecommunications hack in our nation's history. These

hackers infiltrated U.S. telecommunications companies' networks, impacting at least nine providers. This infiltration enabled the hackers to "geolocate millions of individuals and record phone calls," and impacted senior U.S. officials, including then- President-elect Trump and Vice President-elect Vance.[1]

In addition to these vulnerabilities, there are an increasing number of physical attacks on communications infrastructure, such as undersea cables. These cables are responsible for carrying data traffic across oceans and are susceptible to damage by the elements and unintentional acts, such as anchors dragging along the seafloor. But they have also been intentionally sabotaged and because of their physical location under the ocean, it can be difficult to monitor unauthorized access to these cables.

[1] Rosie Perper, *Chinese hackers used broad telco access to geolocate millions of Americans and record phone calls*, Politico (December 27, 2024), https://www.politico.com/news/2024/12/27/chinese-hackers-telco-access-00196082

We must take decisive steps to address these threats. I was proud to support funding for the Secure and Trusted Communications Networks Reimbursement Program, which will support the removal of the remaining Chinese equipment in our communications networks.

Another key aspect of securing our communications infrastructure is the review of foreign investments in U.S. networks. “Team Telecom” is an interagency working group that reviews foreign investments in certain communications applications that come before the FCC.

Team Telecom assesses the national security risks, law enforcement, and other policy considerations that may be associated with such investments. While this process is important, applications often get bogged down by delays and bureaucratic hurdles. We must find ways to make sure that national security concerns are addressed without hindering deployment.

Satellite technology also plays an increasingly important role in our communications infrastructure. Satellites provide broadband services, as well as mission critical services to critical infrastructure companies and the Federal government. Yet the regulations governing satellite operations have not kept pace with the growth in the industry.

Last Congress, this committee led bipartisan legislation to streamline regulatory processes for satellite operators, and the Federal Communications Commission adopted many of these reforms. But more work remains to provide clarity and more certainty in the licensing process to ensure the U.S. remains a leader in this sector.

Conclusion

We must meet these challenges head-on. Innovation has provided untold benefits to Americans and to our economy. I look forward to hearing from the witnesses today about these issues.

I now yield five minutes to my colleague, Ranking Member Doris Matsui, for her opening statement.

Mr. HUDSON. I now recognize the ranking member, Doris Matsui, for her opening statement. You are recognized.

OPENING STATEMENT OF HON. DORIS O. MATSUI, A REPRESENTATIVE IN CONGRESS FROM THE STATE OF CALIFORNIA

Ms. MATSUI. Thank you very much, Mr. Chairman.

Today's hearing comes on the heels of Salt Typhoon, one of the worst hacks of U.S. history. Salt Typhoon is a wakeup call that drives home the vulnerabilities in our communications networks. These networks are the backbone of modern life, connecting us to businesses, public safety, healthcare, education, and communities. That is what makes them such a ripe target for attack by malicious actors, and why we must strengthen how we protect this critical infrastructure.

Yet, I fear that we are moving backwards as the Trump administration won't even own up to its own pattern of security failures. President Trump is defending the indefensible, rallying behind the blunders of his Secretary of Defense, who leaked classified war plans to his wife and brother over an unsecured Signal chat. Likewise, he is standing blindly by his National Security Advisor and countless other senior officials who use Signal and personal Gmail accounts to conduct sensitive Government business.

The Trump administration is handing highly sensitive data to deeply unserious people who can't be bothered to follow the law or basic common sense when it comes to protecting cybersecurity and keeping sensitive information safe. The world is watching. Bad actors are ready to take advantage of this administration's gross incompetence.

In Congress, my Republican colleagues talk tough about protecting America against foreign adversaries, but talk is cheap. Their refusal to hold the Trump administration accountable despite serious security breaches speaks volumes. Republicans are also staying silent as President Trump slashes our Federal cyber workforce, gutting our Nation's capability to prepare for and respond to attacks on our critical infrastructure.

As one of his earliest acts in office, President Trump disbanded the Cyber Safety Review Board, leaving in limbo our investigation into the largest telecommunications hack in U.S. history. Instead, Salt Typhoon remains active as this administration jeopardizes our Government's ability to assess the damage and work on solutions.

As President Trump is wreaking havoc on our critical communications infrastructure with his destructive tariffs, rather than boosting U.S. companies, his tariffs have driven up cost and damaged supply chains at exactly the wrong time. Meanwhile, Democrats have been working diligently to increase network safety and protect American's information.

As coauthor of the Secure and Trusted Communications Network Act, I have been a staunch advocate of securing our network supply chain. Last Congress, we secured the last $3 billion to fully fund the Rip-and-Replace Program and remove vulnerable Chinese equipment from our telecommunications infrastructure. I urge our agencies to ensure smooth and timely completion of this national security imperative.

I have been dedicated to advancing innovations such as open radio access networks, or open RAN, to bolster our supply chain diversity. And earlier this week, the FUTURE Networks Act passed the House. This bill would bring the brightest minds across industry, academia, and government to collaborate on the development of our next-generation wireless technologies, including identifying supply chain and cybersecurity vulnerabilities so that we can more effectively prevent them.

These are important steps to strengthen network security, and we must build on this work as America faces growing cyber threats. This is not the time for inaction. I urge my Republican colleagues to speak up and hold the administration accountable for security failures. We must work on bipartisan solutions to secure our communications networks as our subcommittee has historically done.

I look forward to hearing from our witnesses on how we can proactively protect against future attacks.

[The prepared statement of Ms. Matsui follows:]

Committee on Energy and Commerce

Opening Statement as Prepared for Delivery
of
Subcommittee on Communications and Technology Ranking Member Doris Matsui

Subcommittee on Communications and Technology Hearing on "Global Networks at Risk: Securing the Future of Telecommunications Infrastructure"

April 30, 2025

Thank you, Chairman Hudson.

Today's hearing comes on the heels of Salt Typhoon, one of the worst hacks in U.S. history.

Salt Typhoon is a wake-up call that drives home the vulnerabilities in our communications networks.

These networks are the backbone of modern life– connecting us to businesses, public safety, healthcare, education, and communities.

That's what makes them such a ripe target for attack by malicious actors. And why we must strengthen how we protect this critical infrastructure.

Yet, I fear that we are moving backwards, as the Trump administration won't even own up to its pattern of security failures.

President Trump is defending the indefensible—rallying behind the blunders of his Secretary of Defense, who leaked classified war plans to his wife and brother over an unsecured Signal chat.

Likewise, Trump is standing blindly by his National Security Advisor, and countless other senior officials, who used Signal and personal Gmail accounts to conduct sensitive government business.

The Trump administration is handing highly sensitive data to deeply unserious people, who can't be bothered to follow the law—or basic common sense—when it comes to protecting cybersecurity and keeping sensitive information safe.

The world is watching. Bad actors are ready to take advantage of this administration's gross incompetence.

In Congress, Republicans talk tough about protecting America against foreign adversaries. But talk is cheap. Their refusal to hold the Trump administration accountable—despite serious security breaches—speaks volumes.

Republicans are also staying silent as President Trump slashes our federal cyber workforce, gutting our nation's capability to prepare for and respond to attacks on our critical infrastructure.

As one of his earliest acts in office, President Trump disbanded the Cyber Safety Review Board, leaving in limbo our investigation into the largest telecommunications hack in U.S. history.

Instead, Salt Typhoon remains active, as this administration jeopardizes our government's ability to assess the damage and work on solutions.

And President Trump is wreaking havoc on our critical communication infrastructure with his destructive tariffs.

Rather than boosting U.S. companies, Trump's tariffs have driven up costs and damaged supply chains at exactly the wrong time.

Meanwhile, Democrats have been working diligently to increase network safety and protect Americans' information.

As co-author of the Secure and Trusted Communications Networks Act, I have been a staunch advocate of securing our network supply chain.

Last Congress, we secured the last $3 billion to fully fund the Rip and Replace program and remove vulnerable Chinese equipment from our telecommunications infrastructure. I urge our agencies to ensure smooth and timely completion of this national security imperative.

I have been dedicated to advancing innovations such as open radio access networks, or Open RAN, to bolster our supply chain diversity.

And earlier this week, my bill, the FUTURE Networks Act, passed the House. This bill would bring the brightest minds across industry, academia, and the government to collaborate on the development of our next generation wireless technologies. Including identifying supply chain and cybersecurity vulnerabilities, so that we can more effectively prevent them.

These are important steps to strengthen network security. And we must build on this work, as America faces growing cyberthreats.

This is not the time for inaction. I urge my Republican colleagues to speak up and hold the Trump administration accountable for security failures.

We must work on bipartisan solutions to secure our communications networks, as our Subcommittee has historically done.

I look forward to hearing from our witnesses on how we can proactively protect against future attacks.

And with that, I yield the balance of my time…

Ms. MATSUI. And with that, I yield the balance of my time.

Mr. HUDSON. Thank you.

I now recognize the chairman of the full committee, the gentleman from Kentucky, for 5 minutes for his opening statement.

OPENING STATEMENT OF HON. BRETT GUTHRIE, A REPRESENTATIVE IN CONGRESS FROM THE COMMONWEALTH OF KENTUCKY

Mr. GUTHRIE. Thank you. Thank you, Chair Hudson. I appreciate the opportunity to be here for this important hearing.

Americans are connected to internet in nearly every aspect of their daily lives. Whether it is work, staying in touch with loved ones, or receiving healthcare, reliable connectivity is essential. The underlying communications infrastructure is what allows Americans in businesses of all sizes to utilize the many digital services that have redefined our economy in society. And while reliable access is important, it must also be secure. That is why today's hearing is very important.

Sophisticated cyber actors, specifically the governments of China, Russia, North Korea, and Iran, directly engage in activities aimed at infiltrating our critical infrastructure, especially our communications networks. These state adversaries and other malicious cyber actors continuously seek to exploit weaknesses in our networks, not only to steal sensitive data and commit fraud against Americans, but they also stand to gain sensitive business and government information as they seek to establish footholds for surveillance in future exploitation.

We have seen these efforts play out in recent attacks. We only have to point back to October when Chinese hackers breached the American court wiretap system. Our adversaries could also have the capability to cut off our communication services altogether, and think about how disruptive and devastating that would be for society.

Our networks are vulnerable to physical disruptions. For instance, fiber cuts can take months to repair, depending on where they are located, and if we are talking about subsea cables that are isolated in the ocean, these cuts could interrupt international data flows and result in degraded service for millions of people over an extended period of time, given the relative difficulty of repair.

Increasingly, satellite-provided services are being used to help close the digital divide and provide positioning navigation and timing data for government and private-sector uses. Foreign adversaries, again, like China and Russia, are reportedly developing antisatellite capabilities, which would cause serious disruption to critical services.

And in the case of GPS, a satellite-provided service, we have very few alternatives. Disruption to these critical communication services has the potential to cause chaos here in the homeland and reverberate throughout the economy. It could also give our adversaries the ability to disrupt American military mobilization in the event of conflict or attack.

Securing our communications systems from bad actors has been a longstanding priority—bipartisan priority of this committee and is essential to preserving our national economic security. This com-

mittee led the effort to rip and replace untrusted vendor equipment from our mobile networks by passing the Secure and Trusted Communications Networks Act. We built on these efforts by passing USA Telecommunications Act in 2020 to foster a more competitive market for trusted equipment vendors by promoting open RAN technology. More work remains to protect our critical infrastructure and harden these essential services against adversarial threats.

Thank you to the witnesses for your participation. I look forward to hearing from you about how to protect our communications infrastructure and ensure that the U.S. is prepared to defend against the CCP and any other adversaries. I really appreciate you all being here today, and I look forward to the discussion.

[The prepared statement of Mr. Guthrie follows:]

Opening Statement of Chairman Brett Guthrie
Subcommittee on Communications and Technology
"Global Networks at Risk: Securing the Future of Communications Infrastructure"
Wednesday, April 30, 2025 at 10:00 AM

Thank you, Chairman Hudson for holding this important hearing on the resilience of our communications infrastructure.

Americans are connected to the internet in nearly every aspect of their daily lives. Whether it is for work, staying in touch with loved ones, or receiving healthcare, reliable connectivity is essential. The underlying communications infrastructure is what allows individual Americans and businesses of all sizes to utilize the many digital services that have redefined our economy and society, even if we take them for granted.

Having worked in my family's manufacturing business, I can tell you that it is impossible to operate a business of any size today without access to the internet.

While reliable internet access is important, it must also be secure. That's why this hearing today is so important.

Sophisticated cyber actors, specifically the governments of China, Russia, North Korea, and Iran, directly engage in activities aimed at infiltrating our critical infrastructure, especially our communications networks. These state adversaries and other malicious cyber actors continuously seek to exploit weaknesses in our networks not only to steal sensitive data and commit fraud against Americans, but they also stand to gain sensitive business and government information as they seek to establish footholds for surveillance and future exploitation.

We have seen these efforts play out in recent attacks. We only have to point back to October when Chinese hackers breached the American court wiretap systems. Thankfully, we have so far avoided the worst of the potentially devastating outcomes. But depending on how far they were able to penetrate our networks, our adversaries could also have the capability to cut off our communications services altogether. In other words, they could shut down our mobile and fiber networks, preventing our cell phones and other devices from working. Think about how disruptive—and devastating—that would be to our society.

Our networks are also vulnerable to physical disruptions. For instance, fiber cuts can take months to repair depending on where they're located and even the time of year. If we're talking about subsea cables that are isolated in the ocean, for example, these cuts could interrupt international data flows and result in

degraded service for millions of people over an extended period of time given the relative difficulty of repair.

Increasingly, satellite-provided services are being used to help close the digital divide, and provide positioning, navigation, and timing data for government and private sector users. Foreign adversaries like China and Russia are reportedly developing anti-satellite capabilities, which would cause serious disruption to critical services. In the case of GPS, a satellite-provided service, we have very few alternatives. Disruption to these critical communications services has the potential to cause chaos here in the homeland and reverberate throughout the economy. It could also give our adversaries the ability to disrupt American military mobilization in the event of a conflict or attack.

Securing our communications systems from bad actors has been a longstanding bipartisan priority of this Committee and is essential to preserving our national and economic security. This Committee led the effort to rip and replace untrusted vendor equipment from our mobile networks by passing the *Secure and Trusted Communications Network Act*. We built on those efforts by passing the *USA Telecommunications Act* in 2020 to foster a more competitive market of trusted equipment vendors by promoting Open RAN technology. By diversifying our supply chains and removing untrusted equipment, we can help make our mobile networks more resilient to supply chain shortages and bolster them against bad actors like the CCP and the companies affiliated with them.

More work remains to protect our critical infrastructure and harden these essential services against adversarial threats. We

must remain vigilant in protecting our national security, and that starts with understanding the threats and considering policy changes to counter them.

Thank you to the witnesses for your participation. I look forward to hearing from you about how to protect our communications infrastructure and ensure that the U.S. is prepared to defend against the CCP and other adversaries.

Mr. Chairman, I yield back.

Mr. GUTHRIE. And with that, Mr. Chairman, I will yield back.

Mr. HUDSON. The gentleman yields back.

I will now recognize the gentleman from New Jersey, the ranking member, for 5 minutes for your opening statement.

OPENING STATEMENT OF HON. FRANK PALLONE, JR., A REPRESENTATIVE IN CONGRESS FROM THE STATE OF NEW JERSEY

Mr. PALLONE. Thank you, Mr. Chairman.

While today's discussion is important and timely, I am worried that my Republican colleagues are failing to even acknowledge the unprecedented and troubling actions of the Trump administration that are putting our national security at risk. Defending our telecommunications infrastructure from our foreign adversaries and other bad actors is critically important. On a daily basis, our Nation's telecommunications networks carry enormous amounts of data that not only include our most personal information but also sensitive Government materials that any foreign nation would love to digest.

And late last year, we learned that SAC—no, Salt Typhoon, I am sorry, that Salt Typhoon, a cyber espionage operation backed by China, infiltrated several American telecommunications networks to gain access to detailed information on President Trump, former Vice President Harris, other political figures, and American surveillance information.

And that is why it is so disturbing to watch as the Trump administration has mishandled sensitive national security information. In one of the worst security failures in decades, Defense Secretary Hegseth last month shared highly sensitive war plans on Signal, an unofficial and unsecure messaging app. The unsecure group chat was created by National Security Advisor Waltz, and he inadvertently included a reporter in the chat. Hegseth also shared this same information in a separate chat with some family members.

Now, this reckless conduct put the lives of our American troops at risk, in my opinion. If any adversary got access to these messages, they could have shut down—or they could have shot down American planes or targeted American ships. And yet Secretary Hegseth continues to lead the Department of Defense. I don't know for how long, but it is an outrage, and shows that the administration doesn't take these threats very seriously.

And this is on top of the fact that Elon Musk and his DOGE minions are being given access, often unauthorized, to sensitive information and undermining American's security on a daily basis, and that could include our nuclear secrets. Musk and DOGE are also haphazardly and indiscriminately cutting and slashing important Government programs and experienced public servants, which is weakening our country, without any pushback from congressional Republicans.

And while President Trump likes to act tough against China, he is blatantly violating Congress' bipartisan TikTok legislation and continuing to allow the Chinese Communist Party to compromise American devices, harvest American's data, promote pro-Communist propaganda, and undermine American interests.

So securing our country's telecommunication networks and infrastructure is serious business, but the Trump administration is not taking the task seriously. Imposing arbitrary tariffs on telecommunications equipment and ships that are vital to enhancing the safety and security of our networks one day and then pausing them the next day is only causing chaos and confusion. The administration's actions are increasing the chances that our foreign adversaries and others attempt even larger-scale attacks on our telecommunications networks, which no one wants to see.

Despite President Trump's recklessness and my Republican colleagues' silence, today's hearing topic underpins a significant part of the American economy. From healthcare to energy to public safety, nearly every facet of American life relies on our Nation's telecommunications networks and infrastructure. And while the innovations and advancements that these networks enable us to do are remarkable, it also makes them and the devices that run on top of them targets.

So this will only increase as more devices in our homes are connected. If cars, television, home security systems, and more are connected to the internet, they are vulnerable to attacks. The reality means that our homes can now be attacked without anyone touching a single door or window.

So it is imperative that we understand the vulnerabilities and risks our networks and devices face to better protect our country and consumers from attack, and to keep up with the rapidly evolving technological landscape our Nation faces.

And I urge my Republican colleagues to stop these irresponsible budget reconciliation plans as well. Rather than using spectrum auction proceeds to fund giant tax breaks to American billionaires and big corporations, we should use the proceeds from spectrum to help fund Next Generation 9–1–1, which will enhance the safety of our energy networks and save countless American lives.

The Trump administration must also stop delaying sending States their funds from the BEAD Program. These funds will ensure reliable connectivity across the country, which is crucial for our national security and economic prosperity. The only person who benefits from these delaying tactics is Elon Musk, who is trying to get taxpayer money funneled to his Starlink service.

So I look forward, Mr. Chairman, to hearing from today's witnesses, and I do think this is an important hearing about our telecommunication infrastructure and devices.

[The prepared statement of Mr. Pallone follows:]

Committee on Energy and Commerce

Opening Statement as Prepared for Delivery
of
Ranking Member Frank Pallone, Jr.

Subcommittee on Communications and Technology Hearing on "Global Networks at Risk: Securing the Future of Telecommunications Infrastructure"

April 30, 2025

While today's discussion is important and timely, I am worried that my Republican colleagues are failing to even acknowledge the unprecedented and troubling actions of this Administration that are putting our national security at risk.

Defending our telecommunications infrastructure from our foreign adversaries and other bad actors is critically important. On a daily basis, our nation's telecommunications networks carry enormous amounts of data that not only include our most personal information, but also sensitive government materials that any foreign nation would love to digest.

Late last year, we learned that Salt Typhoon – a cyber espionage operation backed by China – infiltrated several American telecommunications networks to gain access to detailed information on President Trump, former Vice President Harris, other political figures, and American surveillance information.

That is why it is so disturbing to watch as the Trump Administration has mishandled sensitive national security information. In one of the worst security failures in decades, Defense Secretary Hegseth last month shared highly sensitive war plans on Signal – an unofficial and unsecure messaging app. The unsecure group chat was created by National Security Advisor Waltz and he inadvertently included a reporter in the chat. Hegseth also shared this same information in a separate chat with some family members. This reckless conduct put the lives of American troops at risk. If any adversary got access to these messages, they could have shot down American planes or targeted American ships. And yet Secretary Hegseth continues to lead the Department of Defense. It's an outrage and shows that the Administration doesn't take these threats seriously.

This is on top of the fact that Elon Musk and his DOGE minions are being given access – often unauthorized – to sensitive information and undermining Americans' security on a daily basis, and that could include our nuclear secrets. Musk and DOGE are also haphazardly and indiscriminately cutting and slashing important government programs and experienced public servants, which is weakening our country without any pushback from Congressional Republicans.

And while President Trump likes to act tough against China, he is blatantly violating Congress's bipartisan TikTok legislation and continuing to allow the Chinese Communist Party

to compromise Americans' devices, harvest Americans' data, promote pro-Communist propaganda, and undermine American interests.

Securing our country's telecommunications networks and infrastructure is serious business, but the Trump Administration is NOT taking this task seriously. Imposing arbitrary tariffs on telecommunications equipment and chips that are vital to enhancing the safety and security of our networks one day and then pausing them the next is only causing chaos and confusion. This Administration's actions are increasing the chances that our foreign adversaries and others attempt even larger scale attacks on our telecommunications networks, which no one wants to see.

Despite President Trump's recklessness and my Republican colleagues' silence, today's hearing topic underpins a significant part of the American economy. From health care, to energy, to public safety, nearly every facet of American life relies on our nation's telecommunications networks and infrastructure. While the innovations and advancements that these networks enable are remarkable, it also makes them – and the devices that run on top of them – targets.

This will only increase as more devices in our homes are connected. If cars, televisions, home security systems, and more are connected to the internet, they are vulnerable to attacks. This reality means that our homes can now be attacked without anyone touching a single door or window.

So, it is imperative that we understand the vulnerabilities and risks our networks and devices face to better protect our country and consumers from attack.

And to keep up with the rapidly evolving technological landscape our nation faces, I urge my Republican colleagues to stop their irresponsible budget reconciliation plans.

Rather than using spectrum auction proceeds to fund giant tax breaks for America's billionaires and big corporations, we should use the proceeds to help fund Next Generation 911, which will enhance the safety of our emergency networks and save countless American lives.

The Trump Administration must also stop delaying sending states their funds from the Broadband Equity, Access, and Deployment (BEAD) Program. These funds will ensure reliable connectivity across the nation, which is crucial for our national security and economic prosperity. The only person who benefits from these delaying tactics is Elon Musk, who is trying to get taxpayer money funneled to his Starlink service.

I look forward to hearing from today's witnesses about securing our telecommunications infrastructure, devices, and consumer data, and I yield back the balance of my time.

Mr. PALLONE. Thank you, Mr. Chairman. I yield back.

Mr. HUDSON. Thank you.

We have now concluded with Member opening statements. The Chair reminds Members that, pursuant to the committee rules, all Members' opening statements will be made part of the record.

We would like to thank our witnesses for being here today to testify before this subcommittee. Our witnesses will have 5 minutes to provide an opening statement, which will be followed by a round of questions from the members.

The witnesses here before us today are Tom Stroup, president of the Satellite Industry Association; David Stehlin, chief executive officer, Telecommunications Industry Association; Jamil " Ja-far"—or "Jaff-er." Jaffer, I apologize—founder and executive director, National Security Institute; and Laura Galante, former intelligence community cyber executive and Director, Cyber Threat and Intelligence Integration Center, Office of the Director of National Intelligence.

Mr. Stroup, you are recognized for 5 minutes for your opening statement.

STATEMENTS OF TOM STROUP, PRESIDENT, SATELLITE INDUSTRY ASSOCIATION; DAVID STEHLIN, CHIEF EXECUTIVE OFFICER, TELECOMMUNICATIONS INDUSTRY ASSOCIATION; JAMIL N. JAFFER, FOUNDER AND EXECUTIVE DIRECTOR, NATIONAL SECURITY INSTITUTE, GEORGE MASON UNIVERSITY SCALIA LAW SCHOOL; AND LAURA GALANTE, FORMER DIRECTOR, CYBER THREAT INTELLIGENCE INTEGRATION CENTER, OFFICE OF THE DIRECTOR OF NATIONAL INTELLIGENCE

STATEMENT OF TOM STROUP

Mr. STROUP. Chairman Hudson, Ranking Member Matsui, Chairman Guthrie, Ranking Member Pallone, and distinguished members of the subcommittee, thank you for inviting me to testify before you today. I am Tom Stroup, president of the Satellite Industry Association.

Satellites are the backbone of modern society. We rely on them for communications, position navigation and timing, and remote sensing across the globe. Satellites provide critical services to hundreds of millions of Americans and billions of people around the world every day. The companies represented by SIA are poised to provide resilient services in any situation to empower U.S. leadership and support U.S. citizens and allies in an interconnected and contested world.

We are at a time of tremendous innovation in the space industry with over 12,000 active satellites on orbit today and plans for tens of thousands more through the end of the decade. Satellite services support all 16 critical infrastructures, including through communications for emergency services, position navigation and timing for agriculture, resilience for global telecommunications, and remote sensing data to improve our national security.

Satellites are the fastest way to connect the unconnected, with multiple American companies providing high-speed internet and more launching in the near future. The satellite industry provides

FCC-defined broadband service today across the globe and is ready to bring the Nation into an interconnected future as a backbone for 5G, IoT, and AI technologies.

In addition, satellites play a critical role in preparation response and recovery from natural disasters, electrical outages, and terrorist attacks. Remote sensing data and analytics can help pinpoint and quantify initial damage assessments in the immediate aftermath of a disaster. Synthetic aperture radio satellites can see through clouds and allow the mapping of damaged regions when storms are still overhead. Furthermore, unlike terrestrial communications counterparts, satellite networks are not susceptible to damage from such disasters because the primary repeaters are on board the spacecraft and not part of the ground infrastructure.

In addition to the benefit of having its primary infrastructure in space, many communications satellite operators provide customer connectivity through multi-orbit services. These services marry the low latency of LEO systems with the ability of GEO systems to deliver large amounts of capacity in high-traffic areas. While both GEO and non-GEO systems have the ability to provide large amounts of capacity, the combined solutions offer the best of both systems, enhancing the resiliency and reliability of services.

Another recent development furthering network resiliency is the deployment of direct-to-device mobile satellite connectivity led through major partnerships between satellite operators and both wireless carriers and manufacturers, which greatly expand the range of communications available to mobile customers.

The satellite industry today is investing continuously to ensure it can address the challenges of the future and to make its technologies available to every American. Satellite companies are working to optimize the use of spectrum by investing in high-throughput satellites and flexible software-defined payloads that allow for instantaneous reallocation of spectrum resources and the mitigation of harmful interference. Satellite system operators are continuing to invest in network cybersecurity, including using AI for vulnerability testing. Launch costs have also declined dramatically, providing opportunities for rapid replenishment of satellite constellations.

While the U.S. has long led the space sector, China is closing the gap with similar investments in space technologies that will challenge our national security community while also undermining democracy around the globe. It is critical for Congress to support continued domestic innovation and avoid regulations that put U.S. providers on an unequal playing field internationally.

Our members are dedicated to advancing the national interests, ensuring competitiveness of satellite companies in the U.S. and globally, and driving progress for the benefit of all Americans.

In furtherance of these goals, we have five priorities: Number one, promote American space innovation through streamlined regulations without unnecessary red tape and bureaucracy; two, lead standards development internationally; third, enact effective space debris policies and rigorously advocate for adoption of similar policies in other countries and in international fora; fourth, streamline space system procurement for greater efficiency in government ac-

quisition; and finally, spur development in investment through access to sufficient spectrum resources.

I appreciate the opportunity to appear before you today on behalf of the satellite industry, and I look forward to your questions.

[The prepared statement of Mr. Stroup follows:]

House Energy & Commerce: Communications and Technology Subcommittee Hearing: "Global Networks at Risk: Securing the Future of Communications Infrastructure"

Summary of Testimony of Tom Stroup, Satellite Industry Association

Satellites are foundational to modern life, supporting global communications, navigation, remote sensing, and emergency response. SIA members provide critical, resilient services to Americans and allies worldwide, enabling U.S. leadership in an increasingly interconnected and contested world.

With over 12,000 active satellites and plans for many more, we are in an era of rapid innovation. Satellite services support all 16 critical infrastructure sectors, from emergency communications to precision agriculture and resilience for global telecommunications. Satellites are uniquely positioned to connect unserved populations and serve as a backbone for 5G, IoT, and AI technologies.

They also play a vital role in disaster response. Remote sensing satellites provide real-time damage assessments, and unlike terrestrial systems, satellite networks remain operational during disasters due to their space-based infrastructure.

Multi-orbit services, combining the strengths of low Earth orbit (LEO) and geostationary (GEO) satellites, enhance resiliency and performance. Direct-to-device satellite connectivity is expanding mobile coverage through partnerships with wireless carriers and manufacturers.

The industry is investing in advanced technologies such as high-throughput satellites, flexible software-defined payloads, and AI-powered cybersecurity tools. Declining launch costs further boost responsiveness and innovation.

While the U.S. has long led the space sector, China is closing the gap, with similar investments in space technologies that will challenge our national security community while also undermining democracy around the globe. It is critical for Congress to support continued domestic innovation and avoid regulations that put U.S. providers on an unequal playing field internationally.

SIA and its members have five main priorities for this administration: promote American space innovation through streamlined regulations, lead standards development internationally, enact effective space debris policies and rigorously advocate for adoption of similar policies in other countries and in international fora, streamline space system procurement for greater efficiency in government acquisition, and spur development and investment through access to sufficient spectrum resources.

House Energy & Commerce: Communications and Technology Subcommittee Hearing:

"Global Networks at Risk: Securing the Future of Communications Infrastructure"

Wednesday, April 30, 2025 10:00 AM

Testimony of Tom Stroup, Satellite Industry Association

Chairman Hudson, Ranking Member Matsui, and distinguished Members of the Subcommittee, thank you for inviting me to testify before you today. I am Tom Stroup, President of the Satellite Industry Association (SIA).[1] SIA is a U.S.-based trade association that represents leading satellite operators, service providers, manufacturers, launch services providers, space situational awareness companies, and ground equipment suppliers.

Satellites are the backbone of modern society. We rely on them for communications, position, navigation and timing, and remote sensing across the globe. Satellites provide critical services to hundreds of millions of Americans and billions of people around the world every day. The companies represented by SIA are poised to provide resilient services in any situation to

[1] SIA Executive Members include: Amazon; Comtech; DIRECTV; EchoStar Corporation; Eutelsat Group; HawkEye 360; Intelsat S.A.; Iridium Communications Inc.; Kratos Defense & Security Solutions; Ligado Networks; Lockheed Martin Corporation; Planet Labs PBC; SES Americom, Inc.; Spire Global Inc.; and Viasat Inc. SIA Associate Members include: The Aerospace Corporation; Artel, LLC; AST Space Mobile; Astranis Space Technologies Corp.; The Boeing Company; Eutelsat America Corp + OneWeb Technologies; ExoAnalytic Solutions; Integrasys; Kinematics; Kymeta Corporation; Omnispace; Ovzon; Panasonic Avionics Corporation; Skyloom; and Telesat.

empower U.S. leadership and support U.S. citizens and allies in an interconnected and contested world.

We are at a time of tremendous innovation in the space industry, with over 12,000 active satellites on orbit today and plans for tens of thousands more through the end of the decade.[2] Satellite services support all sixteen critical infrastructure sectors, including through communications for emergency services, positioning, navigation, and timing (PNT) for agriculture, resilience for global telecommunications, and remote sensing data to improve our national security.

Americans have long relied upon satellites to provide direct to home TV, satellite radio, and distribution of programming to cable companies as well as to TV and radio broadcasters. Satellites are the fastest way to connect the unconnected, with multiple American companies providing high-speed internet and more launching in the near future. The satellite industry provides FCC-defined broadband service today across the globe and is ready to bring the nation into an interconnected future as a backbone for 5G, IoT, and AI technologies. Satellites today provide anytime, anywhere global connectivity to consumers, utilities, supply chain logistics providers, the IoT community, cruise and other ships, airlines, and unmanned aerial vehicles.

In addition, satellites play a critical role in preparation, response, and recovery from natural disasters, electrical outages and terrorist attacks. Remote sensing data and analytics can help pinpoint and quantify initial damage assessments in the immediate aftermath of a disaster. Synthetic aperture radar satellites can see through clouds and allow the mapping of damaged

[2] BryceTech and Satellite Industry Association, internal research, April 4, 2025.

regions when storms are still overhead. Furthermore, unlike terrestrial communications counterparts, satellite networks are not susceptible to damage from such disasters because the primary repeaters are onboard the spacecraft and not part of the ground infrastructure. Hand-held terminals, portable Very Small Aperture Terminal (VSAT) antennas, and temporary fixed installations can all be rapidly brought into a post-disaster environment to provide support to relief and recovery efforts.

Unfortunately, no technology is able to provide 100% reliability. Fiber and cable systems are subject to cuts, both intentional and accidental, and wireless systems are subject to damage to transmitters during natural disasters as well as the loss of service if terrestrial connections are cut. Satellites provide critical back-up in such circumstances.

In addition to the benefit of having its primary infrastructure in space, many communications satellite operators provide customer connectivity needs through multi-orbit services. These services marry the low-latency of LEO systems with the ability of GEO systems to deliver large amounts of capacity in high-traffic areas. While both GEO and non-GEO systems have the ability to provide large amounts of capacity, the combined solutions offer the best of both systems, enhancing the resiliency and reliability of services.

Another recent development furthering network resiliency is the deployment of direct to device mobile satellite connectivity, led through major partnerships between satellite operators and both wireless carriers and manufacturers, which greatly expand the range of communications available to mobile customers.

Satellite technology is also making American agriculture more efficient and adaptable, providing resilience against international supply chain risks. Satellite broadband, for instance, enables remote farms with livestock sensors, soil monitors, and autonomous farming equipment in rural America, far beyond where terrestrial wireless and wireline can reach or make economic sense to deploy. Precision GPS and Earth observation technologies allow farmers to increase crop yield by optimizing use of fertilizer, pesticides, and herbicides, and applying site-specific treatments to fields. Satellite advances in weather forecasting help farmers prepare for drought, floods, and other adverse weather conditions.

The satellite industry today is investing continuously to ensure it can address the challenges of the future and to make its technologies available to every American. Satellite companies are working to optimize the use of spectrum, by investing in high-throughput satellites and flexible, software defined payloads that allow for instantaneous reallocation of spectrum resources and the mitigation of harmful interference. Costs are dropping for both space and ground systems through the use of modular satellites, digital engineering, intersatellite links, flat panel antennas and cloud-integrated ground stations, which minimize the need for expensive ground architecture. Satellite system operators are continuing to invest in network cybersecurity, including using AI for vulnerability testing. Launch costs have also declined dramatically, providing opportunities for rapid replenishment of satellite constellations.

SIA The voice of the satellite industry

The U.S. space and satellite industry is continuously gaining momentum, with employment growing to 373,000 jobs in 2023[3] and producing an estimated revenue of $118 billion in 2024.[4] However, this figure does not reflect revenues generated from businesses which rely on satellite services behind the scenes. Satellites remain a pillar of U.S. infrastructure, enabling the American economy in ways consumers might not be aware, such as supporting smartphone app transactions, to use just one example.

While the U.S. has long led the space sector, China is closing the gap, with similar investments in space technologies that will challenge our national security community while also undermining democracy around the globe. China's GPS rival Beidou provides free military-grade service to some of its allies. Chinese companies, with state support, have deployed remote sensing satellites that match or surpass American satellites in technical capability.[5] Chinese enterprises have planned multiple LEO broadband constellations of thousands of satellites, of which over seventy have already launched. As these services are offered below market rate or free of charge globally, these capabilities will come with backdoor security risks for China to exploit (as exist today with Huawei). It is critical for Congress to support continued domestic innovation and avoid regulations that put U.S. providers on an unequal playing field internationally.

---

[3] Patrick Georgi and Chris Surfield, *New and Revised Statistics for the U.S. Space Economy, 2012–2023* (Suitland, MD: Bureau of Economic Analysis, 2025), https://apps.bea.gov/scb/issues/2025/03-march/0325-space-economy htm.

[4] Satellite Industry Association and BryceTech, internal research, April 10, 2025.

[5] Kari A. Bingen, David Gauthier, and Madeleine Chang. *Gold Rush: The 2024 Commercial Remote Sensing Global Rankings* (Washington, DC: Center for Strategic and International Studies, 2024), https://www.csis.org/analysis/gold-rush-2024-commercial-remote-sensing-global-rankings

Our members are dedicated to advancing national interests, ensuring the competitiveness of satellite companies in the U.S. and globally, and driving progress for the benefit of all Americans. In furtherance of these goals, we have five priorities:

1. Promote American space innovation through streamlined regulations without unnecessary red tape and bureaucracy. Congress and the Administration should embrace policies in regulatory areas such as licensing and export controls that allow the market and consumers, not government regulators and policymakers, to choose "winners" and "losers."

2. Lead standards development internationally. In particular, strong U.S. leadership at the International Telecommunication Union (ITU) on spectrum matters has been critical to enabling US industry innovation and advancement. Without sustained investment and leadership by the United States in the ITU, others – particularly China – will fill the void, threatening U.S. national and economic security interests.

3. Enact effective space debris policies and rigorously advocate for adoption of similar policies in other countries and in international fora. That would include encouraging responsible behavior by China, which (contrary to industry norms) has been leaving the upper stages of rocket launchers in low Earth orbit. An appropriate pro-investment, stable and transparent regulatory environment for the commercial space industry, among other things, means ensuring that federal policies regarding orbital debris mitigation and remediation enable the U.S. to lead the international

commercial space industry, protect those operating in space from collisions and debris, and do not have unintended consequences.

4. Streamline space system procurement for greater efficiency in government acquisition. The U.S. government should continue its focus on investing in and procuring cutting-edge satellite capabilities from the commercial space sector, including hardware as well as remote sensing data and analytics, broadband, and other services.

5. Spur development and investment through access to sufficient spectrum resources. The U.S. should ensure sufficient spectrum allocations are available domestically and internationally to support innovative and rapidly growing commercial satellite operations.

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

Mr. HUDSON. Thank you.

Mr. Stehlin, you are recognized for 5 minutes for your opening statement.

STATEMENT OF DAVID STEHLIN

Mr. STEHLIN. Chairman Hudson, Vice Chair Allen, Ranking Member Matsui, and members of the subcommittee, my name is Dave Stehlin. I am the CEO of TIA, the Telecommunications Industry Association, and I appreciate the opportunity to speak about this important subject: Securing the future of telecommunications infrastructure so that Americans can depend on trusted, secure, resilient, high-speed networks.

For more than 85 years, TIA has, with our 400-member organizations, developed technical and process improvement standards and advanced new technologies that drive our economy and improve the lives of our citizens. TIA's current standards cover a wide range of areas, including data center infrastructure, cell tower structures, structured cabling, public safety and emergency responder radios, hearing aid compatibility with mobile devices, telecom quality management, and our most recent focus on cyber and supply chain security.

We are a technology-agnostic organization, meaning that we support all wire line, wireless, and satellite-trusted technologies. In short, TIA has nearly a century of experience in ensuring that communications networks are built efficiently and resiliently with trusted suppliers.

I have been the CEO of TIA for the past 5-plus years and have run both publicly traded and venture-backed telecom technology companies for the past 40 years. I have seen tremendous change in technology improvement, but I also recognize that security improvements always lag behind technology advancements. I have experienced firsthand how state-owned entities like Huawei operate on a global stage undermining a competitive market of trusted ICT vendors.

As a graduate of the Naval Academy and former Marine officer, I take national security very seriously, and I understand that the national security threat posed by entities controlled by our adversaries can cause dramatic and significant, long-lasting effects to our communications networks.

Every type of critical infrastructure, from electrical grid to water systems to emergency responders to the internet, all use similar information communications technologies and systems. Potential vulnerabilities in these systems have a broad impact due to the unique role played by communications networks in our infrastructure. Every one of CISA's 16 identified critical infrastructures uses fundamental ICT networks.

Network attacks come from many directions, including state-sponsored enemies, criminals, and terrorists. And while the attack possibilities are endless, we must have a defense in depth, which starts with supply chain security. We must ensure that the products and services that make up our networks are coming from trusted suppliers who can demonstrate that security is designed in. We must verify before trusting.

All of this is critical to the success of building trusted, resilient, and secure global networks. In this context, subsea cable systems are an area of growing concern. Across the globe, nefarious actors are increasingly disrupting networks by cutting cables and damaging the points where the cables come ashore. These subsea cable systems carry more than 99 percent of internet traffic across the continents, and more than $10 trillion of financial transactions. These cables are irreplaceable backbones of the global internet, and while satellite communications plays an integral role in our networks, the data capacities of subsea cables cannot be overstated.

Of course, in addition to these physical threats to our communication networks is the fundamental threat from untrusted software, hardware, and suppliers. As network architectures continue to advance and become more complex, the potential attack surface grows and expands as well. This gives bad actors, including those who are state sponsored by foreign adversaries, such as the CCP, more targets, for example, the recent Salt Typhoon attack.

The U.S. Government has a long and bipartisan recognition of the supply chain threat vulnerabilities posed to our Nation's infrastructure. The industry recognizes this, and that is one of the reasons we at TIA initiated and developed the industry's first supply chain security standard, SCS 9001, about 3 years ago. This standard was designed with input from our members and both the U.S. Government and trusted allied governments, and aligns and operationalizes the NIST Cybersecurity Framework, the Prague Principles, and many other guidelines.

SCS 9001 is a supply chain security management system intended to define and measure the requirements and controls for the design, development, production, and operations of ICT products and services. This is an effort that reaches beyond our domestic infrastructure, and TIA has been working with the Department of Commerce and the Department of State to help allied countries build trusted, wireless fiber and satellite networks.

We appreciate the leadership that this committee brings us and has demonstrated by holding this hearing, and I would like to thank you for your time.

[The prepared statement of Mr. Stehlin follows:]

Telecommunications Industry Association
1201 Wilson Boulevard, Floor 27
Arlington, VA 22209 | www.tiaonline.org

Executive Summary

David Stehlin, CEO of the Telecommunications Industry Association (TIA), will testify before the subcommittee on the importance of securing the future of telecommunications infrastructure. He will emphasize TIA's long history of developing standards and advancing technologies to improve the lives of citizens and drive the economy. Stehlin will highlight the growing complexity and reach of networks, particularly with the rise of connected IoT devices and cloud-based data centers. He will stress the need for supply chain security to ensure that products and services come from trusted suppliers, and the importance of building high-quality networks with security and resiliency in mind. Additionally, Stehlin will address the growing concern over subsea cable systems, which carry the majority of internet traffic and financial transactions across continents, and the challenges posed by nefarious actors disrupting these cables. He will discuss the threat from untrusted software, hardware, and suppliers, and the need for a public-private partnership to verify trust and continually improve network security. Stehlin will conclude by highlighting TIA's efforts to develop the SCS 9001 supply chain security standard and the importance of working with allied countries to build secure, global networks.

Written Testimony

Chairman Hudson, Vice Chairman Allen, Ranking Member Matsui, and members of the subcommittee - My name is David Stehlin, the CEO of the Telecommunications Industry Association (TIA). I appreciate the opportunity to speak to this Subcommittee about this important subject: Securing the Future of the Telecommunications Infrastructure, so that Americans can depend on trusted, secure, resilient, high-speed networks.

For more than 85 years, TIA has, with our 400 member organizations, developed technical and process improvement standards and advanced new technologies that drive our economy and improve the lives of our citizens. TIA’s current standards cover a wide range of areas, including Data center infrastructure, cell tower structures, structured cabling, public safety/ emergency responder radios, hearing aid compatibility with mobile devices, telecom quality management and our most recent focus on cyber and supply chain security.

Telecommunications Industry Association
1201 Wilson Boulevard, Floor 27
Arlington, VA 22209 | www.tiaonline.org

We are technology-agnostic, meaning that we support all wireline, wireless and satellite trusted technologies. In short, TIA has nearly a century of experience in ensuring that communications networks are built efficiently and resiliently with trusted suppliers.

I have been CEO of TIA for the past 5+ years and have run both publicly traded and venture-backed telecom technology companies over my 40 years in the industry. I've seen tremendous change and technology improvements, but I also recognize that security improvements always lag behind technology advancements.

I've experienced, firsthand, how state-owned entities like Huawei operate on the global stage, undermining a competitive market of trusted ICT vendors. As a graduate of the U.S. Naval Academy and a former Marine officer, I take the national security threat posed by entities controlled by our adversaries seriously, especially in light of the ever-growing critical role of communications networks.

The complexity and reach of networks have grown dramatically in the past decade, and that growth is accelerating. For example, the number of connected IoT devices in our homes already numbers in the billions, and will reach over 30 billion in just the next five years. Most networks today are cloud-based which means that data centers are at their hub. And these data centers rely more and more on Artificial Intelligence and the Graphics Processing Units (GPUs) which are vital to power these AI applications. Keeping these data centers secure as our intent is to keep the U.S. safe and forward-leaning while we live in a globally connected world. If we want our tree of prosperity to flourish, we need to ensure all the connected roots are healthy.

Every type of critical infrastructure: from the electric grid to water systems, to emergency responders, to the internet that we use to communicate and conduct business, all use similar information communications technologies and systems. Potential vulnerabilities in these

Telecommunications Industry Association
1201 Wilson Boulevard, Floor 27
Arlington, VA 22209 | www.tiaonline.org

systems have a broad impact due to the unique role played by communications networks in our infrastructure. Every one of CISA's 16 identified critical infrastructure networks is fundamentally driven by ICT networks.

Network attacks come from many directions including, state-sponsored enemies, criminals, and terrorists. While the attack possibilities are endless, we must have a defense in depth, which starts with supply chain security. We must ensure that the products and services that make up our networks are coming from trusted suppliers who can demonstrate that security is designed in.

We must verify before trusting. And we should remember that security is a subset of quality, a high-quality network must be based on infrastructure built with security and resiliency in mind. All of this is critical to the success of building trusted, resilient, and secure global networks.

In this context, subsea cable systems are an area of growing concern. From the Red Sea to the Taiwan Strait, to the Baltic Sea and beyond, nefarious actors are increasingly disrupting global networks by cutting cables and damaging the points where the cables come ashore. These subsea cables carry 99% of internet traffic across continents, and more than $10 trillion of financial transactions. These cables are the irreplaceable backbone of the global internet, and while satellite communications play an integral role in our networks, the data capacities of subsea cables cannot be overstated. For instance, we have seen estimates that by 2026, the total

Telecommunications Industry Association
1201 Wilson Boulevard, Floor 27
Arlington, VA 22209 | www.tiaonline.org

global satellite capacity is expected to be about half a percentage of the total global subsea cable capacity.[1]

Despite the essential nature of this technology, cables are increasingly getting caught up in an endless cycle of red tape. Well-intentioned efforts by the DOJ-led interagency group known as Team Telecom to mitigate national security threats have made laying new cables increasingly difficult. This has had the practical effect of reducing cable redundancy, which makes U.S. subsea infrastructure more susceptible to cuts or breaks. We must take the necessary steps to ensure that the U.S. remains at the forefront of promoting common-sense practices for subsea cable deployment that appropriately balance the critical national security roles this infrastructure plays with the economic realities of cable deployment.

Of course, in addition to these physical threats to our communications networks is the fundamental threat from untrusted software, hardware and suppliers. As network architectures continue to advance and become more complex, the potential attack surface grows and expands as well. This gives bad actors, including those that are state-sponsored by foreign adversaries, like the Chinese Communist Party, more targets. For example, the recent Salt Typhoon attack.

The US Government has a long and bipartisan recognition of the threat supply chain vulnerabilities pose to our nation's infrastructure, and there is a shared consensus that these vulnerabilities are forecasted to be a top network attack vector. The industry recognizes this, and that is the reason we at TIA initiated and developed SCS 9001, the ICT industry's first Supply Chain Security standard, in 2022. This standard was designed with input from our members and

[1] Dan Swinhoe, *Space Comes for Fiber: Can Satellites Offer Data Centers a New Resiliency Option?*, Data Center Dynamics (Sept. 29, 2023), https://www.datacenterdynamics.com/en/analysis/space-comes-for-fiber-can-satellites-offer-data-centers-a-new-resiliency-option/

Telecommunications Industry Association
1201 Wilson Boulevard, Floor 27
Arlington, VA 22209 | www.tiaonline.org

both U.S. and trusted allied governments and aligns with and operationalizes the NIST Cybersecurity Framework, the Prague Principles, and many other guidelines.

SCS 9001 is a supply chain security management system intended to define and measure the requirements and controls for the design, development, production, operations, and service of ICT products and services. By aligning with the standard, suppliers can demonstrate and verify that their products and services can be trusted.[2]

This is an effort that reaches beyond our domestic infrastructure, and TIA has been working with the Departments of Commerce and State as they help allied countries build trusted networks. As I previously mentioned, in a connected world, it is critical that our partners also build security into their wireless, wireline, satellite and critical infrastructures.

I believe these many past high-profile attacks, such as the previously mentioned Salt Typhoon attack, clearly indicate the need to address vulnerabilities within our ICT supply chain and mitigate them wherever possible. Before Salt Typhoon was the hacking of U.S. presidential campaigns, the CrowdStrike vulnerability, the SolarWinds hack, and many others that we must not forget. The growing number and sophistication of these attacks should concern us all.

A public-private partnership that builds in the elements needed to verify trust and continually improve can change behavior and reduce the effect that bad actors have on our many critical networks.

[2] For instance, TIA has reviewed the vulnerabilities exploited in the high-profile Log4j breach and determined that SCS 9001 certification would have mitigated the vulnerability and limited exposure. A detailed summary of this review is available here: https://tiaonline.org/wp-content/uploads/2022/07/Log4j-vs-SCS-9001.pdf

Telecommunications Industry Association
1201 Wilson Boulevard, Floor 27
Arlington, VA 22209 | www.tiaonline.org

We appreciate the leadership that this committee has demonstrated by holding this hearing today, and I would like to thank you for your time. I am happy to answer any questions you might have.

David Stehlin
Chief Executive Officer
Telecommunications Industry Association

Mr. HUDSON. Thank you.

Mr. Jaffer, you are recognized for 5 minutes for an opening statement.

STATEMENT OF JAMIL N. JAFFER

Mr. JAFFER. Chairman Hudson, Ranking Member Matsui, members of the subcommittee, thank you for inviting me here today to discuss the threats facing our global networks and the telecommunications infrastructure of our Nation, its allies, and its partners. I want to thank the chairman and the ranking member for holding this hearing, particularly given the major threats that we face today against our global telecommunications infrastructure from China, Russia, Iran, and North Korea.

While recent reports have come to light about the major hacks of the United States telecommunications infrastructure and the deployment of destructive capabilities within our infrastructure by China, these are only a small part of a much larger effort architected by our adversaries. These adversaries include not just the Nations of China, Russia, Iran, and North Korea but their proxies as well.

And they are aimed not just at collecting information and intelligence on the American government and our Federal policies and priorities but on our citizens, and putting in place capabilities that if they decide to use could take down significant parts of our financial system, our energy infrastructure, and the like. And, of course, our entire Nation and all of its capabilities, including the modern AI revolution, runs on top of the global telecommunications infrastructure that we are talking about today.

And so, while our hearing today is focused on this global infrastructure, we need to think about it in the context of two major issues: the larger national security and economic competition with China and its key economic and technological elements, and the increasing and robust collaboration between China, Russia, Iran, and North Korea.

We know—the Director of National Intelligence told us that China presents the most comprehensive and robust military threat to U.S. national security, with a joint force capable of full-spectrum warfare. This is true in the cyber domain as well, where the Director of National Intelligence told us that China remains the most active and persistent cyber threat to the U.S. Government, private sector, and critical infrastructure networks, and that China has demonstrated the ability not just to compromise U.S. infrastructure with those formidable cyber capabilities but also that has the ability to conduct destructive and disruptive activities. And this is where Volt Typhoon and Salt Typhoon come into play.

Now, none of this is particularly new when it comes to China. Since at least 2019, we have known that the Director of National Intelligence told us that China is improving its cyber attack capabilities and that it had the ability back in 2019—6 years ago—to launch cyber attacks that could cause localized temporary disruptions and disruptive effects on our critical infrastructure, including the disruption of natural gas pipelines for days to weeks. That was 6 years ago.

And so we think about what their capabilities look like today, and we realize that this threat is much larger and much more significant than we think. And so let's talk about one particular example of how this plays out. We look at the Salt Typhoon hacks of the U.S. telecommunications infrastructure. In that effort, the FBI has told us that China targeted commercial telecommunications infrastructure and had a broad and significant cyber espionage campaign. They have compromised networks at multiple telecommunications companies—the chairman mentioned nine of them—to enable the theft of customer call records, the compromise of private communications, actual content on a number of individuals, while primarily focusing on U.S. Government and political activity, and the copying of information subject to U.S. law enforcement requests.

Let me say it again: The Chinese Government was able to hack not just our call records, not just the communications of American government and political officials, but the records of U.S. law enforcement requests. That means people that we have on collection, whether for criminal purposes, maybe for foreign intelligence purposes, are now in the hands of the Chinese Government. And if the Chinese have it, they are almost certainly going to share it with the Russians, potentially with the Iranians, and potentially with the North Koreans.

And don't believe me. Then-chairman of the Senate Intelligence Committee John Warner—sorry, pardon me—Mark Warner said it was the worst telecom hack in our Nation's history. The current Secretary of State, Marco Rubio, referred to it as "an egregious, outrageous, and dangerous breach of our telecommunications systems across multiple companies."

So what can we do? In the last minute and a half remaining, I want to address one thing we should not do. We should not blame the private sector standing alone. The idea that we would expect the private sector to defend against nation state attacks standing alone makes no sense. We don't expect Target or Wal-Mart to put surface-to-air missiles on the tops of their warehouses to defend against Russian Bear bombers. Why should we expect any of our telecommunications companies to be able to effectively defend against committed nation state attackers who have virtually unlimited resources of national governments? It doesn't make sense.

At the same time, we have to look internally at the Government to say, what did the Government know? When did it know about it? And why didn't it take action to protect its own data residing on these networks? So there's a lot of work to be done here. There are a lot of things we could talk about.

I appreciate the opportunity to be here, and I look forward to your questions.

[The prepared statement of Mr. Jaffer follows:]

Statement for the Record
of
Jamil N. Jaffer[1]
on
Global Networks at Risk: Securing the Future of Telecommunications Infrastructure[2]
before the
Subcommittee on Communications & Technology
of the
United States House of Representatives Committee on Energy & Commerce

April 30, 2025

I. Introduction

Chairman Hudson, Vice Chairman Allen, Ranking Member Matsui, and Members of the Subcommittee: thank you for inviting me here today to discuss the threats facing global networks and the telecommunications infrastructure of our nation, its allies, and its partners.

I want to thank the Chairman, the Vice Chairman, and the Ranking Member for holding this hearing, particularly given the major threats—including actual hacks and capabilities being put in place for destructive attacks—that we've recently seen targeting the global cyber and telecommunications infrastructure, particularly but not exclusively, coming from China and its ruling cabal of the Chinese Communist Party.

I want to be clear here—while recent reports have come to light about the apparently highly successful Chinese government penetration of United States telecommunications networks, as well as their newly-discovered efforts to infiltrate destructive capabilities into the heart of global networks—these efforts, known as Salt Typhoon and Volt Typhoon, respectively, are only part of the story. There is a much larger effort afoot in the cyber domain, architected not just by China,

---

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

[2] Portions of this testimony may have been drawn from prior testimony provided to the House or Senate by Prof. Jaffer. Citations and quotations marks from such testimony may have been omitted, including certain portions excerpted verbatim.

but also by Russia, Iran, and North Korea, and a wide range of proxy actors operating on their behalf, to target America's cyber infrastructure, and that of our allies and partners as well.

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

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

While today's hearing is focused on global threats to telecommunications sector (and the technology that rides on top of it) and assessing what we ought do about them, it is important that we understand this specific are of threats in the context of two key issues: (1) the larger national security threat and competition from China, including its key economic and technological elements; and (2) the ongoing and increasingly robust collaboration between our adversaries in China, Russia, Iran, and North Korea.

II. The National Security, Cyber, and Technology Threat Environment

A. China

Starting with China, the current Director of National Intelligence, in her first-ever Annual Threat Assessment of the Intelligence Community, has made clear that the People Republic of China (PRC) "presents the most comprehensive and robust military threat to U.S. national security…[with] a joint force that is capable of full-spectrum warfare" and active efforts ongoing that are "aimed at making the PLA a world-class military by 2049."[3] As a result, the DNI expects that China will seek to remain "in a position of advantage in a potential conflict with the United States…[while also]…conducting wide-ranging cyber operations against U.S. targets for both espionage and strategic advantage."[4]

At the same time, the DNI expects that "Beijing will continue to strengthen its conventional military capabilities and strategic forces, intensify competition in space, and sustain its industrial- and technology-intensive economic strategy to compete with U.S. economic power and global leadership."[5] As we think about the most likely flashpoint with China—over Taiwan—it is worth noting that the DNI is of the view that "[a] conflict between China and Taiwan would disrupt U.S. access to trade and semiconductor technology critical to the global economy…[and] [e]ven

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

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

[5] *Id.* at 9.

without U.S. involvement in such a conflict, there would likely be significant and costly consequences to U.S. and global economic and security interests."[6]

Speaking specifically about threats in the cyber domain, the DNI has stated unambiguously that China "remains the most active and persistent cyber threat to U.S. government, private-sector, and critical infrastructure networks[,]"[7] further noting that that "China has demonstrated the ability to compromise U.S. infrastructure through formidable cyber capabilities that it could employ during a conflict with the United States."[8] Indeed, the DNI's view is that if China believes "a major conflict with Washington [is] imminent, it could consider aggressive cyber operations against U.S. critical infrastructure and military assets," with the aim of "deter[ring] U.S. military action by impeding U.S. decision-making, inducing societal panic, and interfering with the deployment of U.S. forces."[9]

And this is where the Volt Typhoon and Salt Typhoon efforts by China come into play. The DNI has stated that the Volt Typhoon "campaign [by China] to preposition access on critical infrastructure for attacks during crisis or conflict," and the "more recently identified compromise of U.S. telecommunications infrastructure [by China], also referred to as Salt Typhoon, demonstrates the growing breadth and depth of the PRC's capabilities to compromise U.S. infrastructure."[10]

But truth be told, none of this is all that new when it comes to China. Since at least 2019, over half a decade ago, the U.S. Intelligence Community has been flagging that "China presents a persistent cyber espionage threat and a growing attack threat to our core military and critical infrastructure systems," and specifically warning that China "is improving its cyber attack capabilities," and noting specifically that "China has the ability to launch cyber attacks that cause localized, temporary disruptive effects on critical infrastructure—such as disruption of a natural gas pipeline for days to weeks—in the United States."[11]

This drumbeat continued into 2021, with the then-new Administration warning that "China presents a prolific and effective cyber-espionage threat, possesses substantial cyber-attack capabilities, and presents a growing influence threat[,]" and specifically noting that China both "can launch cyber attacks that, at a minimum, can cause localized, temporary disruptions to critical infrastructure within the United States[,]" and noting specifically for the first time that China's "cyber-espionage operations have included compromising telecommunications firms, providers of

---

[6] *Id.* at 11.

[7] *Id.* at 11.

[8] *Id.* at 9.

[9] *Id.* at 12.

[10] *Id.* at 11.

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

managed services and broadly used software, and other targets potentially rich in follow-on opportunities for intelligence collection, attack, or influence operations."[12]

This was followed, in 2022 with continued warnings of China's "almost certain[]" capability "to launch[] cyber attacks that would disrupt critical infrastructure services within the United States, including against oil and gas pipelines and rail systems," and noting once again the threat to telecommunications, software and other target rich environments.[13]

It is also worth noting that these cyber threats—both historic and ongoing—are also undergirded by China's efforts to "dominat[e] global markets and strategic supply chains…making other nations dependent on China[,]" particularly in areas that are critical to United States technology leadership, such as critical minerals, semiconductors, and artificial intelligence.[14] For example, the current DNI has made clear that "China's dominance in the mining and processing of several critical materials is a particular threat, providing it with the ability to restrict quantities and affect global prices."[15] We also know that China seeks to "become a global [science and technology] superpower, surpass the United States, promote self-reliance, and achieve further economic, political, and military gain...[by] prioritiz[ing] technology sectors such as advanced power and energy, AI, biotechnology, quantum information science, and semiconductors."[16]

And the tie-in between these efforts and the threats to our telecommunications and cyber infrastructure is that the Chinese are actively exploiting our communications networks to juice their efforts to become a technology superpower. They are doing so in a range of ways, including engaging in intellectual property theft at industrial scale, directly stealing "hundreds of gigabytes of intellectual property from companies in Asia, Europe, and North America in an effort to leapfrog over technological hurdles, with as much as 80 percent of U.S. economic espionage cases as of 2021 involving PRC entities."[17] China also use its intelligence collection capabilities on U.S. networks to identify investments, recruit talent, evade sanctions, and conduct cyber operations, all of which are key parts of their effort to "accelerat[e] [China's] S&T progress through a range of licit and illicit means."[18]

---

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

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

[14] *See 2025 Annual Threat Assessment*, *supra* n. 3 at 12.

[15] *See id.*

[16] *Id.* at 13.

[17] *Id.*

[18] *Id.*

And it is worth noting that China's ongoing "multifaceted, national-level strategy designed to displace the United States as the world's most influential AI power by 2030,"[19] is not simply aimed at economic gain but is also designed to support China's intelligence collection efforts and its plan to undermine American national security. Indeed, the current DNI has made clear that "Chinese AI firms are already world leaders in voice and image recognition, video analytics, and mass surveillance technologies," and that the "[t]he PLA probably plans to use large language models (LLMs) to generate information deception attacks, create fake news, imitate personas, and enable attack networks."[20]

And these intelligence collection efforts and covert and overt messaging take place over the entirety of our telecommunications networks. One obvious example is very real threat that TikTok, poses to our national security.[21] While many Americans view TikTok as a way to watch a bunch of kid and dog videos, the fact is that TikTok's extensive collection on data on Americans and our allies, its ties to the Chinese Communist Party, and the Chinese government's influence over TikTok's algorithm, makes it a unique and serious national security threat.[22] Indeed, when one combines the massive amount of data that TikTok collects on its users with other data stolen by Chinese government hackers, including security clearance files and the sensitive financial, health, and travel data of millions of Americans, it is clear that the Chinese government can use this data—powered by AI—to drive future sophisticated intelligence collection and disinformation campaigns targeting Americans and our allies.[23]

As if this weren't enough, it is worth noting that China also seeks to increase its already central role in the semiconductor supply chain to undermine U.S. telecommunications networks, including our ability to build them and to secure them. The DNI has identified that the China has "made progress in producing advanced 7-nanometer (nm) semiconductor chips for…cellular devices using previously acquired deep ultraviolet (DUV) lithography equipment," and has noted that while they may face volume production challenges, China is also continuing to "explore applying advanced patterning techniques to DUV machines to produce semiconductor chips as small as 3nm,"[24] a claim that appears to be supported by recent reporting in the last two weeks that Chinese semiconductor company SMIC has managed to get to a 5 nm chip using such techniques with DUV machines.[25] And, of course, the DNI rightly notes that "China [already] leads the world in

---

[19] *Id.*

[20] *Id.*

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

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

[23] *Id.* at 4-13.

[24] *See 2025 Annual Threat Assessment*, *supra* n. 3 at 14.

[25] *See* Ananya Gairola, *China's Chip Breakthrough Without ASML Makes Chamath Palihapitiya Take Stock Of Beijing's 'Formidable' Nature: 'America Can Win If... '*, Benzinga (Apr. 23, 2025), *available online at*

legacy logic semiconductor (28nm and up) production, accounting for 39.3 percent of global capacity, and is expected to add more capacity than the rest of the world combined through 2028[,]" for chips that are "vital to producing automobiles, consumer electronics, home appliances, factory automation, broadband, and many military and medical systems,"[26] including critical parts of our telecommunications networks and systems.

Finally, when it comes to the threats posed by China to American telecom networks, we cannot forget about China's efforts to compete with the United States in the space domain and, in particular, its ability to potentially take action against the United States in that arena. While it is true that in recent decades, the long-haul telecommunications infrastructure has pivoted from satellite-based communications to undersea cables, the reality is that we are increasingly relying on space-based assets for a range of services and capabilities that are critical to our communications capabilities, including position, navigation, and timing, as well as broadband access across the globe, both for government and industry use cases. As such, China's rapidly developing capabilities in intelligence, surveillance, and reconnaissance (ISR), where the DNI finds that it has "achieved global coverage…in some of its…constellations and world-class status in all but a few space technologies[,]" as well as its Beidou constellation which competes with our GPS system, and its recent launch of a low Earth orbit (LEO) constellation for satellite Internet services,[27] are all concerning trends.

These trends, of course, are also particularly concerning when viewed in light of China's counterspace capabilities, which the DNI has made clear "will be integral to PLA military campaigns," particularly given that "China has counterspace-weapons capabilities intended to target U.S. and allied satellites."[28] Chinese capabilities to go after America's space-based communications infrastructure don't just include "ground-based counterspace capabilities, including EW systems, directed energy weapons (DEWs), and antisatellite (ASAT) missiles intended to disrupt, damage, and destroy target satellites," but also includes "orbital technology demonstrations…[and] on-orbit satellite inspections of other satellites," capabilities that "while not counterspace weapons tests, prove [China's] ability to operate future space-based counterspace weapons…[and] which probably would be representative of the tactics required for some counterspace attacks."[29]

B. Russia

Turning to Russia, it is clear—and the current DNI agrees—that "Russia's current geopolitical, economic, military, and domestic political trends underscore its resilience and enduring potential threat to U.S. power, presence, and global interests[,]" and that Russian President Vladimir Putin is "prepared to pay a very high price to prevail in what he sees as a defining time in Russia's

---

<https://www.benzinga.com/tech/25/04/44970472/chinas-chip-breakthrough-without-asml-makes-chamath-palihapitiya-take-stock-of-beijings-formidable-nature-america-can-win-if>.

[26] *See 2025 Annual Threat Assessment*, *supra* n. 3 at 13.

[27] *Id.* at 15.

[28] *Id.*

[29] *Id.*

strategic competition with the United States, world history, and his personal legacy"[30] Indeed, the DNI believes that "Moscow's massive investments in its defense sector will render the Russian military a continued threat to U.S. national security," noting that Russia has "increased its defense budget to its heaviest burden level during Putin's more than two decades in power," while also "import[ing] munitions such as UAVs from Iran and artillery shells from North Korea… enhancing the threat its military poses."[31]

Like China, Russia's "disinformation, espionage, influence operations, military intimidation, cyberattacks, and gray zone tools…[are also part of an effort] to try to compete below the level of armed conflict and fashion opportunities to advance Russian interests."[32] Indeed, the current DNI has made clear that Russia's cyber-enabled "influence activities…including [] stoking political discord in the West, sowing doubt in democratic processes and U.S. global leadership, degrading Western support for Ukraine, and amplifying preferred Russian narratives…will continue for the foreseeable future and will almost certainly increase in sophistication and volume."[33] And current DNI's view is that Russian "information operations efforts to influence U.S. elections are advantageous, regardless of whether they affect election outcomes, because reinforcing doubt in the integrity of the U.S. electoral system achieves one of [Russia's] core objectives."[34]

The fact, of course, is that much of these efforts, take place through Russia's cyber exploitation of American telecommunications and technology networks and systems. Specifically, the DNI has determined that "Russia's advanced cyber capabilities, its repeated success compromising sensitive targets for intelligence collection, and its past attempts to pre-position access on U.S. critical infrastructure make it a persistent counterintelligence and cyber attack threat."[35]

Such capabilities should be a major concern for the United States because the "practical experience [Russia] has gained integrating cyber attacks and operations with wartime military action…[will] almost certainly amplify[] its potential to focus combined impact on U.S. targets in [a] time of conflict."[36] Indeed, the DNI assesses that Russia's "demonstrat[ion] [of] real-world disruptive capabilities during the past decade, including gaining experience in attack execution by relentlessly targeting Ukraine's networks with disruptive and destructive malware[,]"[37] provides Moscow with a "unique strength" in the cyber domain.[38]

---

[30] *Id.* at 16.

[31] *Id.* at 18.

[32] *Id.*

[33] *Id.* at 20.

[34] *Id.*

[35] *Id.* at 19.

[36] *Id.*

[37] *Id.* at 20.

[38] *Id.* at 19.

As with China, however, these facts should not be surprising, particularly given that since at least 2019, the United States has been raising concerns about Russia's efforts to "map[] our critical infrastructure with the long-term goal of being able to cause substantial damage," and given that the then-DNI, Senator Dan Coats, specifically disclosed that Russia was actively "staging cyber attack assets to allow it to disrupt or damage US civilian and military infrastructure during a crisis."[39]

This is the exact same kind of deployment of cyber capabilities that we saw Volt Typhoon put in place more recently on behalf of the Chinese government. Indeed, as one thinks about the capabilities that a nation like Russia has available to target American telecommunications systems and networks today, it is worth noting that back in 2019, the then-DNI stated that "Russia has the ability to execute cyber attacks in the United States that generate localized, temporary disruptive effects on critical infrastructure—such as disrupting an electrical distribution network for at least a few hours[.]"[40]

And these concerns only grew more troubling, particularly for our telecommunication's infrastructure, in 2021 and 2022, when the DNI specifically noted that "Russia continues to target critical infrastructure, including underwater cables and industrial control systems, in the United States and in allied and partner countries, as compromising such infrastructure improves—and in some cases can demonstrate—its ability to damage infrastructure during a crisis."[41]

Like China, as well, it is worth noting Russia also has advanced "space programs threaten the Homeland, U.S. forces, and key warfighting advantages,"[42] and that "Russia continues to train its military space elements and field new antisatellite weapons to disrupt and degrade U.S. and allied space capabilities[, including by]….expanding its arsenal of jamming systems, DEWs, on-orbit counterspace capabilities, and ASAT missiles designed to target U.S. and allied satellites."[43]

It is also clear that "Russia has proven adaptable and resilient, in part because of the expanded backing of China, Iran, and North Korea[,]"[44] that "Russia's relationship with China has helped Moscow circumvent sanctions and export controls to continue the war effort, maintain a strong market for energy products, and promote a global counterweight to the United States, even if at the cost of greater vulnerability to Chinese influence[,]" and that Russia's "increase[ed] military cooperation with Iran and North Korea… continue[s] to help its war effort[.]"[45]

---

[39] *See 2019 Worldwide Threat Assessment*, *supra* n. 11 at 6.

[40] *Id.*

[41] *See 2021 Annual Threat Assessment*, *supra* n. 12 at 9; *2022 Annual Threat Assessment*, *supra* n. 13 at 12.

[42] *See 2025 Annual Threat Assessment*, *supra* n. 3 at 19.

[43] *Id.* at 20.

[44] *Id.* at 16.

[45] *Id.* at 17.

C. Iran

This committee, of course, is also well aware of the significant threat that Iran poses to American national security and our interests, allies, and partners globally, including our longstanding allies in the Middle East, including Israel, Jordan, Saudi Arabia, the United Arab Emirates, and Bahrain, to name a few. This threat is perhaps most clear in the Iranian regime's support of all manner of terrorist groups globally from Hizballah to Hamas and Palestinian Islamic Jihad to the Yemeni Houthis and all manner of groups in Iraq and Syria that have directly attacked—and kidnapped and killed—Americans citizens and soldiers. The DNI recently made clear that Iran "will continue to directly threaten U.S. persons globally and remains committed to its decade-long effort to develop surrogate networks inside the United States…[including] seek[ing] to target former and current U.S. officials it believes were involved in the killing of…IRGC[]-Qods Force Commander Qasem Soleimani in January 2020[, having] previously [] tried to conduct lethal operations in the United States."[46]

And we well know of Iran's longstanding efforts to pursue nuclear weapons capabilities, against the interests of the United States and our allies. But it is also worth noting that Iran is also building up—and sharing with other U.S. adversaries—its conventional weapons capabilities as well. Indeed, according to the DNI, "Iranian investment in its military has been a key plank of its efforts to confront diverse threats and try to deter and defend against an attack by the United States or Israel[,]" including through its efforts to "bolster the lethality and precision of its domestically produced missile and UAV systems,"[47] and to share them with countries like Russia, which has long been using Iranian Shaheed drones in Ukraine.

But the one of the most important—and undercounted—threats posed by Iran are its efforts in the cyber domain, including its efforts to target our telecommunications networks and systems. Specifically, according to the DNI, "Iran's growing expertise and willingness to conduct aggressive cyber operations also make it a major threat to the security of U.S. and allied and partner networks and data."[48] Indeed, the current DNI has noted that "[g]uidance from Iranian leaders has incentivized cyber actors to become more aggressive in developing capabilities to conduct cyber attacks."[49] This is particularly concerning because in 2019, the-DNI Coats told Congress that Iran was "attempting to deploy cyber attack capabilities that would enable attacks against critical infrastructure in the United States and allied countries," and that it was then "capable of causing localized, temporary disruptive effects—such as disrupting a large company's corporate networks for days to weeks—similar to its data deletion attacks against dozens of Saudi governmental and private-sector networks in late 2016 and early 2017."[50]

And also know that "Iran often amplifies its influence operations with offensive cyber activities[,]" including efforts during the last election cycle to acquire information from the

---

[46] *Id.* at 22.

[47] *Id.*

[48] *Id.*

[49] *Id.*

[50] *See 2019 Worldwide Threat Assessment*, *supra* n. 11 at 6.

President's campaign and to "manipulate U.S. journalists into leaking [the] information illicitly acquired from the campaign."[51]

D. North Korea

The DNI also assesses that North Korea will "continue to pursue strategic and conventional military capabilities that target the [United States], threaten U.S. and allied armed forces and citizens, and ...undermine U.S. power and reshape the regional security environment in [North Korea's] favor."[52]

North Korea's focus, in the cyber domain, is targeting American telecommunications networks and the financial institutions that ride upon them to "fund[] its military development—allowing it to pose greater risks to the United States—and economic initiatives by stealing hundreds of millions of dollars per year in cryptocurrency."[53] However, the DNI also assesses that North Korea "may also expand its ongoing cyber espionage to fill gaps in the regime's weapons programs, potentially targeting defense industrial base companies involved in aerospace, submarine, or hypersonic glide technologies."[54]

Like with China, Russia, and Iran, much of this unsurprising because we knew back in 2019 that "North Korea poses a significant cyber threat to financial institutions [and] remains a cyber espionage threat...us[ing] cyber capabilities to steal from financial institutions to generate revenue[,]...includ[ing] attempts to steal more than $1.1 billion from financial institutions across the world [and]...a successful cyber heist of an estimated $81 million from the New York Federal Reserve account of Bangladesh's central bank."[55]

We also learned, interestingly, in 2019 that North Korea "retains the ability to conduct disruptive cyber attacks,"[56] a capability that we more recently learned was focused on American cyber networks. Specifically, in 2021, the DNI told Congress that that "Pyongyang probably possesses the expertise to cause temporary, limited disruptions of some critical infrastructure networks and disrupt business networks in the United States, judging from its operations during the past decade, and [further that] it may be able to conduct operations that compromise software supply chains."[57] We also learned, in 2022, that "Pyongyang is well positioned to conduct surprise cyber attacks given its stealth and history of bold action."[58]

III. Assessing the Threats to the Global Telecommunications Infrastructure

---

[51] *See 2025 Annual Threat Assessment*, *supra* n. 3 at 26.

[52] *Id.*

[53] *Id.* at 28.

[54] *Id.*

[55] *See 2019 Worldwide Threat Assessment*, *supra* n. 11 at 6.

[56] *Id.*

[57] *See 2021 Annual Threat Assessment*, *supra* n. 12 at 14; *2022 Annual Threat Assessment*, *supra* n. 13 at 17.

[58] *See 2022 Annual Threat Assessment*, *supra* n. 13 at 17.

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

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

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

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

One need only look at the Salt Typhoon hacks aimed at our telecommunications infrastructure—primarily for intelligence collection—to understand just how vulnerable (and underprepared) we are to deal with these adversaries.

In that case, we learned—after years and years of knowing that the Chinese government and its military and intelligence institutions were focused on this effort—that China had obtained widescale access to our telecommunications networks.[59] Specifically, the FBI stated that

---

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

China's "targeting of commercial telecommunications infrastructure has revealed a broad and significant cyber espionage campaign," and that Chinese-affiliated actors "have compromised networks at multiple telecommunications companies to enable the theft of customer call records data, the compromise of private communications of a limited number of individuals who are primarily involved in government or political activity, and the copying of certain information that was subject to U.S. law enforcement requests pursuant to court orders."[60]

This was an astounding event; according to the then-Chairman of the Senate Intelligence Committee, Senator Mark Warner (D-VA), it was the "worst telecom hack in our nation's history — by far,"[61] and according the then-Vice Chair of the Committee (and now current Secretary of State) Senator Marco Rubio (R-FL) referred to the hack as "an egregious, outrageous and dangerous breach of our telecommunications systems across multiple companies[.]"[62]
And yet, after the reported convening of a White House Unified Coordination Group (UCG),[63] a lengthy (and apparently ongoing) law enforcement investigation,[64] and a nascent (and incomplete) investigation by the Cyber Safety Review Board (of which I was once a member),[65] not to mention proposed regulation by the Federal Communications Commission,[66] the release of a 9-page security guidance document with at least eight national intelligence and law

---

and companies to gain access to presidential candidate communications. With that access, they could potentially retrieve unencrypted communication (e.g., voice calls and text messages).")

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

[61] Ellen Nakashima, *Top senator calls Salt Typhoon "worst telecom hack in our nation's history,"* Washington Post (Nov. 21, 2024), *available online at* <https://www.washingtonpost.com/national-security/2024/11/21/salt-typhoon-china-hack-telecom/>.

[62] Patrick Maguire, *Sen. Marco Rubio says Chinese hacking of U.S. telecom companies is a "very serious situation that we face*," CBS News (Nov. 3, 2024), *available online at* <https://www.cbsnews.com/news/marco-rubio-chinese-hacking-american-telecom-companies/>.

[63] *See, e.g.*, Ellen Nakashima, *White House forms emergency team to deal with China espionage hack*, Washington Post (Nov. 11, 2024) ("The White House on Tuesday convened a meeting of deputy secretaries of key agencies to stand up what's known as a 'unified coordination group.' The group's role is to ensure there is consistent interagency visibility into the response by the FBI, the Office of the Director of National Intelligence, and the Department of Homeland Security's Cybersecurity and Information Security Agency (CISA)."); *see also Salt Typhoon Hacks*, *supra* n. 58 at 2 (discussing Salt Typhoon and noting that "[b]y publicly available counts, this is the fourth time that the U.S. government has established a Cyber UCG—which were previously established for China's compromise of Microsoft Exchange services in 2021, Russia's compromise of SolarWinds in 2021.")

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

[65] Martin Matishak, *Cyber incident board's Salt Typhoon review to begin within days, CISA leader says*, The Record (Dec. 3. 2024), *available online at* <https://therecord.media/salt-typhoon-csrb-review>.

[66] *See* Federal Communications Commission, *Chairwoman Rosenworcel Announces Agency Action to Require Telecom Carriers to Secure their Networks* (Dec. 5, 2024), *available online at* <https://docs fcc.gov/public/attachments/DOC-408013A1.pdf>.

enforcement agency seals from four different countries,[67] and legislation introduced by at least one Senator,[68] we have precious little to show for this hacks.

According to press reports, at least some of the telecommunications companies involved have managed to remove the attackers (or at least those they could identify),[69] and the breadth of the hack appears to have been global, affecting at least nine telecommunications companies,[70] at least a dozen nations,[71] and targeting senior U.S. government officials,[72] with significant amounts of metadata and the content of certain individuals' communications obtained.[73]

At the same time, just this past week, more than six months after the hack was identified, the FBI now appears to be asking—perhaps surprisingly—for the public's help in "report[ing] information about PRC-affiliated activity publicly tracked as 'Salt Typhoon' and the compromise of multiple US telecommunications companies, especially information about specific individuals behind the campaign[,]" and specifically noting that if members of the public, "have any information about the individuals who comprise Salt Typhoon or other Salt Typhoon activity, we would particularly like to hear from you."[74] And the Treasury Department—apparently having identified at least one responsible party—has issued sanctions against one Chinese company.[75]

---

[67] *See* Cybersecurity and Infrastructure Security Agency, et al., *Enhanced Visibility and Hardening Guidance for Communications Infrastructure* (Dec. 3, 2024), *available online at* <https://www.ic3.gov/CSA/2024/241203.pdf>

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

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

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

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

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

[73] *See On-The-Record Press Gaggle*, *supra* n. 69 ("Our understanding is that a large number of individuals were geolocated in the Washington, D.C./Virginia area. We believe it was the goal of identifying who those phones belong to and if they were government targets of interest for follow-on espionage and intelligence collection of communications, of texts, and phone calls on those particular phones. So, we believe a large number of individuals were affected by geolocation and metadata of phones; a smaller number around actual collection of phone calls and texts. And I think the scale we're talking about is far larger on the geolocation; probably less than 100 on the actual individuals.") (statement of A. Neuberger).

[74] *See FBI Seeking Tips*, *supra* n. 63.

[75] *See, e.g.*, U.S. Department of the Treasury, *Treasury Sanctions Company Associated with Salt Typhoon and Hacker Associated with Treasury Compromise* (Jan. 17, 2025) ("Additionally, OFAC is sanctioning Sichuan Juxinhe Network

And yet, in perhaps one of the most stunning revelations to come out of this incident, even as the FCC and White House were calling for significant regulation of American telecommunications companies,[76] the outgoing head of the Department of Homeland Security's Cybersecurity and Infrastructure Security Agency (CISA), published a blog post stating that "CISA threat hunters previously detected the same actors in U.S. government networks."[77] The next day, at an on-the-record event at the Foundation for the Defense of Democracies, the CISA Director stated that while the government had previously detected the Salt Typhoon actors on other federal networks at the time "[w]e saw it as a separate campaign called another goofy name[.]"[78] According to newspaper reports, "CISA's observations didn't prevent Salt Typhoon from attacking the telecom networks en masse, but [the CISA Director] presented the agency's threat hunting and intelligence gathering capabilities as an example of intra-government and public-private collaboration improvements made under her stewardship of the agency."[79]

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

As I previously noted in testimony before another House committee back in 2020, while we've established an entity with the theoretical responsibility for defending the nation in the cyber domain in U.S. Cyber Command, we've never provided it with anywhere near the kind of authorities or resources it would take to actually do that job.[80] And while there may not be a consensus in our nation today on what the government's role in defending our nation's overall cyber infrastructure ought exactly be, the idea that we ought leave our critical infrastructure

---

Technology Co., LTD., a Sichuan-based cybersecurity company with direct involvement in the Salt Typhoon cyber group, which recently compromised the network infrastructure of multiple major U.S. telecommunication and internet service provider companies. People's Republic of China-linked (PRC) malicious cyber actors continue to target U.S. government systems, including the recent targeting of Treasury's information technology (IT) systems, as well as sensitive U.S. critical infrastructure.")

[76] *See Chairwoman Rosenworcel Announces Agency Action*, supra n. 65; *see also On-The-Record Press Gaggle*, *supra* n. 69 ("[W]e need to see every member of the — all the FCC commissioners vote to implement the required minimum cybersecurity practices across telecom, because once those are in place, once companies are taking those steps to make their networks defensible, we would feel more confident to say that the Chinese actors have been evicted and can continue to not be able to come in.") (statement of A. Neuberger).

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

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

[79] *Id.*

[80] *See CISA Clocked Salt Typhoon*, *supra* n. 78.

provider alone to defend themselves against foreign nation-state threat actors—or even worse penalize them when they find themselves unable to stop such actors who come to the fight with virtually unlimited resources—is not only unrealistic, it is setting up ourselves to fail every time.[81] Just as we don't expect Target or Walmart to have surface-to-air missiles on the roofs of their warehouses to defend against Russian Bear aircraft dropping bombs in the United States, we ought not expect the same from our telecommunications and infrastructure companies in the cyber domain.[82]

IV. Considering Effective Responses to Defend the Global Telecommunications Infrastructure

This, of course, puts front and center the question of what might be done to address this clear and present threat to the global telecommunications infrastructure.

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

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

---

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

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

our adversaries by leaving companies in the telecommunications, infrastructure, and technology sectors alone to defend themselves against nation-state attacks.

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

Another key effort that the government ought take up is affirmatively harmonizing existing compliance requirements and regulations across various agencies. At a minimum, the government ought permit compliance with one set of regulations serve as effective compliance with others where the subject matter of the regulation is similar. Likewise, getting unhelpful regulations out of the way and avoiding undermining our own national security policies for political gain by going after our best players—large and small—in the technology industry is critical to avoid. Efforts in recent years to amend longstanding and highly effective antitrust laws that have served our economy well for decades,[83] are a key example of the kind of new policies that would be highly detrimental in the context of the ongoing economic and national security competition with China. These efforts, which target a handful of technology companies based on the nature and scale of their business, are largely driven by policy issues unrelated to innovation or competition.[84] It also sends the wrong message to startup innovators, namely, that if they thrive and become highly successful, the government might seek to target them for special attention, creating laws just to cut them down to size.[85] The White House has made clear it is on

---

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

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

[85] *See* Klon Kitchen & Jamil Jaffer, *The American Innovation & Choice Online Act Is A Mistake*, The Kitchen Sync (Jan. 19, 2022), *available online at* <https://www. thekitchensync.tech/p/the-american-innovation-and-choice> ("Going after our technology companies, particularly a targeted shot at certain big ones, sends the wrong message to startups and investors alike; it tells them that if you are innovative enough to be successful and grow significantly

a strong deregulatory path, and action across all of these domains, could help significantly ensure that we are empowering the American private sector to innovate and create and implement better cyber defenses in partnership with the government.

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

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

The government also ought provide the right incentivizes for industry to build out both domestic and allied telecommunications infrastructure and to invest in the capacity and innovation to deliver advanced technology capabilities globally. To that end, the government should provide tax and other economic incentives for increased private investment in the development of such technologies, the broader deployment of large-scale computing infrastructure to support cloud and edge computing, and the expansion of AI capabilities being made available to U.S. and allied innovators across the globe. Likewise, the government should work with innovators and investors across the who share our interests to understand key government needs and priorities to develop the innovations and capabilities to address those needs.

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

---

larger, you may be targeted for different treatment....This undermines not only the companies that are likely to be investing in R&D over the next decade and generating some of the key innovations that will contribute to our national security, it also undermines a central proposition that has created a robust tech ecosystem in this country: take risk, innovate, fail fast and often, and when you succeed, reap the rewards so long as you don't exploit your position to gain unfair advantage."); Evanina & Jaffer, *Kneecapping U.S. Tech Companies*, *supra* n. 78 ("Picking and choosing individual companies to be treated differently than others under our antitrust laws is inconsistent with the heart of our economic system, which Seeks to reward innovation and success, not penalize them.").

and infrastructure industries, and to ensure that we have the skilled workers necessary to build and maintain this capacity and capability.

When it comes to addressing lessons learned from the Salt Typhoon hacks and the Volt Typhoon capability deployments, Congress ought consider collaborating with the Executive Branch to appoint an independent third-party commission, taking a page from the successful 9/11, Intelligence Reform, and Cyberspace Solarium Commissions, putting legislators on the panel alongside distinguished private sector and policy leaders to identify key challenges and draft actionable proposals that can actually be enacted by Congress and implemented by the Executive Branch in the near-term.

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

V. Conclusion

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

Mr. HUDSON. Thank you.

Ms. Galante, you are recognized for 5 minutes for your opening statement.

STATEMENT OF LAURA GALANTE

Ms. GALANTE. Thank you.

Telecommunications fail.

Good morning. Honorable Chair, Ranking Member, esteemed members of the committee, thanks for the opportunity to testify. I am Laura Galante. I served as the intelligence community cyber executive and the Director of the Cyber Threat Intelligence Integration Center at ODNI. I was also the intelligence community's lead for what is called the Unified Coordination Group, which responded to Salt Typhoon.

I will focus my remarks today on the national security considerations for the U.S. telecom sector, whose growth has closely mirrored the digital transformation of our economy. Over the past 25 years, telco companies have evolved from phone service providers to complex, multiservice digital organizations navigating the convergence of communications, media, and technology. As with so many major digital shifts during this period, intelligence services have also become increasingly adept at targeting the immensely valuable data that telcos manage through their vast networks of digital roads.

In short, companies in this sector have become key targets for foreign adversaries' operations. This leads us to the recent Chinese Government-sponsored operation, Salt Typhoon, regarded as the most expansive and consequential espionage ever conducted against the U.S. Sponsored by the Chinese Government and executed by contractors working for Beijing's Ministry of State Security, their intelligence bureau, this operation was first publicly detailed last fall, in 2024.

At least nine U.S. telcos—that number was again confirmed by the FBI yesterday—and wireless communication companies were the victim of this extensive intelligence-gathering operation. The actors breached multiple layers of major telecoms' networks. They gained unprecedented access to U.S. mobile communications across different carriers and various wireless technologies. The access enabled them to compromise voice and text communications of key political figures and national security officials.

Salt Typhoon gives us a window into three major issues. The first is the increased scale of adversary intelligence operations. Rather than focusing just on the communications of specific high-target individuals, what these Chinese actors did was they went after multiple data and access points through different victim companies in order to have this broad-scoped approach and a persistent intelligence capability to get after high-value information for a period of time. This wasn't a smash-and-grab, in-and-out type of cyber operation that we saw for years in the past. This was much larger.

Second was the delayed detection of Salt Typhoon across the sector. Despite the telcos' significant cybersecurity programs, detecting Salt Typhoon required—and still requires—an extensive joint government and industry effort to respond. The ability to detect and

then rapidly remediate and respond to these compromises against our most high-value networks, which we have all discussed, must be a core capability for companies in the sector.

Third is that AI is rapidly expanding our adversaries' ability to process data. Rapid breakthroughs in AI have now equipped these actors with the capability to make sense of large and disparate data sets that previously required immense amounts of time and resources to understand what the data they collected meant and what to do with it. AI has supercharged their ability to analyze this.

These capabilities enable even less sophisticated actors. We have been talking about highly sophisticated ones with China, but now less sophisticated actors will be able to extract key insights from vast amounts of data collected in different sectors and different industries.

The hard question that this committee faces is how to strike that balance between securing these digital roads and everyday life with the enormous and growing demand for digital connectivity. We are not going to regulate our way out to find an enduring answer. The technology changes too quickly. The ingenuity of our adversaries is relentless.

We have to build a better dynamic operational security model than what we have today. That model requires bringing threat intelligence and national security expertise, the intelligence community, together with private-sector representatives in the telco and secure technology sectors. This intelligence-driven approach is what will drive an operationally sound set of practices that companies can continue to implement and refine in their own infrastructure.

The good news is we have done this before. One of the mechanisms available to drive this process until it was dissolved last month was called the Enduring Security Framework founded in 2007. Implemented by the National Security Agency, along with the Office of the Director of National Intelligence, and then DHS's CISA's Critical Infrastructure Partnership Advisory Council, this same framework proved successful enough that British intelligence and Australian intelligence used it as their model for their national cyber centers.

In this model, security practitioners in government and industry alike used this to come up with dynamic processes about how you re-architected secure infrastructure for the future. Other boards that have also been dissolved, including the Cyber Safety Review Board, also worked to get to root causes of hard security and technical problems, and they investigated major cyber incidents, like Salt Typhoon.

These are the joint efforts that created evidence-based approaches to address major security breaches, and threats in coordination with the private sector who owns the critical infrastructure in this country. This collaborative security and intelligence work has been America's differentiator in our global secure technology market. It is an ecosystem of security professionals, intelligence officials, analysts, and operators who work together to track vulnerabilities and threats as quickly as they spread—and that is fast in cyberspace—and deploy the patches and fixes and new security paradigms that we need to stay ahead of these threats.

Dismantling this security ecosystem weakens our collective defense and our national security posture. It is not a risk we can afford at this moment.

I look forward to your questions.

[The prepared statement of Ms. Galante follows:]

Testimony by Laura Galante

Before the House Committee on Energy and Commerce, Subcommittee on Communications and Technology

On "Global Networks at Risk: Securing the Future of Telecommunications Infrastructure"

30 April 2025

Honorable Chair, Ranking Member, and esteemed members of this Committee, thank you for the opportunity to testify on the security of US telecommunications networks and their role in national security and US competitiveness.

My name is Laura Galante. I served as the Intelligence Community's Cyber Executive and the Director of the Cyber Threat Intelligence Integration Center (CTIIC) at the Office of the Director of National Intelligence (ODNI) from January 2022 to January 2025. Prior to this role, I led organizations that track, attribute, and expose cyber operations. I'll focus my remarks today on national security considerations for the US telecom sector.

The Telecommunications Sector in the Cross Hairs

This Committee recognizes that reliable and affordable telecom services form the backbone of America's digital infrastructure, enabling America's economic engine and global competitiveness.

The growth of the telecom sector has closely mirrored the digital transformation of our economy. Over the past 25 years, telecom companies have evolved from phone service providers into complex, multi-service digital organizations, navigating the convergence of communications, media, and technology. As with many tectonic digital shifts during this period, intelligence services have also become increasingly adept at targeting the immensely valuable data telcos manage through the vast network of digital roads they operate. In short, companies in this sector have become key targets for our foreign adversaries' operations.

Salt Typhoon: Beijing's Intelligence Operation against US Telecoms

Salt Typhoon marks a turning point. The operation, sponsored by the Chinese government and executed by contractors linked to Beijing's Ministry of State Security, was detailed publicly in Fall 2024 in media reports. They revealed that at least nine U.S. telecom and wireless communications companies were victims of extensive Chinese intelligence-gathering efforts.

In this multi-year operation, the actors breached multiple layers of major telecom networks, gaining unprecedented access to U.S. mobile communications across different carriers and various wireless technologies. This access enabled them to compromise the voice and text communications of top political figures and national security officials. Due to its sheer breadth and scope, this operation is regarded as the most expansive and consequential cyber espionage operation ever launched against the US.

Salt Typhoon presents three major issues that companies and governments will need to face:

1. **Increased Scale of Adversary Intelligence Operations:** Rather than focusing solely on the communications of specific high-value individuals, Chinese malicious actors breached and analyzed the complex operational networks of nine different telecom companies. This broad-scope approach underscored their intent to develop a durable, persistent intelligence capability that can support future objectives, rather than employing a task-specific, 'smash-and-grab' style operation.

2. **Delayed Detection of Salt Typhoon across the Telecom Sector:** Despite the telecoms' significant internal cybersecurity programs, detecting the Salt Typhoon compromise has required an extensive joint government-industry response. The ability to detect and rapidly remediate compromises against our most high-value networks must be a core capability for companies in this sector.

3. **AI Rapidly Expanding Data Processing Capabilities:** Rapid breakthroughs in AI have now equipped actors with powerful capabilities to make sense of large and disparate data sets that previously required immense time and resources to analyze at scale. These capabilities also enable even less sophisticated adversaries to extract key insights from vast amounts of data collected and merged from different industries and sectors.

Building a Secure Future

The hard question this Committee faces is how to strike a balance between securing the digital roads of our economy and everyday life with the enormous, growing demand for fast and affordable digital connectivity.

We can't regulate our way to an enduring answer. The technology changes too quickly, and the ingenuity of our adversaries is relentless. But we must build a better, more dynamic operational security model than what we have today. This model will require bringing the threat intelligence and national security expertise of the Intelligence Community together with key private sector representatives in the telecom and secure technology sectors. This intelligence-driven approach should then drive operationally-sound practices that companies implement across their infrastructure.

The good news is, we've done this before. One of the mechanisms available to drive this process–until it was dissolved last month–was the Enduring Security Framework founded in 2007. This was a partnership run by the National Security Agency along with the Office of the Director of National Intelligence, and it operated under the authorities of the Department of Homeland Security's Critical Infrastructure Partnership Advisory Council (CIPAC). The Enduring Security Framework proved successful enough that both the British and Australian intelligence services used it as the model for their own highly regarded national cyber centers.

Serious security practitioners in government and industry alike used the now-dissolved Enduring Security Framework along with other CIPAC boards including the Cybersecurity Review Board (CSRB)--also dissolved–to convene and work through hard tech security challenges and develop solutions. The CSRB, similar to the National Transportation Safety Board, investigated major cybersecurity incidents, like Salt Typhoon. These joint efforts developed evidence-based approaches to address major security breaches and threats in coordination with the private sector entities responsible for securing our critical infrastructure.

This collaborative security and intelligence work has been America's differentiator in the global secure technology market. It is an ecosystem of security professionals, intelligence officials, analysts, and operators that track vulnerabilities and threats as quickly as they spread and deploy patches, fixes, and new security paradigms.

Dismantling this public-private security ecosystem will weaken our collective defense and national security posture. A risk, I believe, we can't afford to take.

I look forward to your questions.

Mr. HUDSON. Thank you.

We will now begin questioning, and I recognize myself for 5 minutes.

Mr. Jaffer, I represent, as I mentioned, Fort Bragg. We like to call it the epicenter of the universe, home of our special forces and airborne. Why is maintaining the security of our communication networks essential to protecting our warfighters and our national security, especially as it relates to our adversaries, as we mentioned?

Mr. JAFFER. Well, Mr. Chairman, it is hard to overstate how critical it is to protect our global telecommunications infrastructure. It is the backbone on which everything else runs, whether it is warfighter activities, communications with families and spouses, and the collection and analysis of all of our intelligence. While we do have highly classified systems that run on separate networks, that communication grid is connected, and if we don't—if that communication grid doesn't operate, it simply doesn't work.

And fundamentally, our entire economics system turns on this global telecommunications infrastructure as well. The United States is so successful particularly because we built the system, it runs on our equipment, it runs on our capabilities and that our of allies. And the day it doesn't—and as it has transitioned over to equipment run by adversaries, the more vulnerable it has become, the less secure we become, the less secure our warfighters are, and the less secure our entire economy is.

Mr. HUDSON. Appreciate that.

Mr. Stehlin, do you have anything to add to that?

Mr. STEHLIN. Yes, I would 100 percent agree with everything that is going on there. We do need the public/private connection to make sure we address this. Everything we do from the military to our home lives uses ICT networks, and fundamentally they are all based on the same set of technologies and architectures, and we have to verify that those technologies and architectures are secure.

Mr. HUDSON. Emerging technologies have the potential to both enhance cybersecurity of our networks, but also threaten their security. It is kind of a double-edged sword.

Mr. Stroup, in your testimony you talk about how AI can be harnessed to do vulnerability testing. Can you tell us more about how this is being deployed in the satellite industry?

Mr. STROUP. Yes. Thank you for the question. There are a number of ways in which it is being deployed. First, is for anomaly detection, being able to identify if there is a different type of data that is coming into a network, being able to identify that in advance. Another is being able to take advantage of cybersecurity enhancements, being able to detect and respond to threats in real time, also being able to address signal-jamming detection and mitigation.

And then finally, I would also like to emphasize it is important in space situational awareness. There are so many objects in space, and the opportunity to be able to identify, analyze, and determine whether they are going to pose a threat or risk to satellites are one of the uses of AI.

Mr. HUDSON. I appreciate that.

Mr. Jaffer, how can AI be used in the communication networks to enhance security?

Mr. JAFFER. Well, look, there's a lot of opportunities we have. These LLMs can identify threats and vulnerabilities. We just saw in the last few months the discovery of brand new vulnerabilities that we weren't aware of discovered by LLM models running over network data, right. So there is a big debate about will AI improve the attacker more or improve the defender more, and I actually it is a mixed bag, right.

In some ways, it will definitely, as Ms. Galante pointed out, enable attackers who don't have capabilities today to have more capabilities. At the same time, the defender will have an edge as well because they will be able to get ahead of the threats, identify vulnerabilities, cut them off at the pass and go after the attackers.

So while the offense, like in football, always has a little bit of an edge, right, and AI will enhance that, AI is going to enhance defenders as well. And its expanded use and ensuring that we don't overregulate it and crush it with unnecessary regulation will ensure that we maintain the edge. The reality is, our adversaries are going to use it on the offense. If we overregulate it and don't use it on the defense, we will fail.

Mr. HUDSON. I agree.

Mr. Stehlin, economic security is national security. One of President Trump's top priorities is reshoring American manufacturing as the United States continues to reshore critical manufacturing and expand domestic data center capacity, secure, high-speed connectivity will be essential. What specific policy actions do you believe are necessary to ensure our communications infrastructure can meet these increasing demands without comprising on supply chain security or network resiliency?

Mr. STEHLIN. Yes, two things come to mind: First of all, we need to reshore as much as possible. The active components that make up our ICT networks, whether it be a core router or a base station, or even a home IoT device, these devices have semiconductors which are not made for the most part in the United States. Major security shortfall. That is not something that can change overnight. It is something that will take a long time.

And it is not only that moving the fabs and things like that back here, but it is the whole ecosystem, moving that back here. And that is why many parts of Asia are successful in this area because the whole ecosystem is closely located to each other. So that whole supply chain needs to be both closely located with each other but also based in the United States. That is a fundamental strategic change and a long-term investment that we need to make.

And I would refer back to something I mentioned before: supply chain security. You have to ensure that the supply chain itself is secure, not only that ecosystem but all the devices that make up a product, and the only way to do that is ensure that the processes that are used to make a product are verified to be trusted. So that is something that this standard does is it verifies trust. You have to verify it before giving trust out.

Mr. HUDSON. Got it. Thank you. My time is expired.

I will now recognize the ranking member, Ms. Matsui, for 5 minutes to ask your questions.

Ms. MATSUI. Thank you very much, Mr. Chairman.

This Salt Typhoon attack exemplifies how expansive cyber operations against the U.S. have become. In an increasingly digital era where artificial intelligence emerging technologies can increase the capabilities of bad actors, we must address how America stays ahead of our adversaries.

Ms. Galante, what is the most pressing issue this committee must resolve to prevent major cyber attacks like Salt Typhoon?

Ms. GALANTE. Mature security programs in cyberspace are really important for major organizations, especially in the telco sector, to continue to refine and improve. There's some basic pillars of what a strong security program looks like: identity and access management; the tools and infrastructure to make sure they can look at their network and really log events that are happening; incident preparedness; risk in governance; and then their third-party vendor risk, which has been articulated quite a bit in how to manage that.

But one of the key performance measures that I look to when I am talking with CISOs, chief information security officers, and others who have to secure these networks and are in charge of that edge of American security and competitiveness is their time to detect malicious activity and their time to respond. And it is those two measures that are key that we drive across critical industries like this so that we aren't caught with multiyear, major operations that have the scale and impact like Salt Typhoon.

Ms. MATSUI. OK. Now, you mentioned CISA, and obviously it provides crucial support also to the States and localities at the front lines for protecting critical infrastructure. Now, what does this administration risk when it downsizes our Federal cyber workforce and puts more burdens on States and local agencies?

Ms. GALANTE. Cybersecurity is inherently a Federal issue. The internet doesn't know State boundaries, no put it mildly.

Ms. MATSUI. Right.

Ms. GALANTE. And what CISA does and what other Federal cybersecurity and national cybersecurity agencies do is they are able to articulate the risk to networks out in States, critical infrastructure providers, energy companies, banks, and get that information out to them so that they can employ it in their security programs. We have to take a Federal approach to do this, because inherently the threat is one that goes after us at a national level.

Ms. MATSUI. OK. Now, I think this was mentioned before too, but as more smart devices known as the Internet of Things are adopted into American's homes, we need to help consumers make informed choices and decisions about the technology products that they purchase. Those interconnected smart devices can be an entry point also for cyber attacks. That is why I have supported steps like the FCC's U.S. Cyber Trust Mark, a labeling program that identifies trustworthy and secure products in the marketplace.

Ms. Galante, how do voluntary measures like this instill trust and security in our technologies?

Ms. GALANTE. I like the Cyber Trust Mark Program a lot. If people haven't seen it yet, it is a sticker, it is a badge, and a QR code. And what it is, is it is a shorthand to the consumer that says the product that you are buying here has a security management pro-

gram behind it. It is going to get patched. There is going to be data protection, some of the key standards that we want behind that product.

It is a little bit like when you turn your microwave around and there is that metallic sticker that you can't pull off that says you can plug this in and you are not going to get shocked. It is the same concept for interconnected devices. I think it should catch on.

Ms. MATSUI. OK. Great. And talking more about standards, I have long championed that the U.S. leadership in global technology standards and that the next generation reflect American values, including open market transparency and democracy.

Mr. Stehlin, you mentioned SCS 9001. That is a supply chain security standard for information and communications technology industry. How can this and other standards ensure communications infrastructure is resilient against attacks from malicious actors?

Mr. STEHLIN. Yes, 9001 uses looking at not only the vendor of the supplier of equipment—is it a trusted vendor?—but it looks at the hardware and the software used in a product. Every single product out there uses open-source software, for example.

Ms. MATSUI. Yes.

Mr. STEHLIN. How do we trust that that open-source software is coming from an organization that can be trusted? Is there provenance that we can prove? Can we do things like incident management and move more quickly?

We need to speak in one voice when it comes to cyber and supply chain security. And SCS allows the ability for both public networks and private networks to do so all the way down to IoT devices, like the FCC is working on with the cyber labeling program.

Ms. MATSUI. Well, I consider that very important, the standards that we set in our country for U.S. leadership, in particular, because we understand that the actors, the unfortunate actors that are against us are going to be going out there and doing their own thing.

I want to talk more about—oh, I think I have run out of time already, right, Mr. Chairman?

Mr. HUDSON. Yes. Time flies when you are having fun.

Ms. MATSUI. But anyway, I will follow up later. OK. Thank you very much.

Mr. HUDSON. Thank you.

I will now recognize—is it Dunn?—Dr. Dunn from Florida for 5 minutes to ask your questions.

Mr. DUNN. Thank you very much, Mr. Chairman.

You know, I would say that Americans have every form of technology at their fingertips for broadband deployment and fiberoptic cable and fixed wireless. And particularly important where I live, in rural Florida, is satellite systems.

Historically, our country has done very well. They have done a stellar job, in fact, at building our telecoms infrastructure, and I think that under U.S. leadership, that industry is flourishing. Despite many challenges, the marketplace is providing responsive, innovative capabilities for commercial-use research intelligence and national security. But to sustain that dominance, we must invest in the infrastructure necessary to continue that rapid expansion in the future. That is just basic infrastructure investment.

Accordingly, this week, Representative Carbajal and I are reintroducing the bipartisan bill, Secure United States Leadership in Space Act, which enables the tax-exempt status of private bonds on FAA-licensed spaceports, pretty basic stuff. It is like, you know, highways and, you know, seaports or whatnot.

What makes this bill impactful is that it empowers the growth of the spaceport infrastructure that is so essential to a nation's enterprise to be funded more by private capital than, in fact, by the taxpayers. And this plays into the strengths, of course, of the U.S. system in our competition with China.

As a member of this committee for many years, I have continued to work on legislation to streamline and secure our telecoms networks. Last year, Congress passed and the President signed into law, with my friend Darren Soto, the Launch Communications Act that addresses the satellite launch communications spectrum, so very outdated regulations at the FCC, and they are currently implementing those now. This year we will continue to prioritize that, all those efforts.

Mr. Stroup, do you believe that the tax-exempt bonding rights for our spaceports can help secure U.S. leadership in space and space infrastructure, and engage private markets? Does that help the taxpayers?

Mr. STROUP. Yes. Our industry is most dependent upon spaceports, and having access to as many spaceports as possible will benefit the industry. So while SIA does not represent the spaceport industry, our members are very dependent upon them.

Mr. DUNN. So, I am from Florida. We have at least as many spaceports as most States, and I am very pleased with that. I sat on the board of spaceports for a number of years. I am really, really proud of the efforts in our State on that.

Again, Mr. Stroup, you mentioned in your testimony, access to sufficient spectrum resources is necessary to secure our infrastructure. Can you briefly elaborate on this and share what kind of spectrum authorities you think would make the most sense right now for space industry?

Mr. STROUP. Yes. Our industry is growing substantially. As an example, approximately 10 years ago, we had about 1,000 operational satellites; today, that number is over 12,000. That is just to give you a sense of the growth in the industry. We provide a wide range of services, and we are increasingly expected to share spectrum with other industries. In some cases, it is the wireless industry.

The industry, the satellite industry, for a long time shared spectrum amongst itself as well as with some other terrestrial users, such as microwave systems. But there is a continuous effort to get more spectrum, not only for the satellite industry, other growing industries like the wireless industry. So we are in a competitive environment just amongst ourselves, meaning those that use spectrum, but also in the global environment, and so seeking to have access to additional spectrum through the ITU process.

I might note that the next WRC, which is taking place in 2027, over 85 percent of the issues that are on the agenda are space-related, many of them giving us access to additional spectrum. So specifically relating to the ITU recommendations, seeking that the

United States take the leadership position, as well as making additional spectrum available within the United States.

Mr. DUNN. Well, thank you for that. I spent a lot of time, you know, focusing on space. But let's be honest, there is a lot of information flowing through the fiberoptic cables.

And in the few seconds left, I am hoping Mr. Stehlin can address the resilience of the cables, the undersea cables. What can we do to protect these things? There has been nothing but interruptions of these cables lately. It seems like anybody with a motorboat can interfere. Can you give us some confidence?

Mr. STEHLIN. Yes. Well, first of all, there are somewhere in the range of 600 undersea cable systems around the globe, 1,700 landing points. More landing points will help for sure. More repair ships, very much needed. If it takes a month or two to find a repair ship, you have a problem. So we need to rebuild the whole shipping side of things.

Mr. DUNN. Well, thank you very much.

Mr. Chairman, my time has elapsed, but I would love to talk to these people for the rest of the day. Thank you.

Mr. ALLEN [presiding]. I thank the gentleman for yielding.

Now, I will turn it over to Ranking Member Pallone for 5 minutes for your questioning.

Mr. PALLONE. Thank you, Mr. Chairman.

As I mentioned earlier, it is critically important that our country's telecommunications networks have the capabilities to effectively defend against foreign adversaries and other bad actors, but given the Trump administration's mishandling of sensitive information on Signal, and Musk and DOGE's access to sensitive Government information, it is clear that it is not just our telecommunications infrastructure that needs updated security standards and protocols.

So I wanted to ask, Ms. Galante, are Signal, Gmail, and other commercial services the proper channels and tools for government officials to use in making national security decisions?

Ms. GALANTE. National security decisions and deliberations from our adversaries' standpoint are intelligence gold, right. This is what they seek out. And it is for this reason that we have got classified communication channels.

Mr. PALLONE. OK. Now, under—I have a bill—bipartisan bill, the Secure and Trusted Communications Networks Act, and the FCC must place communications equipment or services that have been deemed a national security threat on its covered list, which effectively removes the equipment or services from our country's supply chain.

So, again, Ms. Galante, will broadening the types of communications technology that can be placed on the FCC's covered list help us better secure our country's telecommunications networks and data from foreign adversaries?

Ms. GALANTE. It will help us. The FCC's covered list goes a long way to give predictability and clarity about what products are insecure and what technologies shouldn't be used in our telecommunications technology.

Mr. PALLONE. OK. And, you know, the frequency of cyber attacks on our telecommunications networks I think shines a bright spot-

light on the amount of personal data that these networks carry day in and day out, and it is imperative that our networks have strong security protocols in place so that our data is not an easy target for our foreign adversaries.

But let me ask you again—or let me ask you this question: What types of capabilities should be built into our telecommunications networks to ensure they can successfully protect our data from the increasingly sophisticated cyber attacks and espionage we see from foreign adversaries? And if there is time, I would ask the others the same question.

Ms. GALANTE. Telecommunications networks are incredibly complex. They are dealing with a stack of technologies that ranges from literally the ground up. And these are tough to secure, and they require really advanced security programs to do it the right way.

Two of the measures that a secure program should be looking for, though—in how they perform, how the people and the tools and the team around this work—is their time to detect malicious activity and their ability to respond to it quickly. And the faster both of those things can happen, the more secure their program is going to be and the more resilient our entire sector will be.

Mr. PALLONE. You know, I wanted to ask others to comment on it, but I am still not sure, when I asked the first question about Signal and email and you said that—you know, I asked whether, you know, those are—commercial services are the proper channels for government officials to use in making national security decisions. What was your response again?

Ms. GALANTE. Classified channels are the right place for national security deliberations——

Mr. PALLONE. And these are not.

Ms. GALANTE. These are not classified channels.

Mr. PALLONE. OK. All right. Anyone else want to comment on the types of capabilities that should be built into the networks? I still got another minute. Yes.

Mr. STEHLIN. Yes, sir. We should look at the entire makeup of the vendor base. It is one of the challenges that we have around the world, is as we try to bring Western technology to friendly countries, we know that the Chinese will—and have for years worked their way in there by offering way underpriced product, offering the ability to fund the development and management of these networks, and then they work really hard with the legislative branch of many countries around the world.

We have an uphill battle. And one of the challenges we have is, as China has often sold products way under cost, it has put so much pricing pressure on Western technology that R&D investment has gone way down.

So the things we can do to help R&D rebuild in the United States would make a big difference.

Mr. PALLONE. Anyone else want to comment?

Mr. JAFFER. Mr. Ranking Member, I think the other important thing to keep in mind is that the Government has a role to play here too. The Government needs to partner tightly and collaborate with industry to defend against these threats. If we leave the pri-

vate sector alone to defend against these threats, we will fail every time.

These private-sector companies are not in the business of defending against cyber threats. They are in the business of providing telecommunication services and capabilities to our citizens, to our allies, and to partners around the globe. And so, if they are going to do it effectively, the Government has to take the information it knows about and has. For example, in the Salt Typhoon case, it turns out we found out 5 days before the administration ended that we had detected the Salt Typhoon attackers on U.S. Government networks, hadn't realized who they were, and hadn't shared that information.

It is almost like before 9/11, where we knew the attackers, some of the terrorists were in Malaysia and Kuala Lumpur, the CIA saw them there and then didn't bother to tell the FBI. That is a massive, massive failure of the Government to do its job to share information with the industry, help the industry protect itself, and take accountability for the fact that we had that information, didn't know what to do with it.

Mr. PALLONE. Thank you.

Thank you, Mr. Chairman.

Mr. ALLEN. I thank the gentleman for yielding.

And now I recognize myself for 5 minutes for questioning.

I want to thank our expert witnesses for joining us here today.

As home to the Army Cyber Command in Augusta, Georgia, my district is a hub for cybersecurity expertise, and we hear significant concerns about Federal agency roles and regulatory burdens hindering our ability to secure critical infrastructure.

Mr. Jaffer, cybersecurity—and you have already started to comment on this—cybersecurity professionals in my district highlight confusion over which agency—CISA, the Department of Defense, FCC or others—has primary jurisdiction over securing critical infrastructure, which would include telecommunications, satellites, and undersea cables. This lack of clarity can impede responses to threats like you mentioned, the Salt Typhoon breach.

Mr. Jaffer, how are the roles of CISA, DoD and FCC currently defined, and what steps can reduce confusion to enhance coordination and protect our infrastructure?

Mr. JAFFER. Well, thanks, Mr. Vice Chairman. I mean, the challenge here is that there is no one agency in the Government today responsible for defending our entire global cyber infrastructure, the U.S.'s, which we have built around the globe. And the problem is that, if you expect private industry to do it, it won't succeed. If you don't task somebody in the Government and give them the resources and the authorities to do it, it won't succeed.

Now, in theory, we said to U.S. Cyber Command, "It is your job to defend the infrastructure against nation states." But, of course, U.S. Cyber Command isn't resourced, doesn't have any authorities. And I am not sure there is a consensus amongst Congress and the administration about whether the Department of Defense should do that defense. In the absence of that consensus, the only way in which we can have the Government work effectively in the industry is to share information at scale.

We have legislation today, the Cyber Information Sharing Act that was passed in 2015—set to expire in the next few months—that needs to be reauthorized. But, more importantly, we need to actually incentivize the sharing of information. We passed the authority, but we didn't provide the necessary regulatory liability protections to encourage to actually share.

So the lawyers are telling them, "Do the minimal amount necessary." What you want to do is you want to line up boards of directors, you want to line up the lawyers, and you want to line up industry with government. Government wants information. It has information. Both need to share. Neither are doing it effectively because the incentives aren't there, and the Government says, "Well, we are not going to share all types of information with industry."

Well, if we are not going to do it, no one is going to do it. They are not going to know what the threat is. They are not going to defend well. And then we will all be looking back and saying, "Why didn't they defend themselves better?," and we will have no one to blame but ourselves.

Mr. ALLEN. Thank you, sir.

The Cyber Incident Reporting for Critical Infrastructure Act aimed to streamline reporting to CISA, yet stakeholders note persistent issues with the duplicative requirements across other agencies, including varying definitions and timelines—the very things that you are talking about—inconsistent incident definitions, like substantial laws versus potential adverse effects, and a lack of reciprocity, diverting resources from mitigating threats like those from the Chinese Communist Party.

Mr. Stroup and Mr. Stehlin, how do these challenges impact the communication sector's ability to secure infrastructure, and what can the FCC's new Council on National Security do alongside CISA to harmonize reporting, standardize definitions, and establish reciprocity to strengthen resilience?

Mr. Stroup.

Mr. STROUP. Thank you for the question. So most satellite systems are dual use, and as a result, many of the issues that we are talking about are addressed through our supply chain because, for a long time, the security in supply chain has been important. There is a certification process that satellite companies need to go through in order to provide service to the U.S. Military.

But I think that, getting to the cybersecurity issue, in terms of sharing information, I think that the key is the points that have been made by other members of the panel today, ensuring that there is a means of sharing the threats, giving companies an opportunity to address it. And, whether that is done through CISA, the FCC, I think making sure that there is a single point where members of our industry and other industries have access to that information is key to being able to address them.

Mr. ALLEN. Mr. Stehlin.

Mr. STEHLIN. Thank you, sir. Yes, I would agree. We have to speak in one voice. We have to send clear messages across the country on both the public and the private side. We have to send clear messages to our international partners that we speak in one voice.

And then we have to use things like benchmarking and continuous improvement to measure how we are doing and how we do things like incident reporting, how do we more quickly deal with problems like that to more quickly identify these incidences and to fix them.

Mr. ALLEN. Good. Well, I hear that we have got to centralize this issue, and we have got multiple agencies involved. So thank you so much for sharing your expertise with us.

Now, let's see, who do we go to next?

Representative Soto, I yield to you 5 minutes for questioning.

Mr. SOTO. Thank you, Chairman.

From satellites to cellphones, WiFi to the internet, there is so much information, communications, commerce, learning, telehealth, streaming and other daily activities that go through our telecommunication system.

We saw with SolarWinds, Salt Typhoon, and other cyber attacks, these were a huge warning across multiple administrations, and we are going to continue to work with you all on resiliency.

Unfortunately, we still can't protect ourselves from stupidity, as we see with the Signalgate scandal, but there have been efforts under the CHIPS Act with $3 billion for rip and replace to help with both U.S. telecom manufacturing, microchip manufacturing, and trying to replace a lot of this equipment made in China that we have no faith in anymore. U.S. telecom equipment will strengthen our network against attacks.

Mr. Stehlin, we have seen some increase in manufacturing in the U.S. for telecom equipment and microchips. How is it going so far, and what can we do to improve it?

Mr. STEHLIN. I would say, at best, it is going OK. We have a long way to go. As I mentioned before, this is a strategic, multidecade change that has to occur. We have to build the whole ecosystem for the supply chain for the ICT networks.

Fundamentally, 50 to 60 percent of the cost of every active device is the chip itself, and those chips are not made in the United States. And, if we can solve that problem, we will go a long way to having much more success in rebuilding our infrastructure, making sure that it is secure, and, also, adding jobs.

And, since you are from Florida, sir, I want to mention that we recently started a program called Broadband Nation, which is a program to attract, train, and deliver the next generation of talent in the broadband space from cybersecurity to installers, and the State of Florida is the first to sign up with us. So we are working with Miami Dade College, the Secretary of Commerce in Florida to help push this across your State.

Mr. SOTO Well, we are thrilled about that. I realize, as we are doing U.S. manufacturing, there are still going to be some inputs from abroad, whether it is metals or other things. How are tariffs affecting our ability to bring back and manufacture telecom equipment?

Mr. STEHLIN. Tariffs will only raise prices. At the end of the day, that is the problem.

Fundamentally, it makes sense to find ways to bring things back to the U.S., but if over a long period of time those prices are raised, fewer networks are going to get built, and that is a problem.

Mr. SOTO. And how would a potential recession affect investment to bring more manufacturing back? We saw a negative first quarter, first one since 2022. Do you see investments slowing, or are things moving along steadily?

Mr. STEHLIN. I haven't seen investments slowing yet, but fundamentally that is an issue. As somebody that has run a publicly traded company, I recognize that CAPX is critical, and that is one of the first things that you want to squeeze is CAPX.

Mr. SOTO. Mr. Stroup, we are proud of Cape Canaveral in Central Florida. You know, my colleague, Dr. Dunn, mentioned already the Launch Communications Act that we passed last term. We have seen 34 launches so far, mostly for satellites, right.

What are some of the strengths and advantages of satellite internet against cyber attacks?

Mr. STROUP. Thank you for the question. I think that one of the key strengths of the industry is the number of companies that are providing service and the ability to be able to provide service from multiple paths. Most satellite companies have multiple satellites, whether they are in geo or nongeo orbits, and as a result, if there is an attack on one of them, one of the satellites, there is an ability to be able to provide service from another satellite.

In many cases, companies have also deployed multiorbit capabilities. So they are bringing to bear service from both geo and nongeo systems.

And, of course, it is not just the satellites that are key in making this work. Terminals that operate across multiple operators, multiple frequencies are some of the means that the industry has to be able to address those kinds of attacks on their systems.

Mr. SOTO. So you mentioned that hive technology, where, if you take out one satellite, the rest still operate as a network. We have seen that be a strength so far in some areas, like in Ukraine.

Ms. Galante, we saw the review board for cybersafety terminated before the end of the Salt Typhoon investigation. What effect does this have on learning from what happened with that cyber hack?

Ms. GALANTE. The Cyber Safety Review Board functioned like the National Transportation Safety Board, and then it root caused major cybersecurity incidents to figure out what went wrong and then build a path towards a better remediation plan for others to learn from. Cutting off that investigation into Salt Typhoon early really limits the teleco sector's ability to understand from all the different sides of the house—the intelligence side, law enforcement, and then victim networks—how we can improve. So it really shortchanges our national security to not have that investigative board available to learn from.

Mr. SOTO. Thank you. My time has expired.

Mr. DUNN [presiding]. Thank you, Mr. Soto. I appreciate your line of questioning.

He yields back, and we recognize Representative Latta for 5 minutes of questions.

Mr. LATTA. Well, thank you very much, Mr. Chairman. And thank you so much to our witnesses for appearing today.

Mr. Stehlin, we know that Communist Chinese-flagged vessels have been suspected in cutting undersea cables across the globe, but particularly those connected to Taiwan. Taiwan has reported

five cases of seabed cable damage this year alone compared with just three each in 2023 and 2024.

Is the answer to this growing problem more cable redundancy, or are there other technologies that can provide more reliable communications in the case of a coordinated attack?

Mr. STEHLIN. Thank you for that question, sir. The answer is more redundancy. We are not going to—and find a way to find a more efficient and bandwidth-capable technology than fiber optics.

So there are 600 or so cable systems, subsea cable systems, in operation today. On average, 200 are damaged per year. And the great majority of those are Mother Nature or an anchor or something like that that is just an accident, but more and more, as you say, are coming from nefarious actors. It could be the Taiwan Strait. It could be the Baltic Sea. We have seen those in the past 6 months or 12 months. And it takes a long time to first find the problem, where is the break, and then fix it.

And, as I mentioned earlier, we don't have enough ships out there to fix. One of the three biggest repair and installation companies is called WMN Technologies, which used to be called Huawei Marine Network Technologies. So they are the ones that drive a lot of this activity in the Far East. In the U.S. we have SubCom, and in Japan we have NEC, as other examples for friendly countries. But this is a big issue that needs to be addressed. More redundancy, yes, but we have got to find ways to more quickly repair issues.

Mr. LATTA. And, just a quick followup to what you just said: How long does it take to usually fix a cable?

Mr. STEHLIN. A sub cable, depending on where it is, if it is close to the shore, it is a lot quicker than if it is in the middle of the ocean. So it could take upwards of 2 months.

Mr. LATTA. Thank you. The other followup, I am really impressed by the technological innovations happening in the last several years as it relates to the internet and cellular connectivity using satellites. Are satellites at a point that they can provide backup for large amounts of data processing in the case of a widespread physical cable outage? Just a quick followup.

Mr. STEHLIN. Sure. Satellites can certainly help and support, but the bandwidth capability and the latency, low latency of fiber cables can't be replaced.

Mr. LATTA. OK. Thank you. And I hope I pronounced it—is it "Ga-lant"?

Ms. GALANTE. "Ga-lant-ay."

Mr. LATTA. "Ga-lant-ay." I am sorry. Ms. Galante, I have always been alarmed when a business in my district says that they have had their cybersecurity handled because—and hit because of bad actors, and they are always changing tactics and becoming more increasingly skilled at targeting our networks. As soon as you get one thing done, you would find out somebody figured their way around it.

And these small businesses, in particular, small telecommunication companies, in my district and across the country aren't likely to have in-house personnel, let alone teams of professionals and cybersecurity expertise.

You say in your written testimony that we can't regulate our way to securing our digital networks. So what role can the Federal Government play in ensuring that the private sector has those tools to secure our communications infrastructure?

Ms. GALANTE. I think we need to focus effort with telco security companies, and that is really a range of different types of companies, to focus on what the goals need to be for their specific technology stacks and systems. We have done this in a large way in the banking sector and also in the energy sector. In both of those areas, there is a level of predictability and an increased ability to find malicious activity and remediate it quickly.

Those performance measures are what we need to implement and think through and make real for implementation with the variety of companies in the telco sector.

Mr. LATTA. Thank you.

Mr. Stehlin, just going back to you, I have legislation on the Routers Act, which passed the House earlier this week, to study the threat of certain routers built by our adversaries.

What are you looking at to make American-made or routers made by our allies a better choice?

Mr. STEHLIN. We need to eliminate those that are bad choices, first of all, and we have to do quick evaluations of those companies and their history and the products that they develop and remove those bad choices from the consumer.

Probably—there is an investigation underway right now for a company that is probably a bad choice but is the most frequently used home router out there.

Mr. LATTA. Thank you very much.

Mr. Chairman, we have a lot of work to do in this area.

And I want to thank our witnesses for appearing today. And I yield back the balance of my time.

Mr. DUNN. We thank the chairman for his comments, and we will recognize the gentlelady from Michigan, Representative Dingell.

Mrs. DINGELL. Thank you, Mr. Chair.

This committee has led bipartisan efforts to secure our communications networks, strengthen resiliency, and work closely with both Federal agencies and industry. We know threats are evolving and that we have got to continue to adapt. And now is the time to address additional risks across our communications technology networks, from vulnerabilities in our global supply chains and weaknesses in domestic critical infrastructure, to the risk emerging from new technologies now in mainstream and sectors like the automotive industry.

To meet this moment, we must boost competition, continue to invest in domestic innovation and manufacturing, and ensure the integrity of systems Americans rely on daily, from wireless networks to broadband and cloud infrastructure.

We are also seeing growing national security concerns from companies like BYD, a leading Chinese EV manufacturer, and DeepSeek, an emerging Chinese AI firm, raising alarms about how data is collected, transmitted, and exploited.

We have to be proactive in addressing this. We have got to secure our critical infrastructure to ensure we outpace those who

seek to undermine our national security and exploit our vulnerabilities, and we must also ensure that our Government officials are using basic security protocols for national security matters, as we have discussed, instead of commercial apps like Signal and Gmail.

But, Ms. Galante, as all of you know, China doesn't play by the rules, especially in the auto sector. China has propped up the electric vehicle and battery manufacturers with state subsidies, allowing them to undercut global competitors, flood international markets, and destroy competition.

This not only threatens American jobs and undercuts domestic manufacturing, but it also raises serious concerns about the security and the integrity of connected vehicles.

As connected vehicles collect vast amounts of sensitive personal and location data, as well as the autonomous vehicles do that they are testing here, how can we ensure that foreign adversaries, especially those with ties to China, are not exploiting these technologies to access and misuse American data?

Ms. GALANTE. Thank you, Congresswoman Dingell.

I really appreciate your question on connected vehicles' security. This is a critical area. And you can't think of one where there is more of a combination of data privacy issues, potentially GPS and other location security needs, in addition to all of the different metrics that are used and will increasingly be used to have these autonomous vehicles and connected vehicles work.

Security is critical here, and we can't tack it on after the fact. We have got to build this in, in what we call in the security industry, by design. Security by design. And one of the engineering principles that has to be at the center of how Detroit and others are focused on security in this area is called DevSecOps, development security operations, right.

We need to make sure that we have got the minds across companies and across this sector who are focused on the security implementations working together on this. And the security concerns need to outweigh some of the competitive concerns here because a secure auto industry is good for America, and it is good for our allies as well. We have to be the leaders on that, and we need to take it from the design level up.

Mrs. DINGELL. Well, I agree. I am working with a group. I have got—I am going to go to a 5G question for Mr. Stehlin very quickly.

Can you speak to the importance of beginning now to plan, invest, and lead in the next generation of advanced wireless technologies.

Mr. STEHLIN. Yes. Thank you for that question. Typically these advancements take a decade. So we are starting to work on 6G, even though 5G has just been rolled out over the past couple years.

One of the challenges is we need 5G to be financially successful, or the CFOs at the big ISPs are not going to want to invest in 6G. So it is really critical that these technologies are successful. It takes a long time to make them strong.

But, yes, we are working now on things like 6G that will affect everything from the home to the business to automated cars.

Mrs. DINGELL. So, in 40 seconds, what specific steps should Congress take to better align its efforts to help you and ensure U.S. leadership stays?

Mr. STEHLIN. R&D tax credits. Let's start there. Let's find ways to increase the investment in the United States so that we can spend more money in R&D. That innovation is something that has been a hallmark of our industry. Look at how your price per megabit has come down over the past 10 or 20 years as compared to your cost for kilowatt hours. We have gone down by 95 percent because of innovation.

Mrs. DINGELL. Thank you, Mr. Chair, and I yield back.

Mr. DUNN. Thank you, Representative Dingell. We now give 5 minutes to Dr. John Joyce from Pennsylvania.

Mr. JOYCE. Thank you, Mr. Chairman and Ranking Member Matsui, for holding today's hearing.

Thank you, also, to our witnesses for agreeing to be present with us.

We all know it is no secret that we are living in a world where our communications infrastructure is increasingly at risk. Between cyber attacks from foreign entities, such as Chinese Communist Party, to targeted network infiltration, it is more important than ever that the United States is more vigilant and prepared to defend itself against these multiple bad actors. That is why, along with Representative Susie Lee, that I introduced H.R.2061, the Information and Communication Technology Strategy Act.

This important legislation will develop that the Department of Commerce is consistently updating Congress on what needs to be done to adequately secure our communication systems through our supply chains. This will be one step in a long list of necessary actions that the U.S. Government needs to be taking to adequately protect our critical networks.

Mr. Jaffer, how would you evaluate the readiness of our current telecommunication systems against these identifiable and well-known bad actors, and I will list them: Specifically, how are we prepared when it comes to China, when it comes to Iran, and when it comes to North Korea,who we recognize are repeat offenders?

Mr. JAFFER. Well, you know, Dr. Joyce, we are very—we are ill prepared. Our telecommunication infrastructure is vulnerable. We know it, our Government is not effective at deterring bad activity by our adversaries, and we are not working together collaboratively to defend that piece of critical infrastructure.

There are other pieces of critical infrastructure as well that we are not good at defending, but that is one area where we need to work more effectively as a government and industry together.

There are a few things we can do in the immediate term to address some of these issues. One, to your point about supply chains, we know today that we rely massively on China for things like semiconductors, critical minerals. We are seeing it today in the tariff wars, where China is cutting us off from critical minerals. We need to develop a domestic and ally capability to refine, to extract and refine those.

We have critical minerals here in the United States. We have the ability to obtain them for our allies and partners abroad. We sim-

ply send 96 percent upwards of that material in kiers over to China to refine. It makes no sense.

The signature semiconductors, we see the situation in Taiwan. If we are going to survive on our current technology basis, we have got to be able to defend Taiwan. China is threatening it. It is not clear that if today China were to go across the Taiwan Straits, that the United States would do anything or that we could get there in time to effectively defend our friends in Taiwan.

Mr. JOYCE. Mr. Jaffer, can you help me understand a different issue? How has Huawei become the global behemoth that it is today, and what more do we need to do to counter Huawei in the spread of untrusted telecommunications equipment, especially when we see allies and partners using equipment from Huawei?

Mr. JAFFER. Dr. Joyce, it is a great question. The way they have obtained this advantage is they have done it on the backs of stolen intellectual property from American companies, including Cisco. They have built routers that look a lot like a Cisco router because they stole that technology.

Now, they have improved on it. They modified it over time, but that is where they stole it from in the beginning.

On top of that, they have depended on low-interest loans and no-interest grants from the Chinese Government. The Chinese Government goes around the globe subsidizing their purchases, giving countries other stuff, other benefits for taking Huawei equipment.

And so we have got to compete in a world in which China is acting noneconomically to put their surveillance gear in place in allied countries and countries around the globe—not just allies, but partners as well. We can't do that effectively until we partner with our friends who make telecommunications.

We don't make a ton of handsets. We make a lot of routers. We make a lot of core network gear. Then we have to get that into those networks.

We did rip and replace at home. That is amazing. That is the right thing to do. We have got to do global replace, and that means putting some of our money and incentivizing our manufacturers and giving them the capabilities to go abroad and deliver that capability to our friends the way the Chinese are doing against us with the Huawei and ZTE.

Mr. JOYCE. Mr. Stehlin, in the moments that are remaining—first of all, thank you for your leadership and your advocacy at SIA. But what specific actions have your member organizations taken to protect themselves against the attacks and strengthen the supply chain?

Mr. STEHLIN. Yes. So we are and our members are very much focused on the processes that are used to develop new products. It is, as you mentioned a minute ago, a big challenge with companies, companies like Huawei, that undercut us financially, often selling below cost just to win the business and to hang onto it.

We need to rebuild our infrastructure here in the U.S. We need to rebuild our vendor base in the U.S., and it starts with the ICT space, specifically with semiconductors.

Mr. JOYCE. And I thank you. And I think you, I, and President Trump all recognize that building that infrastructure, that supply

chain right here in the U.S. is important and, actually, paramount for our success.

I thank all of our witnesses for being with us here today, and, Mr. Chair, I yield.

Mr. FRY [presiding]. The gentleman yields.

The Chair now recognizes the gentlelady from California, Ms. Barragán.

Ms. BARRAGÁN. Thank you, Mr. Chairman. We just heard that it is important to build the infrastructure here, chips made in the U.S., develop a domestic capability. We kind of heard this.

Mr. Stehlin, you brought this up—and this hearing, by the way, is called "Securing the Future of Communications Infrastructure." If we repealed CHIPS, if we repeal the CHIPS Act, would that be helpful?

Mr. STEHLIN. No.

Ms. BARRAGÁN. OK. Why would it not be helpful?

Mr. STEHLIN. It would not be helpful because we need more capital investment in the United States. It needs to be a strategic investment.

I won't address some of the specifics of the CHIPS Act. But, fundamentally and strategically, it is critical that these skills be brought back to the United States as quickly as possible.

Ms. BARRAGÁN. Thank you. I also disagree withthe President that we should repeal the CHIPS Act.

Ms. Galante, in 2017 the San Pedro Bay Port Complex, the busiest in the Nation and located in my district in southern California, experienced a major ransomware attack that forced the shipping company Maersk to halt port operations for several days and ultimately cost the company over $300 million.

This cyber attack prompted the port to establish a Cyber Resilience Center, which monitors the port's technology environment and now fends off 80 million cyber attacks per month.

Ms. Galante, from a national security standpoint, how vulnerable are ports to cyber attacks from foreign adversaries and other bad actors, especially if cybersecurity has not been prioritized in these sectors?

Ms. GALANTE. Port security is national security, and this area and the technology underneath of it is incredibly reliant on digital technology, and ever more so each year.

We have also seen—you mentioned a recent ransomware attack. There has been a variety of targeting at ports in the U.S., but also globally. We have to up cybersecurity in this space.

Last February there was an EEO on maritime cybersecurity. It put $20 billion into this. And I think that was an important investment, and it gave the Coast Guard additional authorities and responsibilities in cybersecurity. We have to take port security seriously.

Ms. BARRAGÁN. Thank you. Cyber attacks often also hit marginalized communities the hardest with disruptions to hospitals, schools, and public services in communities of color that have already seen less resources and support. In fact, people of color have a 12 percent greater chance of experiencing some sort of financial damage resulting from a cybercrime incident and are 6 percent more likely to have their identity stolen.

Ms. Galante, what steps should Congress take to ensure our National Cybersecurity Strategy prioritizes the protection of these vulnerable communities?

Ms. GALANTE. You mentioned two sectors specifically: healthcare, and education and schools. These areas have been really hard hit by ransomware attacks over the last few years. And one of the reasons is because their security posture is incredibly weak. Schools don't have the funding to put in place the types of security measures that the banks, for example, do. We need to find some middle ground that makes these targets more secure.

The other piece here that we haven't talked about but is an enormous problem across the country are cyber scams. I bet everyone in this room has gotten some text saying an Amazon package is headed their way, or "double click" or "message me back, I have a great offer for you." Even love scams. This is a real epidemic that we have here.

And the term in the cybersecurity community is called "pig butchering." What they will do is use social engineering, use a conversation to aggregate and get people to put their funds—sometimes student loan debt, other places where they have money and exposure and are really looking for a way to get money and get out of a bad situation—and they will go and invest it in a fake crypto scheme.

A lot of these criminals behind this activity are in Southeast Asia, they are in Eastern Europe. And they are profiting from it. We need more exposure, and we need to shine a light on these cyber scams and what they are doing to everyday Americans.

Ms. BARRAGÁN. Great. Thank you.

Mr. Jaffer, when I got to Congress, I had two phones. One is my personal phone, and one is a government-issued phone. If I am going to have a conversation with somebody on one of these phones that has classified information, which one should I use?

Mr. JAFFER. Neither one.

Ms. BARRAGÁN. OK. But this one has Signal on it. Are you telling me that Signal—I shouldn't be having classified conversations on Signal?

Mr. JAFFER. No. As Ms. Galante correctly laid out, we have systems for classified communications today—are the only places to have classified communications.

The problem, of course, is those devices, particularly if you are talking about TSCI data, are in SCIFs, right. You can't have classified communications outside of a SCIF at the TSCI level.

So, if you want to communicate about an ongoing activity, you have got to figure out a way to do it. Signal is not a good way to do it.

At the same time, if we don't give our Government officials capable ways of communicating on the fly—the reality is everyone expects instantaneous communication today. That is just the world we live in. And so if you are a Government official, you are in a tough position of saying, "Do I have to go to a SCIF? How do I do that?"

Using Signal is not the right answer, but we have got to give our senior leaders and our Government officials a way to communicate that works on the fly, on the run, that doesn't force them to go in

a room and hide out. Otherwise, they will never use it, and they will find workarounds, and then we will have bad situations where they are having communications over systems they are not authorized to have them over.

Ms. BARRAGÁN. Thank you. You would think the Secretary of the Department of Defense would know that.

I yield back.

Mr. FRY. The gentlelady yields.

The Chair now recognizes the gentleman from Florida, Mr. Bilirakis.

Mr. BILIRAKIS. Thank you.

I appreciate it very much. I thank the witnesses for their testimony today.

I want to start off with Mr. Stehlin. In your written testimony, you mentioned your organization developed the SCS 9001 supply chain security standard. I am a big proponent for industry-led standards generally, but, of course, there has to be something in it for the participants for it to work.

What fundamental elements does a company's product have to show it to receive a certification under your system, and what benefits result from achieving certification?

Mr. STEHLIN. Thank you for that question. Yes, the benefits are tremendous in that you can verify trust, and you can prove that your product, hardware, software, as well as the company itself is a trusted supplier. A service provider or a government or a critical network operator is going to want to buy from companies that have proven that their products are trusted.

And then we use continuous improvement to constantly upgrade the processes. We don't tell a company through the standard how they develop a product. They just have to have certain processes and controls in place and verify that those are there.

Mr. BILIRAKIS. Thank you very much.

Mr. Jaffer, when talking about the Salt Typhoon, much is said about how data, political figures, and corporations were compromised, and that the threats they can pose to national security and business interests. However, less is said about how the privacy and data for—of everyday Americans was compromised and is impacted.

Why should the average American be concerned about the Salt Typhoon attacks on their own data, and what threats does China pose to them by having this individual data?

Mr. JAFFER. Well, Congressman Bilirakis, it is a great question. The challenge that we have today is that the Chinese deeply infiltrate our telecommunications networks. That means they have access to massive amounts of metadata of ordinary Americans. The communications that you and I have, a phone call, the date, time, and duration of that phone call, potentially the same date/time duration of emails that we engage in, and then they can choose who to go after.

So we know they can get both metadata and content. So average Americans should be worried that they have all their metadata, and then, on top of that, if the government, if the Chinese Government chooses to, they can go and collect the contents of those communications as well. So it is a full spectrum capability—if we had

that capability on Chinese networks, we would be thrilled—the Chinese achieved our networks, and yet today we are not focused on this problem, right. We are talking about Signal chats and the like. And, no doubt, that is a big problem, but the real threat is that our entire telecommunications infrastructure was compromised, and the U.S. Government has not responded to it, has not taken accountability for its own failures in detecting that threat and helping our telecommunications system defend it. Instead, our Government has said, "We will blame the telecommunications providers."

You are never going to beat China if you are a private-sector company. You have got to have the Government's help. The Government is not doing its job. This is never going to work.

On top of that, the American people should also be worried about apps they have on their phones like TikTok, which collect massive amounts of data on them. People think, well, you know, these are just videos of kids and dogs and—but the reality is, is that it is collecting a tremendous amount of information, not just who you are communicating with but your voice as well, numerous times, and it passed that data back to Chinese Communist Party.

We have a law—the Congress passed a law in a bipartisan way. That law has yet to be implemented because we, you know, we made a political call that it is better to have TikTok running. We need to enforce the law that is in place today. TikTok should be banned in this country. And, to the extent that American people have access to it, they should take it off their phones because they are voluntarily letting the Chinese Government onto their devices to collect data on them. When you combine that data with all the other information the Chinese Government has, that it is going to conduct a very significant intelligence and operations against American citizens around the globe, that is a bad day for America.

Mr. BILIRAKIS. Thank you very much. I appreciate it.

I yield back, Mr. Chairman.

Mr. FRY. The gentleman yields.

The Chair now recognizes the gentleman from Louisiana, Mr. Carter.

Mr. CARTER OF LOUISIANA. Thank you, Mr. Chairman.

And thank you, witnesses, for being here today. Today's hearing addresses a matter of urgent national importance. I believe this is an important hearing, and the security challenges we face are real, and they can be met with bipartisan cooperation. And I am enthusiastic that this committee can do just that.

Our telecommunications infrastructure faces daily threats from hostile foreign actors, cyber criminals, and even policy failures here at home that we just heard of moments ago, but adversaries like the Chinese Communist Party exploit vulnerabilities in our networks to spy, disrupt, and steal.

The American people are also endangered by reckless behaviors within our own Government. However, I must echo many of my colleagues' comments who are concerned about recent security failures where senior defense officials are using unofficial and unsecure messaging apps like Signal to share sensitive and classified information that should have been put in a SCIF or some much more secure place for communications. We cannot have an important

hearing like this and ignore irresponsible and dangerous lapses of judgment like this.

As President Trump shifts responsibility for cyber defense to underfunded localities, dismantling national protections and disregarding bipartisan security legislation, our country is left more vulnerable. Meanwhile, Democrats are always willing to work across the aisle to modernize and secure our communications.

My home State of Louisiana and the Nation must have the resources necessary to make sure we have the capacity to update our networks and provide for expanded broadband access. Funding for B programs has been vital, have been a vital component to the State's initiative to reduce the digital divide. Yet, in Louisiana, abruptly, before—just as we were completing our final stage, this administration froze those funds, negating all the work that had been done to advance this vital tool in our cybersecurity. This is a problem passed and implemented by a bipartisan Congress—a program that was passed, implemented by a bipartisan Congress. I can't say that enough.

As we look forward to working with my colleagues across the aisle to pass the Next Generation 9–1–1 Act, we must not allow our public safety telecommunications and telecommunicators and first responders to do their jobs with outdated equipment and technologies. It is a must.

I have heard each of you speak. You have spoken eloquently on the needs that we as Members of Congress can do and how we can listen better.

Some things are political, and most things are not. This clearly is one that should not be.

Ms. Galante, in your testimony, you discussed the Salt Typhoon attack that was unprecedented in scope. What risk are we taking by not moving to provide adequate funding to update the 9–1–1 network infrastructure around the country to a more IP-based technology like NG9–1–1——

Ms. GALANTE. The emergency response 9–1–1 networks are incredibly critical to secure, and we have to up the posture on these different organizations and provide the funding to do it.

In fact, over the last several years, emergency response centers and 9–1–1 lines have been widely targeted, especially by ransomware groups who look to freeze those networks and then get a payment in return. We have seen this happen in Texas and Pennsylvania and Florida, and there's probably many unreported instances of this as well. This is critical. We don't want to be in manual dispatch mode when you have ambulances going out.

Mr. CARTER OF LOUISIANA. Mr. Stehlin, OpenRAN allows different parts of our network to be supplied by different equipment and software vendors. My understanding as this plug-and-play approach means that no one vendor has the lock on any component within the network.

How does this plug-and-play approach promote competition among vendors while benefits to everyday consumers like we see with other emerging technology?

Mr. STEHLIN. Thank you for that question. OpenRAN is an excellent technology that allows various aspects of a wireless network to be purchased from various vendors. So, if you have common con-

tinuity between the various parts, if the connections between a RAN device and a base station router are opened up, it allows more competition, so——

Mr. CARTER OF LOUISIANA. You leave me about 6 seconds. Go on.

Mr. STEHLIN. The last thing I would say there is it is a challenging game to build wireless networks.

Mr. CARTER OF LOUISIANA. Thank you. Mr. Jaffer, you mentioned just a moment ago about TikTok and the fact that this bipartisan body passed a ban on TikTok because of the massive breach and threat that it has for our cybersecurity. It has been extended 90 days, and now it has gone beyond that 90 days.

Every day that goes by that the Communist China Party continues to collect the data, what kind of risk does that put our cybersecurity and country in?

Mr. JAFFER. Mr. Carter, that—allowing TikTok to remain on American phones creates a massive, unprecedented risk to America's national security and the privacy and security of every single American citizen who has that app on their phone. It should be—people should voluntarily remove it immediately. The law should be enforced. There is no provision in the law that allows it to be extended beyond 90 days. There is one 90-day extension allowed by law if, in fact, there is a deal in process. There is no provision for a 90-day extension. The law should be enforced today.

And it is worth noting that even if the administration chooses to voluntarily not enforce the law against providers who allow TikTok to remain on their networks in the app stores and the like, those app providers and app subscribers can be held liable in a future administration if it is within the statute of limitations.

So everybody who is allowing TikTok to remain on their devices should know that they are potentially exposing themselves to liability, even if this administration chooses not to enforce the law, in a future administration.

Mr. FRY. Thank you. The gentleman's time has expired. The Chair now recognizes the gentleman from Georgia, Mr. Carter.

Mr. CARTER OF GEORGIA. The other Carter—from the right coast.

Thank you all for being here. I appreciate it very much.

Let's talk about subsea cables because we know they are the backbone of the internet, and we know that they are critical for intercontinental communication and transactions. In fact, it is estimated that $10 trillion of financial transfers occur daily as a result of the subsea cables.

Ten trillion dollars daily. That is a lot of money. That is a lot of transfers.

Anybody who has read the news lately understands that, in the past 6 months, our adversaries have been using and targeting these cables and cutting into critical—to cripple the economic and national security of countries around the world. Obviously, an easy target. We understand that.

Let's talk about the importance of redundancy, because redundancy is extremely important in the resilience of our cables and the diversity of routes that are needed to ensure we limit our vulnerability whenever we are talking about these cables.

I have been working to try to expedite the permitting process of cables in the National Marine Sanctuaries with my bill H.R. 261,

the Undersea Cable Protection Act, and I think we need to think about ways to expedite the permitting process more generally too. We need to get more cables deployed as quickly as possible and ensure that we can meet the capacity needs.

Mr. Stehlin, I want to ask you, can you explain why redundancy is so important for subsea cables, and how important it is from a national security perspective that we don't have one single point of failure?

Mr. STEHLIN. Thank you for that question. Yes, it is really critical that you don't have a single point of failure. As I mentioned earlier, there are about 600 subsea cables in operation today around the world but something like 1,700 landing points. So, as a cable gets closer to shore, it will split and have multiple landing points. We need to increase the number of cables, yes, but we also need to increase the number of landing points here in the United States. There may be 90 or so landing points in the United States.

As you mentioned, permitting is a major issue. In some cases, it can take 400 days on average to get a permit, and sometimes up to 900 days to get a permit.

Mr. CARTER OF GEORGIA. Nine hundred days.

Mr. STEHLIN. Nine hundred days. And so I would argue that, perhaps, we put NTIA, which is the President's advisor for telecom issues, in charge of Team Telecom instead of the DOJ. They look at it from a different perspective. DOJ absolutely should be on the committee but perhaps not have the lead.

Mr. CARTER OF GEORGIA. So I mentioned my bill, H.R. 261, which also aims to prohibit duplicate permits that are currently being required by NOAA in marine sanctuaries especially. I know that there are other areas where there are duplicate permitting reviews that are delaying the deployment of cables.

Can you suggest, Mr. Stehlin, where the committee might be able to work to streamline the permitting process for subsea cables?

Mr. STEHLIN. Yes, a great example might be a trusted partner framework. So, if somebody has built a cable in the past and has proven themselves, should they have to go through every single step yet again, or can they get fast-tracked because they have proven themselves to be a trusted partner?

Mr. CARTER OF GEORGIA. Good. Good. Excellent. The special-use permits that are issued by NOAA are limited to a 5-year license term, which is in stark contrast to the 25-year FCC license term.

Can you speak to the justification of possibly having a 25-year license term for subsea cables and the importance of a guaranteed 25-year term from an investment perspective?

Mr. STEHLIN. Yes. Typical payback for these subsea cables might be 7 years just to break even because you are talking hundreds of millions of dollars of investment upfront, and then you have to go through the permitting process—it might be pulled out, et cetera.

So, by having a longer-term license, it ensures that the company is going to make that investment. If you have 7 years' payback just to break even, that is a tough business decision.

Mr. CARTER OF GEORGIA. I want to talk in general terms right now, and when I say "general terms," I do mean general. I don't care what sector of our economy you are talking about, when people come into my office, when businessmen come into my office,

businesspeople come into my office, it is always the same story, whether it be—whether it be communications, healthcare, energy: "Permitting, regulations crushing us. Crushing us. We have got to do something about this."

Thank you all for being here. Very, very important. I yield back.

Mr. FRY. The gentleman yields.

The Chair now recognizes the gentleman from New Jersey, Mr. Menendez.

Mr. MENENDEZ.Thank you, Mr. Chairman. With international cybersecurity threats on the rise, we are facing increasing threats to our critical infrastructure and our economy.

This past fall, the U.S. experienced a devastating Chinese state-sponsored attack on our telecommunications networks, stealing sensitive geolocation data and targeting both Democratic and Republican elected officials.

We have heard throughout this hearing about bipartisan support for defending our country against cyber threats, as we should, but the Trump administration has been weakening our country's cybersecurity defense system by slashing our cyber workforce and recklessly transmitting sensitive information, making it easier for our foreign adversaries to access Americans'—Americans'—most sensitive personal data.

Ms. Galante, just yes or no, will the Trump administration dismantling the Cyber Safety Review Board weaken collaborative security and intelligence work?

Ms. GALANTE. Yes.

Mr. MENENDEZ. Ms. Galante, is a public-private security ecosystem necessary for a strong collective defense and national security posture?

Ms. GALANTE. Yes, it is critical.

Mr. MENENDEZ. Mr. Jaffer, you even said yourself, private companies cannot compete with China alone. So it seems that a public-private security ecosystem is essential for our national security. Would you agree with that, yes or no?

Mr. JAFFER. Absolutely.

Mr. MENENDEZ. Thank you.

Ms. Galante, going back to you, with China investing heavily in recruiting and training their cyber workforce, is it important to our national security for the U.S. Government to maintain a robust cyber workforce capable of defending against cyber attacks?

Ms. GALANTE. Incredibly important.

Mr. MENENDEZ. And not just maintain it, but we should be growing it and doing everything we possibly can to get more people at community colleges, at universities across the country, to begin their career in cybersecurity; is that correct?

Ms. GALANTE. Especially at this moment.

Mr. MENENDEZ. Thank you. That is why I am concerned about reports that DOGE plans to cut 1,300 jobs from the cybersecurity workforce at CISA. In fact, even the former head of CISA under the first Trump administration said that he is outraged by these cuts, and I look forward to all of my Republican colleagues joining me on a letter to the administration on this issue.

Sticking with the theme of DOGE cuts, I want to ask a few questions about the increasing number of reports that DOGE has been

leaking and weaponizing Americans' personal data. It seems like every day we hear another report about the mishandling of our personal information—and this is just the first 100 days. From individuals with Russian IP addresses attempting to log into Federal databases at the NLRB to DOGE employees gaining access to networks that hold nuclear secrets, it has become clear that the Trump administration cannot be trusted with our personal information.

Ms. Galante, should Americans be concerned about reports that individuals with Russian IP addresses have attempted to log into a Federal database that holds our personal information?

Ms. GALANTE. Yes. IP addresses coming from Russia and network traffic coming from Russia is typically blocked. So I am surprised that this isn't already getting filtered out.

Mr. MENENDEZ. There have also been reports that ICE is in the process of pulling together data from across Federal agencies for a database they call the alien tracker in order to facilitate mass deportations.

Ms. Galante, just yes or no, would a database that stores personal data from multiple agencies across the Federal Government, such as the alien tracker, be a target-rich environment for our foreign adversaries to attack?

Ms. GALANTE. It would be a prime target.

Mr. MENENDEZ. And once we accept that this administration is going to collect our personal information and put it into a database, whether it is for immigrants or any other group of Americans, it makes it highly susceptible to foreign attacks and puts all of our personal information at jeopardy. Would you agree with that?

Ms. GALANTE. Highly valuable in our adversaries' hands.

Mr. MENENDEZ. So let's turn to AI quickly, because I believe you would agree that AI has increased the sophistication of cyber attacks against target-rich datasets.

Ms. GALANTE. Yes.

Mr. MENENDEZ. And can you just briefly explain. Empowering AI, there are two components, as I understand it. Downstairs, we are on the Energy Subcommittee talking about the energy that goes into AI. The other is the collecting and use of data. Is that correct, and can you speak to that?

Ms. GALANTE. Sure. On the collecting and use of data, your processing powers are incredibly multiplied when you are looking at datasets. You are able to find patterns. You are able to find different insights within large datasets. You are able to cross different modalities. This is the sort of the way that highly analytic endeavors are shorthanded and quickly given to our adversaries so that they can figure out how to make sense out of the noise in huge datasets and deploy them against us.

Mr. MENENDEZ. And this goes back to why we originally banned TikTok. Is that correct?

Ms. GALANTE. It is one of the reasons why TikTok could provide a powerful dataset to our adversary.

Mr. MENENDEZ. So, while AI is strengthening our enemies' cyber capabilities, the Trump administration is leaving us vulnerable to attacks and weaponizing our data against us. This is not a Democratic-Republican issue. Any administration should prioritize pro-

tecting Americans' sensitive data, and my Republican colleagues cannot pretend to take threats from foreign actors seriously while the Trump administration is slashing CISA's workforce and allowing unauthorized DOGE employees to access Americans' data on demand.

This should be a bipartisan issue. It is one I am concerned about. I dealt with it on Homeland Security with Mr. Pfluger—sorry, the clock went off, so I couldn't tell—that we should all be in lockstep on, but that means we have to speak out when our administrations, Democrat or Republican, are failing us. This administration is failing us on this critical issue. Thank you, and I yield.

Mr. FRY. The gentleman yields.

The Chair now recognizes the real chair, Mr. Guthrie from Kentucky.

Mr. GUTHRIE. Not the real chair. The other chair.

So, hey, thanks a lot. I appreciate you guys being here. And, first, Mr. Stroup, I am kind of concerned about satellite GPS. And I am an old artilleryman. Old artilleryman. In my day, you had to use binoculars and see where a round landed, and then you would call it back in, and somebody would use that—literally a slide rule to calculate what the data was, and you had to walk—you had to bracket the target, as we say, or walk it out.

And, now, this has been years. So I don't even know what they do now, but they shoot a shot, they lase the—or they lase the target, send a GPS code to the guns. They shoot, lase the bursts, send the GPS code to the gun, and the guns adjust, and it is one round fired for effect now. That depends on satellites.

So my big concern on satellite security, I mean, just walk through the national security—that is just shooting artillery. That is a whole lot of things that our satellites depend on in the civilian world, but also particularly our military world.

I used to be the proverbial lieutenant with a map. Now you get an eight-digit ZIP Code—just by knowing what your watch tells you. So how do we do that? How do we fix the map?

Mr. Stroup, I guess I couldn't see you. Mr. Pfluger is a tall guy. Sorry.

Mr. STROUP. Thank you for the question. So, yes, obviously adversaries can use location information. The key from our perspective is ensuring that they are not subject to spoofing and to jamming. So the next generation of GPS satellites have increased capabilities against them. And, actually, I think it is important to note that there is already a redundant system for navigation system——

Mr. GUTHRIE. How do you make it redundant for—I know you have got navigation. You have got—I mean, that is just as simple as, like, low artillery. You are talking about 2 or 3 miles communication to each other.

Mr. STROUP. So GPS is a free system provided by the Government. There is also another system operating off of a constellation of satellites, and there are also studies underway to look at other systems. But, certainly for the importance of all of the uses, whether it is military or commercial, we do have redundancy built into the system.

Mr. GUTHRIE. OK. Thank you. I was looking at—Mr. Stehlin, I was looking at you because I couldn't see Mr. Stroup. So I will ask

you this. I mentioned in my opening statement a concern for subsea cables. I mean, gosh, we have so much to protect. What are the threats to subsea cables, and how can we be less susceptible to damage?

Mr. STEHLIN. Redundancy, number one. Number two is having a repair system that is very quick and accurate, meaning more ships, a big shortage of ships, more landing points adds redundancy in the United States, and working with friendly governments to ensure the equipment they are using is trusted equipment.

Mr. GUTHRIE. OK. Thank you. I am not sure how much time I have, but, Mr. Jaffer, the Rip-and-Replace, we led that effort. And, when we think about supply chains, what else do we need to do?

Mr. JAFFER. Well, Mr. Chairman, I think certainly Rip-and-Replace going global is going to be critical, right, because what is happening is our adversaries are putting this Huawei and ZTE and other Chinese gear in around the global. So it is important to expand that broadly.

Beyond that, we need to look at other core supply chains, semiconductors, critical minerals. We know the Chinese have a choke hold on these things, whether it is the processing of critical minerals or the like. We need to get ahead of that and get ourselves out of that.

And then, finally, we need to look at the entirety of the American supply chain. We realized during COVID that we have this dependency on China pharmaceutical precursors, and yet we continued to maintain and allow ourselves to be addicted to Chinese goods of all sorts.

It is one thing to buy T-shirts from China. It is a whole other to buy critical minerals, semiconductors, and routing and——

Mr. GUTHRIE. We had a hearing on medical devices, and we found in the medical device, because it was an investigation and oversight hearing, they had connections with ERL at the University of Beijing, and medical device, just collecting massive amounts of data, I think Mr. Menendez is talking about, so they use it in their AI.

Mr. JAFFER. And just think about connected cars. Think about the havoc you could cause if instead of having a bunch of, whether it is Teslas or Slates, or whatever American EV manufacturer you want—Chevy, right, Ford—if we had a bunch of BYD cars running around the United States—which is what, by the way, China wants us to do. Part of the reason they are cutting us off from critical minerals is they want us to buy their electric cars so that those electric cars are connected. They could turn it off when the time is right.

Mr. GUTHRIE. Well, thanks. I am not sure—I don't see the clock. Have I got a couple minutes?

So I was in Europe, I was on a NATO meeting, and we were talking about all the privacy. We have to deal with privacy on this committee as well, so very interested in that. And my question was, If you have a system of Huawei and ZTE, should you even worry about your privacy? Do you have privacy even if you regulate privacy?

Mr. JAFFER. You know——

Mr. GUTHRIE. Doesn't it seem kind of inconsistent to say we are going to have all these privacy laws, but then we are going to let all the Chinese equipment in our country?

Mr. JAFFER. It is astounding to watch the Europeans come after American companies because they are concerned about our privacy rules and our privacy regulations, and yet, one, they buy tremendous amounts of Chinese gear and are willing to give their privacy up to the Chinese.

We also note that, you know, the Europeans have massive surveillance capabilities internally. They never talk about those. They talk about our industry and our companies. They don't talk about their own government surveillance capabilities.

So I think it is really important to think, look, at the end of the day, if you have to make a decision, you could be like the Europeans, and you can regulate first and innovate second, or you could be like the Americans and innovate first. That's what we have got to do.

Mr. GUTHRIE. Thanks. I can't see a clock, but I think they just gaveled me down, so thank you for your answers. I appreciate it very much. Thanks.

Mr. FRY. The gentleman yields.

Before we recognize the next person, we are going to reset this clock.

[Pause.]

Mr. FRY. There we go. The Chair now recognizes the gentleman from Ohio, Mr. Landsman.

Mr. LANDSMAN. Thank you, Mr. Chair. I appreciate all of you. I want to get into the undersea cable issue. And we have talked about this extensively, rightfully so, and would ask, Mr. Chair, for unanimous consent to enter into the record an article in Newsweek about China: "China Unveils Game-Changing Weapon That Could Decide Future Wars." It just speaks to the fact that cybersecurity is national security, and national security is cybersecurity.

And the article goes into, obviously, everything that China is doing with their submarine technology to disrupt these cables. The vast majority of communications goes through these cables, 95 percent of everything that we do globally. And your testimony today suggests there are several things that we have to do: One is the redundancy work; two is the ships; three, I am assuming, is part of the repair work, but the technologies, the sensors. I mean, I—and maybe I am jumping to a conclusion here that doesn't exist, but I assume that there are early detection work that we could be doing, or do we find out immediately when these things happen?

So I am wondering if you can say a little bit more about—or speak to existing legislation. I know Mr. Carter has a bill around permitting, and that is something that I think we should all jump on and support, especially to your point about trusted partners who are already doing this. Can you talk a little bit about the ships, what we would need to do. What does that look like?

Mr. STEHLIN. Yes. There are certain ships that are designed to lay and repair cables. You can go to Baltimore Harbor and see them from time to time.

Mr. LANDSMAN. Yes.

Mr. STEHLIN. That is one place to see them. And these ships lay out the cable. They are specifically designed to do this. Finding the problem, it can get isolated fairly quickly, because once you lose a signal you can identify where——

Mr. LANDSMAN. Fair enough.

Mr. STEHLIN [continuing]. The problem is, using something called an OTDR, an optical time-domain reflectometer, all right. So that is something that you can use to find out where the problem is. But then you have got an issue of what are the seas like, has the cable moved or shifted around because of tides and currents and things like that.

So adding more ships and having this be a better and bigger industry is really important on top of ensuring that Western technology and Western companies take back the lead in this, rather than Huawei.

Mr. LANDSMAN. How many ships do we have now? How many do we need?

Mr. STEHLIN. I can't answer specifically, but it is single digits to low, maybe. perhaps a dozen.

Mr. LANDSMAN. Yes. Go ahead, sir.

Mr. STROUP. If I may, since the issue of redundancy for undersea fiber cables has come up, I want to stress the importance of satellite, the ability to be able to transition immediately. And while we certainly don't have the ability to carry all of the traffic, as an example, that is carried into Taiwan, what they are doing, I think, is a good example of how we prepare for the potential of an undersea cable cut, and that is putting in place arrangements with multiple satellite companies, obtaining the terminals so that they do have true redundancy in real time. Thank you.

Mr. LANDSMAN. Yes, I think that makes sense. And I think the only point you were making, sir, is that it is not—it is good for redundancy and for those moments of acute need but not necessarily an alternative to the fiberoptics.

I want to get back to the ships. Sorry. If it is single digits, I mean, do we need twice as many?

Mr. STEHLIN. The more landing points, the more cables we have, definitely the more ships you need.

Mr. LANDSMAN. Yes.

Mr. STEHLIN. And there is no doubt about it.

Mr. LANDSMAN. OK. So is there anything else? I mean, between Mr. Carter's bill, getting additional ships, the satellite partnerships that, you know, would expand our capacity, is there anything missing in terms of——

Mr. STEHLIN. Yes. I would reiterate the permitting process——

Mr. LANDSMAN. Yes.

Mr. STEHLIN [continuing]. Needs to be sped up. And, again, I think NTIA ought to have the lead with telecom.

Mr. LANDSMAN. Oh, NTIA. That was the other piece.

Mr. STEHLIN. Yes.

Mr. LANDSMAN. NTIA, got it. And then I know that Mr. Carter's bill does the permitting, or at least that is—it sounds like it does, but the NTIA piece I am not sure is—I will look into that. I appreciate that. That makes sense.

And I yield back.

Mr. FRY. The gentleman yields.

The Chair now recognizes the gentleman from Ohio—or Ohio—Idaho, Mr. Fulcher.

Mr. FULCHER. Thank you, Mr. Chairman.

Mr. Stehlin, I represent the great State of Idaho, and there is a lot of rural space there. And a lot of the ISPs don't have a tremendous number of cybersecurity resources, but yet, they will oftentimes be integrated with major infrastructure components, whether it be a power plant or a grid or flood control or some of those major things, and oftentimes can have an impact there without necessarily the infrastructure or the cybersecurity expertise to fend off some of these new threats that are on their way.

I would like to get any suggestions or comments from you on how CICIG might be a resource for that or other sources of counsel through your role at TIA.

Mr. STEHLIN. Thank you for that. Yes, Idaho is a tremendous opportunity to take advantage of the moneys put forth with Rip-and-Replace, for example. You know, these rural operators have a hard time making money running a business when you are so spread out. So removing things, untrusted gear like Huawei or ZTE gear, critically important. Number two, the BEAD money, very important for States like Idaho, to help those unserved and underserved.

So finding ways to continue to push that money out to rural America is very, very critical, and the way that it is connected to your industry, not just to the consumer. All that is especially interwoven in rural America, so industry as well as rural America consumers are tightly connected, and therefore the networks need to be tightly connected.

Mr. FULCHER. Thank you for that.

I want to do a followup question, same general subject matter, but having to do with cybersecurity incident reporting requirements. That is another one of those things that can be cumbersome, especially if you are a small ISP, and I wanted to get your comments on that as well. Is harmonizing maybe an option or other forms of report sharing something that we should be looking at a little bit deeper?

Mr. STEHLIN. Absolutely. We need to speak in one voice. We need to have one way of reporting incidents. Right now, every company and many agencies and departments in the Government and in State governments have different ways of reporting things. So with all these different requirements, and you are a small rural company, who do you respond to? How do you quickly identify the problem, quickly resolve the problem?

If we speak in one voice and have one voice of mitigation and incident reporting, we will more quickly fix the problem, and then we will continually improve, because that is what a good benchmarking system does. It allows you to get better and better.

Mr. FULCHER. Thank you for that as well.

I am going to shift to Mr. Jaffer, and I am going to magically make you king for a day, OK.

Mr. JAFFER. I love that, Congressman Fulcher.

Mr. FULCHER. Undersea cables——

Mr. JAFFER. Sure.

Mr. FULCHER [continuing]. We have been talking about that a lot, and I don't want to regurgitate what others have brought up or similar questions. I know—I have made notes of the patrolling issues, satellite monitoring, the permitting issues that we have got, the need for redundancy. What we haven't talked about is penalties for nefarious actors, or at least that I have heard. But as king for a day, could you hit that topic again? What are the steps we need to be taking?

Mr. JAFFER. Look, we have to make it clear to our adversaries, Russia and China primarily, when it comes to undersea cables, that we view those as part of our critical infrastructure, and if those are hit and we know it is them, we will make them pay a price. That price could be economic, it might be sanctions, it might be military. The truth is that we rely so much on these networks.

And, by the way, they have similar capabilities in counterspace as well. So it is both our satellites and our undersea cables that are at risk when it comes to China and Russia.

They take out those systems, we have to make clear to them, you will pay a price, and then when they do it, we have to exact that cost. If we don't have credibility, deterrence doesn't work.

And that is one of the fundamental problems, is we don't talk about where our red lines are, we don't talk about what our capabilities are to respond, and then when the bad thing happens, we don't respond. So it is no surprise our adversaries aren't deterred, whether it is the cyber domain, whether it is undersea cables or it is counterspace. These are all vulnerabilities, and our adversaries have gotten too used to coming after us and not paying a price.

Mr. FULCHER. Mr. Chairman, I think I am going to wrap with that. I do have another question or two, but I am going to submit that.

Thank you, Mr. Jaffer, Mr. Stehlin, for your comments, for the entire panel for joining us today. Also, please note that some of us have dueling committees, and so if you got repeat questions, you understand why.

But, Mr. Chairman, with that, I yield back.

Mr. FRY. The gentleman yields.

The Chair now recognizes the gentlelady from New York, Ms. Clarke.

Ms. CLARKE. Thank you very much, Mr. Chairman.

Good afternoon, everyone. And I thank our panelists for their expertise this afternoon.

The security of our communications network is one of the utmost importance to America's national security and continued global economic leadership. Securing our critical infrastructure against cyber attacks has been a top priority of mine since entering Congress, and I am proud to have served as chair of the Cybersecurity and Infrastructure Protection Subcommittee of the Homeland Security Committee in previous Congresses, where I was able to pass legislation to stand up a national reporting infrastructure, the cyber attacks on critical infrastructure regime.

We have seen an uptick in cyber attacks in recent years fueled by advances in technology, including artificial intelligence. Further advances in consumer and commercial technologies alike have

helped spur innovation across industries, particularly within respect to the IoT devices, but also have the potential to create new vulnerabilities that must be addressed.

The very threat vectors which we now face require a serious, focused effort on the part of our Federal Government. And sadly, our current administration has not proven up to the task.

Last month's Executive order on cybersecurity preparedness will weaken our defenses at a time when we face more threats than ever by shifting the responsibility of defending critical infrastructure to State and local governments, which too often lack the funding and expertise to take on this role. This decision leaves schools, emergency service providers, local governments, and others at risk by shifting the burden of warding off attacks from hostile foreign actors onto their backs.

Additionally, this administration's inane, half-baked tariff policy will devastate supply chains and drive up the cost related to defending our communications infrastructure.

Further, securing communications infrastructure begins with practicing good personal cyber hygiene, something the current Defense Secretary and National Security Advisor seems almost willfully unaware of. Their reliance on unofficial and unsecure messaging apps risk the lives of American troops and warrants a serious bipartisan investigation. It is extremely unfortunate that the current administration has consistently sought to dismantle tools and programs meant to protect our critical infrastructure from cyber attacks while senior officials ignore laws and best practices.

We in Congress must, however, continue to our work to increase network and supply chain safety to allow consumers and businesses alike to make informed decisions impacting the security of our communications networks. Recent breaches have shown that vulnerabilities in communication networks stem not just from telecommunications infrastructure but also from compromised end devices and personal behavior.

To that end, the FCC under the Biden administration adopted a voluntary cybersecurity labeling program in March of last year so that approved devices would bear the U.S. Cyber Trust Mark to help consumers identify trustworthy and secure products in the IoT marketplace while encouraging manufacturers to meet higher standards in product development.

My question is to Ms. Galante, but other panelists may weigh in as well: How could the implementation and possible expansion of the Cyber Trust Mark program help address the risk our communication networks face?

Ms. GALANTE. Thank you, Congresswoman Clarke. The cybersecurity—the Cyber Trust Mark, cybersecurity mark on Internet of Things-connected devices, is an important step in getting a baseline so consumers know what products are secure. It is similar to the UL, that Underwriter Laboratory metallic sticker that we all have on our different appliances. And I hope that Cyber Trust Mark goes the same way, which is to give consumers confidence that the company behind that product is following basic rules in cybersecurity that will make that product safer for their own personal use, and also so that they have some reliability that it is going to be patched and updated over time.

Ms. CLARKE. Very well. Anyone else want to add?

Mr. Stehlin, uh-huh.

Mr. STEHLIN. Yes. TIA is very close to the Cyber Trust Mark and has been involved with the FCC from its beginning. We hope that it gets rolled out later this year. There's a lot of steps forward. Right now it is focusing on smart consumer devices and does not include things like home routers. We think it needs to.

Ms. CLARKE. Yes, very well.

Well, listen, my time is up. I thank you all so much for adding your expertise to this very important conversation.

And with that, Mr. Chairman, I yield back.

Mr. FRY. The gentlelady yields.

Mr. FULCHER. Mr. Chairman?

Mr. FRY. Yes, sir.

Mr. FULCHER. Thank you, Mr. Chairman. At the request of my colleague, Mr. Pfluger, I would like to request the committee's permission to enter into the record a letter to the Honorable Brendan Carr, Chairman of the FCC, from a number of us on this committee. It has to do with recommendations on network and cybersecurity. So with the permission of the committee, I would like to submit that into the record.

Mr. FRY. Without objection.

[The information appears at the conclusion of the hearing.]

Mr. FULCHER. Thank you.

Mr. FRY. The Chair now recognizes the gentleman from New Jersey, Mr. Kean.

Mr. KEAN. Thank you, Mr. Chairman.

And thank you to our witnesses for being here today.

As a member of this committee and the Foreign Affairs Committee, I have a strong interest in identifying and advancing commonsense measures that strengthen our communications infrastructure and counter the threats posed by adversaries like China, Russia, and Iran.

Mr. Stehlin, first of all, welcome south. I am happy to have a resident of New Jersey's Seventh Congressional District here, and I am glad you are here to share your expertise. I understand the Team Telecom process can be burdensome and cause delays. What are the obstacles that burden or delay deployment of additional undersea cables?

Mr. STEHLIN. Thank you, sir, for that question. And I have been a longtime resident of East Amwell in the Seventh District, 32 years in the same house.

So NTIA should be the lead in Team Telecom. They are the President's advisor for all telecom issues. Absolutely, the DOJ, Department of Defense, Department of State, DHS ought to be involved as well.

But looking at it from the perspective of how we improve our telecom systems ought to be the first and lead of any type of evaluation, so that type of change would improve the permitting duration. Today it averages over 400 days, some cases as long as 900 days to get a permit, and often before it even gets to the FCC for the final approval. So this long, drawn-out process occurs before the FCC even sees the application. By fundamentally changing that and looking at it from the perspective of how can we improve our

economy rather than a Justice Department that maybe has a different perspective on things, I think that would go a long way to improving it.

Mr. KEAN. OK. And what steps can we take to keep the U.S. as an attractive place for vendors and suppliers across communications technology sector to do business, create jobs, and innovate here in the United States?

Mr. STEHLIN. We ought to reward trust, reward investment, and we ought to point out with a big spotlight those that are not trusted and encourage both the United States and our friends around the world to not buy from folks that are not trusted.

Mr. KEAN. Yes. Thank you.

Mr. Stroup, I agree that it is important to maintain leadership within international standard-setting bodies. In your view, what should American leadership and investment in these international bodies look like to best counter China's efforts to advance its own agenda, particularly in the satellite industry?

Mr. STROUP. Thank you for the question. I think one of the first opportunities is relating to WRC–27, making sure that the United States has positions that are supportive of the satellite industry and that they advocate them with their international counterparts at WRC–27. If there is a void, China most definitely will step in. The same is true with respect to other standard-setting opportunities. If we are not participants, China will definitely take advantage of the opportunity.

Mr. KEAN. OK. And can you talk about the weather satellites could play a role potentially as a redundancy in the event or failure of or attack on undersea cables?

Mr. STROUP. Yes, absolutely. So I gave as an example previously, the government of Taiwan is making arrangements with multiple satellite operators, bringing in the terminals. So should there be a cut, there is an immediate transition to satellite capability. So the good—you know, the benefit of the satellite capabilities are our infrastructure is in the sky, so they are not subject to something like a cable cut.

Mr. KEAN. Thank you.

And, Mr. Stehlin, I appreciate your discussion of strong supply chain security. What are the safeguards against, hypothetically, a previously trusted supplier or vendor suddenly being compromised by an adversarial actor? In other words, how can we make sure that trusted suppliers stay trusted?

Mr. STEHLIN. Continuous verification of trust, so having a certification program that a company has to go through on a regular basis to ensure that the processes they are using are trusted and ensure that the company itself doesn't have injunctions against it since the last time it got certified. Those types of things are really important.

Mr. KEAN. OK. Thank you all for your testimony, and I yield back.

Mr. FRY. The gentleman yields.

The Chair now recognizes the gentlelady from Virginia, Ms. McClellan. Perfect timing.

Ms. MCCLELLAN. Thank you, Mr. Chairman and Ranking Member Matsui, and I apologize for my timing. But given the increased

number of cybersecurity threats threatening our critical infrastructure, this hearing is incredibly important. And the irony of this hearing is not lost on me, that while we scramble to catch up in the increasingly intense cybersecurity arms race, some of my colleagues ignore that one of our Nation's biggest cybersecurity vulnerabilities is the current administration and its drastic cuts to the Cybersecurity and Infrastructure Security Agency, a national security team that prefers to coordinate via unsecure messaging apps instead of following standard security protocols.

And it seems that the biggest step that we could take towards safeguarding our critical telecoms infrastructure is to hold the administration accountable for reckless behavior and unwarranted funding cuts that have made us more vulnerable.

I want to start with Ms. Galante. Can you expand on what you mentioned in your testimony regarding the availability of AI to improve data processing capabilities to allow even unsophisticated adversaries to more effectively extract key insights from stolen data and how worried we should be that AI will also greatly expand the ability of adversaries to get around our cyber defenses and commit even more devastating cyber attacks?

Ms. GALANTE. Thank you, Congresswoman McClellan. AI is a double-edged sword. You can use it for security purposes, you can use it for data exploitation and a whole myriad of other things. Specifically when it relates to how our adversaries are able to advance their skill set quickly, when it comes to the exfiltration and the capture of large data sets, this is an area where we really need to focus on what the counterintelligence gain can be to them and what the vulnerability is to us.

When you are able to sweep up huge amounts of data, whether it is from a telecoms network or another source, and then aggregate those data points, you get valuable patterns of life, you get valuable data sets and insights that can be used against us. It is critical that we understand how our adversaries use this.

Ms. MCCLELLAN. Thank you for that.

And also for you, Ms. Galante, given the growing cooperation that we have witnessed between Russia, Iran, China, and the DPRK in kinetic warfare against Ukraine, to the extent possible, in an unclassified setting, can you elaborate on how concerned we should be about the possibility of greater cooperation among our adversaries to engage in cyber attacks against us and to what extent do you believe that type of cooperation has already begun?

Ms. GALANTE. I am particularly concerned about the sharing, especially of vulnerabilities, in widely used software in the U.S. that our adversaries could share between each other. China, for example, has national laws that require that vulnerabilities found by Chinese researchers or Chinese citizens are first given to the government. That is really important.

That, in a way, gives them, the Chinese Government, an advantage on the zero days, the unexploited vulnerabilities, that are typically at the core of many of the products or a potential vulnerability in many of our products and critical infrastructure across the U.S. If those are shared broadly, this becomes an avenue for a scaled attack against the U.S.

Ms. MCCLELLAN. And how should the United States be preparing itself for both the potential of AI-enhanced cyber attacks on critical infrastructure and the possibility of more coordinated cyber attacks amongst multiple hostile foreign adversaries?

Ms. GALANTE. We have to continue to invest in the ecosystem of security industry researchers, in intelligence operatives with our U.S. intelligence and law enforcement, national security agencies, who together put together the picture of what our adversaries are doing next, and the next edge of attacks that are going to be hitting us. It is that combination that is going to keep us ahead of the threat.

Ms. MCCLELLAN. Thank you, and I yield back.

Mr. FRY. The gentlelady yields.

The Chair now recognizes himself for 5 minutes.

The systems that connect us, our networks, our satellites, cables, towers, and data centers, form the invisible architecture of 21st century life. Safeguarding that infrastructure, as you have all talked about, is not just a matter of technology, it is a matter of strategy, security, and sovereignty. The demand for our networks has exploded. Obviously, every year more devices connect to U.S. networks, more data flows, and more critical services depend on uninterrupted and secure access.

Our systems are under strain not only from increased usage, but geopolitical risks, supply chain disruptions, and escalating cyber threats, particularly from nation states like China, as you have talked about. This isn't only about protecting websites or cell towers, it is about protecting hospitals from ransomware, grid systems from blackouts, and first responders from dropped phone calls.

Telecommunications is infrastructure. It is also national defense, and it is economic security. So let's treat it like that. It is a national priority.

Mr. Stroup, you mentioned rapid expansion and innovation of the satellite industry. Can you elaborate on the most transformative advances that we have seen in maybe the last 5 to 10 years and what they would mean for our national infrastructure?

Mr. STROUP. Thank you for the question. I believe that it starts with reusable launch capability. We have much more rapid launch than ever before. That has allowed many more companies to be able to launch their systems into space. I think, in addition, in terms of capabilities, the utilization of high-throughput-capacity capabilities has allowed expansion for broadband services.

So in terms of services, that is something that I would emphasize. The rapid growth of satellite broadband is really dependent upon that.

In addition, within respect to the remote sensing sector of the industry, the ability to manufacture and launch sensors into space has opened up a completely new industry.

So I would say, those are just some of the points that I would emphasize. And then we have also seen within manufacturing utilization of mass manufacturing techniques just given the increase in the number of satellites that are being manufactured, changing from bespoke manufacturing of large, bus-size satellites to hundreds or thousands of satellites being launched into space each year.

Mr. FRY. Can you point to—and I know we have talked about this broadly, some of the other witnesses—but specific policies that put your industry at a competitive disadvantage compared to, say, foreign competitors?

Mr. STROUP. Yes, certainly. I think that the ease of licensing within the United States is extremely important, and we have made a number of recommendations to the FCC, and we also work with NOAA on remote sensing to be able to streamline the licensing process. We have seen, fortunately, a great deal of investment that has been made in the industry.

But certainly, we don't want to push any of the licensing opportunities offshore, because that is something that I hear about from our members. In the past, it has taken a long time to be able to get a license approved.

I will note that in the last few years, we saw the creation of the Space Bureau with the FCC. At the time, there were 64,000 pending applications, and that has gone a great way to be able to address that. But that has been one of the key points that I have heard from our members, is being able to get a license quickly.

Mr. FRY. Thank you for that.

Mr. Stehlin, you have talked about how vulnerable the U.S. telecom supply chain is today to foreign interference and dependency. What specific areas concern you the most?

Mr. STEHLIN. Specifically, the lack of strategic investment in the United States in the ICT space. We have to pull back as much as possible the development of semiconductors in that entire ecosystem around semiconductor development. That is number one.

Number two, the lack of overall R&D investment. We have to encourage companies, incentivize them to spend more money on R&D, and we can do that through tax credits.

Mr. FRY. So reauthorizing that critical——

Mr. STEHLIN. Absolutely.

Mr. FRY. OK. What key technical or architectural decisions must we make now to ensure that our networks can withstand cyber attacks or disruptions?

Mr. STEHLIN. We need to speak in one voice. Right now, ISPs each have their own methodology for managing cybersecurity and supply chain security. The Government has multiple ways of managing that, so we need to speak in one voice, which will allow us to react more quickly, to evaluate performance more quickly, and to continuously improve. We have to have a defense in depth, and speaking in one voice certainly helps.

Mr. FRY. Thank you for that.

Mr. Jaffer, you talked about our allies. This actually intrigued me a little bit. I assume that our allies are aware of the risks of buying this material from Communist China, and so if they are aware of that, what is causing them to continue to perpetuate the problem?

Mr. JAFFER. It is a great question. I mean, two things: One, you know, our allies—take Europe, for example, they have known long about their addiction to Russian gas and how that caused them problems, and yet, they continue to buy it and buy it. We tried to build them a pipeline back in the Bush administration. They

wouldn't do it. They built a pipeline to Russia instead. They are building a second one now. It makes no sense.

They have the same attitude towards China. You look at the—even the United Kingdom, our closest partner, special relationship, British telecom built Huawei routers into their core networks. And when we went to them and told them this is a real problem, it took us a while to convince them. It took us a while to go around the globe.

The first Trump administration spent lots of hours and days and months and weeks convincing our allies around the globe that this was a real threat. And that was only a decade after the House Intelligence Committee wrote a report about the threat from Huawei and ZTE.

So we have known about this problem. We have been telling our friends and allies. And then, of course, we have had to pay Rip-and-Replace to take it out of our State and local networks as well.

There is a coming threat, though: DJI drones being used by State and local law enforcement, crazy for Americans to be buying that. We should not allow that to happen. It is a huge mistake for American law enforcement to have those drones in their networks.

Mr. FRY. Thank you for that. I see my time has expired.

The Chair now recognizes the gentleman from California, Mr. Obernolte.

Mr. OBERNOLTE. Thank you very much, Mr. Chairman.

And thanks to our witnesses. This has been a really important, really interesting hearing.

Ms. Galante, I would like to start with you if I could. I found your testimony very interesting, and particularly the ways that foreign intelligence services are using security vulnerabilities at telcos to gather information on U.S. infrastructure and building the capacity to disrupt that infrastructure. I am wondering about your thoughts about to what level that constitutes more than just an unfriendly act.

You know, we have kind of an informal understanding that intelligence gathering is something that all countries do, but building the capability to disrupt our infrastructure I think maybe goes beyond that.

And, I mean, for example, if a foreign country did something that was overt, like came into—on U.S. territory, kidnapped American citizens, and took them back to Iran or China, for example, I mean, obviously, that would be tantamount to an act of war. That has started wars.

Do we need to reprioritize our international reaction to acts like this?

Ms. GALANTE. Thanks for the question, Mr. Obernolte. One of the key distinctions that made this more than a sort of standard act of espionage, if you can think of it that way, is the level of access that these actors had within the telco networks. And with telco networks especially, you can almost think of it as sort a multipronged tool. You are able to disrupt traffic. You would be able to take almost kineticlike steps in a network because of the types of tech that are there that would cause an effect that everyone would agree is far beyond espionage.

That hasn't happened yet, as far as we know in these cases. It has just been an intelligence-gathering effort, and the access that these actors had presented additional opportunities. So that might be an area where you can really drive a distinction between what is traditionally known as espionage and what is largely considered prepositioning for an attack.

Mr. OBERNOLTE. Right. I think you have illustrated the key distinction there. I mean, there is information gathering, which is what espionage is geared towards, but then building a destructive capability is something I think might go beyond that. And if someone did something overt, like kidnapping U.S. citizens, we would say that is not all right, that is not OK. We would take a stand. I am wondering if maybe as an international community we need to set new norms about that behavior.

Ms. GALANTE. And I think the discussion has to happen with our allies, right. This is not just a U.S. problem, that Chinese access into telcos. We need to look at countries and allies in Southeast Asia. We also need to look at some of our European friends who have been dealing with this as well. This is not just a U.S. problem, and we need to come together to be able to show where the real lines are here that we are not willing to tolerate.

Mr. OBERNOLTE. Right. Thank you.

Mr. Stehlin, you highlighted the vulnerability of some of our subsea cables, which I was very appreciative of because a lot of people don't realize that vulnerability. Could you talk a little bit about what the backup might be to that, and how do we protect against that vulnerability? Because the problem is, we are uniquely vulnerable in that way, and I just don't see an easy way around that.

Mr. STEHLIN. There is no easy way around it other than having more cables and more landing points and quicker responses because of the volume of bandwidth, volume of traffic that goes across these cables. So that is really important, but we also need to be more on the offense, and as was described earlier, we need to tell our adversaries, "Don't do this. There will be a significant action on our part if you continue to conduct nefarious acts."

Mr. OBERNOLTE. Right. Well, I am hopeful that we can also do some modeling about how much of that international traffic would be debilitating, because it would be—you never know how debilitating it is going to be until it happens. But if you have done some modeling and you have done some exercises, you can kind of predict some of those failures.

Mr. STEHLIN. To build on that, the Houthis took out some cables in the Red Sea last year, and between Asia and Africa more than 50 percent of the traffic went down.

Mr. OBERNOLTE. Right.

Mr. Stroup, with my remaining 47 seconds here, I appreciate your testimony. One of the things that you didn't mention when you are talking about disaster modeling is the really innovative way that satellites are being used for early detection of wildfires. That is critically important in my district. If we can put these fires out with fast aerial resources before we need boots on the ground, it could be a total game changer. Could you give us a quick update on how that is going?

Mr. STROUP. Yes. I have actually seen a company just announce that they are providing as a service. A couple years ago, when I had the pleasure of testifying, you had asked a question about that capability, and I identified a manufacturer of that capability, and in the last 2 years we have seen companies moving forward with offering that as a service.

Mr. OBERNOLTE. Right. Well, m have, as you know, pilot programs, including some legislation that I offered to build out that capability, because I am absolutely convinced it is going to be a game changer for us in the West.

Well, thank you very much for your testimony. I see I am out of time.

Mr. Chairman, I yield back.

Mr. FRY. The gentleman yields.

And the purpose of this hearing now being concluded, I want to thank the witnesses for being here. I appreciate the professionalism, the expertise. I appreciate your testimony.

And we are adjourned.

This is a reminder, I remind all Members that they have 10 business days to submit questions for the record. And I ask the witnesses to respond to the questions promptly. Members should submit their questions by the close of business on Wednesday, May 14.

This hearing is adjourned.

I also ask unanimous consent to enter into the record the documents included on the staff hearing document list.

Without objection, that will be included.

[The information appears at the conclusion of the hearing.]

[Whereupon, at 12:44 p.m., the subcommittee was adjourned.]

[Material submitted for inclusion in the record follows:]

Documents for the Record – 04.30.25

1. A letter from Graphiant to Committee on Energy and Commerce leadership.
2. A March 24, 2025, statement entitled, “China Unveils Game-Changing Weapon That Could Decide Future Wars.”
3. An April 30, 2025, letter from Members of Congress to FCC Chairman Brendan Carr.

graphiant

The Honorable Richard Hudson
Chairman
Subcommittee on Communications and Technology
House Committee on Energy and Commerce
2112 Rayburn House Office Building
Washington, D.C. 20515

The Honorable Doris Matsui
Ranking Member
Subcommittee on Communications and Technology
House Committee on Energy and Commerce
2206 Rayburn House Office Building
Washington, D.C. 20515

The Honorable Brett Guthrie
Chairman
House Committee on Energy and Commerce
2161 Rayburn House Office Building
Washington, D.C. 20515

The Honorable Frank Pallone, Jr.
Ranking Member
House Committee on Energy and Commerce
2107 Rayburn House Office Building
Washington, D.C. 20515

Dear Chairman Hudson and Ranking Member Matsui,

Thank you for holding today's hearing, *Global Networks at Risk: Securing the Future of Telecommunications Infrastructure.* Below, find my statement for the record.

Sincerely,

Ali Shaikh
Chief Product Officer
Graphiant

The Problem

In 2025, the United States continues to face the two-fold problem of cyber security risks: threats to our national security and threats to our business landscape. Data is the lifeblood of innovation as well as the means to attack the nation. Inappropriate use of applications with sensitive data can be exploited, foreign adversaries can get into our critical infrastructure and take advantage of unclosed weaknesses, and we will have no means of enforcing compliance and audit if we do not upgrade our critical infrastructure.

A Solution

These are solvable problems; US companies have a range of solutions to meet the needs of our government and our citizens. It is of the highest importance that we advocate for the accelerated deployment of key capabilities that give us the abilities to ensure compliance and audit for our

regulators and oversight bodies, protect our national interests from threats, and deliver a better infrastructure for individuals and businesses to have better trust.

The best analogy to describe what we should expect as an outcome is that like we use services like Google Maps and Apple Maps that in real-time allow us to see where we are on the planet, and even allow us to see our loved ones travel safely, we should expect real-time ability to see what is happening to our data. We should expect from our infrastructure to tell us where is our data, where it's going and did it safely go from point A to point B without breaking any laws or being stolen.

Key Capabilities

1. Real-Time Oversight: Provide continuous monitoring of network traffic, allowing teams to detect and respond to threats promptly.

2. Advanced Profiling: Utilize sophisticated techniques, identify and categorize data flows, ensuring that sensitive information is handled appropriately.

3. Data Sovereignty: Ensure that data remains within approved geographic boundaries is crucial for compliance with data sovereignty laws.

About Graphiant

Graphiant is a US company that focuses on providing Data Assurance. These are services designed to provide comprehensive visibility, control, and compliance. Graphiant offers visibility into network traffic, enabling real-time monitoring and management. Graphiant employs advanced profiling methods and real-time telemetry to ensure that data is secure, efficient, and compliant.

Conclusion

Graphiant offers comprehensive solutions for modern networking challenges to deliver Data Assurance. By providing real-time visibility, advanced profiling, and compliance management, Graphiant empowers the United States to mitigate risks, enhance performance, and maintain control over their networks. These critical capabilities are essential for dealing with dynamic threats, increasing data complexity, and meeting regulatory requirements to fix our national security crisis.

China Unveils Game-Changing Weapon That Could Decide Future Wars

Published Mar 24, 2025 at 11:31 AM EDT Updated Mar 24, 2025 at 9:10 PM EDT

https://www.newsweek.com/china-unveils-game-changing-weapon-that-could-decide-future-wars-2049477

China has developed a device capable of cutting reinforced undersea cables thousands of feet below the ocean's surface.

The innovation comes amid concerns that Chinese vessels are targeting subsea infrastructure—threatening not only civilian but also military communications during a crisis.

Newsweek reached out to the Chinese embassy in Washington, D.C. with an emailed request for comment.

Why It Matters

Since early 2024, Chinese ships have been implicated in several cases of suspected cable sabotage, including in the Baltic Sea and around Taiwan, the self-ruled island claimed by China. The vessels were discovered to be in the area when the damage occurred, with investigators citing evidence such as anchor dragging as a likely cause.

Meanwhile, China has seen a rise in patent filings for tools designed to cheaply and efficiently sever submarine cables—vital infrastructure that carries more than 95 percent of global communications.

What To Know

The new invention was designed by the China Ship Scientific Research Center and its partner, the state-owned Laboratory of Deep-Sea Manned Vehicles, the *South China Morning Post* reported Saturday.

It can reportedly slice cables at depths of up to 4,000 meters (13,123 feet)—twice as deep as the deepest underwater cables currently in use.

The tool was first made public last month in the Chinese-language journal *Mechanical Engineer*.

The report marks the first time this capability has been unveiled by any country, despite its stated purpose of enabling civilian salvage and mining operations on the ocean floor.

Developed specifically for deployment on submersible vehicles such as the *Fendouzhe* and *Haidou-1*, the device's titanium alloy covering and specialized seals can withstand the intense pressures of that depth for long periods, *Interesting Engineering* cited the authors as saying.

A grinding wheel covered in diamond edges, spinning at a rapid 1,600 revolutions per minute, gives the device the ability to make short work of the protective steel layer encasing a cable.

he device has put China watchers on alert over its potential for more aggressive use, as well as the Chinese government's legal ability to compel cooperation from private companies—raising fears about the disruption of U.S. military communications across the network of Pacific bases including Guam, *SCMP* wrote.

What's Been Said

Bonnie Glaser, the managing director of the U.S. Indo-Pacific Program's German Marshall Fund, wrote on X, formerly Twitter: "Beijing insists it isn't responsible for cutting undersea cables. So why did it just unveil a powerful deep-sea cable cutter that can sever lines at depths of up to 4,000 meters?"

Theresa Fallon, founder and director of the Centre for Russia Europe Asia Studies in Brussels, wrote on X: "Beijing's underwater deep-sea, cable-cutting device makes explanations of 'it was just an accident' far harder to swallow."

Chinese embassy spokesperson Liu Pengyu told *Newsweek*: "We oppose unfounded attacks and smears against China. This tool, developed by China independently, is used in marine scientific research. The U.S. and some European countries also have similar technology. China attaches great importance to protecting undersea infrastructure and has been and will continue to work with the international community to protect undersea cables."

What's Next?

Investigations into suspected Chinese cable sabotage are ongoing, including a recent incident involving a Chinese-crewed vessel sailing under a Togo flag of convenience.

The ship was detained by Taiwanese authorities in February near where a cable linking Taiwan's main island with outlying Penghu County had been damaged.

Update 3/25/25, 1:10 p.m. ET: This article has been updated with a comment from the Chinese embassy.

Congress of the United States
House of Representatives
Washington, DC 20515–4311

April 30, 2025

The Honorable Brendan Carr
Chairman
Federal Communications Commission
45 L Street NE
Washington, D.C. 20554

Dear Chairman Carr:

Firstly, we write to commend your decision to establish the new Council for National Security within the Federal Communications Commission (FCC), a crucial step in safeguarding America's telecommunications infrastructure. Congress stands ready to work with you on this initiative to reduce America's dependence on foreign adversaries, mitigate cyberattack vulnerabilities, and ensure U.S. supremacy in critical technologies.

As you know, the House Energy and Commerce Committee has worked diligently to combat the People's Republic of China's (PRC) efforts to leverage private companies to create backdoors in our telecommunications infrastructure. For example, the House of Representatives just recently passed H.R. 866, the ROUTERS Act, to safeguard Americans' communications networks from foreign-adversary controlled technology, including routers, modems, or devices that combine both. Additionally, in the 118th Congress, the House passed H.R. 7521, the Protecting Americans from Foreign Adversary Controlled Applications Act, which prevents foreign adversary-controlled applications from targeting, surveilling, and manipulating Americans through online applications like TikTok. Congress also worked to ensure that the Secure and Trusted Communications Networks Reimbursement Program, or the "Rip and Replace" program, received proper funding to remove untrusted equipment such as Huawei and ZTE from our networks.

Last year, the House Committee on Homeland Security and the Select Committee on the Chinese Communist Party released their Joint Investigation report into Shanghai Zhenhua Heavy Industries Company (ZPMC), a PRC-owned and operated company. The investigation yielded that ZPMC, or a third-party company contracted with ZPMC, installed cellular modems onto STS cranes currently operational at U.S. ports. These installations fall outside the scope of any contract between the affected U.S. ports and ZPMC. The modems created an obscure method to

collect information and bypass firewalls in a manner that could potentially disrupt port operations.[1]

Even more recently, the U.S. Cybersecurity and Infrastructure Security Agency (CISA) reported that the Chinese-made Contec CMS8000 patient monitors contained a hard-coded IP address linked to an unidentified third party, allowing for reverse backdoor functionality.[2] This vulnerability allows for remote access of the medical device and may allow for potential manipulation, risking patient safety and compromising sensitive health data.

These are just a few examples of how the CCP will use every tool at its disposal to undermine U.S. economic and national security interests to further its agenda. The recent proliferation of cybersecurity incidents underscores the need for the entire federal government to work together to address and deter cyber threats. We write to you today because we believe there is more the FCC can do to reduce the likelihood of such incidents.

As the backbone of the Internet, routers play a critical role in securing communications for consumers and businesses. When these devices are insecure, they can serve as gateways for cyberattacks. For example, weak, default, or easily predicted passwords make routers vulnerable to exploitation. Malicious actors can exploit these vulnerabilities in routers to disrupt service, steal sensitive data, or even launch attacks against critical infrastructure.

It has been reported that TP-Link, a Chinese company, owns roughly 65% of the routers used in U.S. homes and small businesses. Additionally, the Department of Defense and other federal government agencies have used TP-Link Routers before.[3] Multiple TP-Link routers have been added as to the National Institute of Science (NIST) National Vulnerability Database for containing a directory traversal vulnerability, allowing unauthenticated remote attackers to access sensitive files by sending specially crafted requests.[4]

We are increasingly concerned about the prevalence of these devices and that unsecure routers may allow the CCP to surveil American data or disrupt our networks. Although the Department of Commerce is reviewing whether or not to ban routers made by Chinese-owned companies in

---

[1] U.S. House of Representatives Committee on Homeland Security, Subcommittee on Transportation and Maritime Security and U.S. House of Representatives Select Committee on the Strategic Competition Between the United States and the Chinese Communist Party. *Handling Our Cargo: How the People's Republic of China Invests Strategically in the U.S. Maritime Industry*. Washington: Select Committee on the CCP, 12 September 2024. https://selectcommitteeontheccp.house.gov/sites/evo-subsites/selectcommitteeontheccp.house.gov/files/evo-media-document/Joint%20Homeland-China%20Select%20Port%20Security%20Report-compressed.pdf

[2] U.S. Department of Homeland Security, Cybersecurity and Infrastructure Security Agency. *Contec CMS8000 Contains a Backdoor*, 30 January 2025. https://www.cisa.gov/sites/default/files/2025-01/fact-sheet-contec-cms8000-contains-a-backdoor-508c.pdf

[3] Somerville, Heather, et al. "U.S. Weighs Ban on Chinese-Made Router in Millions of American Homes." Wall Street Journal, 24 Dec. 2024. https://www.wsj.com/politics/national-security/us-ban-china-router-tp-link-systems-7d7507e6

[4] U.S. Department of Commerce, National Institute for Standards and Technology. "CVE-2015-3035 Detail." *National Vulnerability Database*, 21 April 2015. https://nvd.nist.gov/vuln/detail/CVE-2015-3035

the future, many of these devices remain on our networks, which nefarious actors could still leverage.

With the new Council for National Security, the FCC can take various actions to mitigate cybersecurity risks associated with unsecure routers. The FCC could leverage equipment authorization through the Telecommunications Certification Body to require routers to allow only uniquely identifiable devices known to the household and securely authenticated by the network owner onto a customer's network. These steps represent broadly accepted minimum security practices under NIST guidance and are necessary first steps toward protecting our nation's consumers and networks from cyber risks. Other immediate-term options, such as prohibiting any new sales of TP-Link routers, or requiring ISPs to block new TP-Link routers from being added to home networks, would stop the influx of these devices on networks. Additionally, as we think beyond TP-Link routers, ISP authentication will strengthen U.S. networks' ability to defend themselves against future untrusted Internet of Things (IoT) devices joining their networks.

We are confident that, under your leadership, we can advance national cybersecurity initiatives and create robust strategies to strengthen U.S. networks against cybersecurity threats. Together, we can foster a secure digital environment that instills trust and confidence among users nationwide.

Sincerely,

August Pfluger
Member of Congress

Robert E. Latta
Member of Congress

Earl L. "Buddy" Carter
Member of Congress

Jay Obernolte
Member of Congress

Nathaniel Moran
Member of Congress

Russ Fulcher
Member of Congress

Gus M. Bilirakis
Member of Congress

Nicholas A. Langworthy
Member of Congress

Troy Balderson
Member of Congress

Erin Houchin
Member of Congress

Telecommunications Industry Association
1201 Wilson Boulevard, Floor 25
Arlington, VA 22209 | www.tiaonline.org

TIA Responses to Additional Questions for the Record
from David Stehlin, Chief Executive Officer

The Honorable August Pfluger

Last year, I introduced the "Undersea Cable Security and Protection Act" to establish an interagency working group to bolster undersea cables' security, resiliency, and integrity.
It is estimated that 95-99% of the entire world's data travels via subsea cables, and cable cuts have become a common tactic by Russia, China, and Iran's terrorist proxy groups to disrupt communications.

1. ***Mr. Stehlin, please briefly expand upon why protecting subsea cables is important to consumers and the telecommunications industry, as well as why it is within the national security interests of the United States to protect them.***

Response: Subsea cables enable fast, reliable communication for consumers and businesses and supports critical functions key to both the economic and national security of the U.S. The U.S. depends on these cables for efficient data transmission, and any disruption can lead to significant service outages, financial losses, and damage to business operations, particularly for data-heavy industries like finance, cloud computing, and e-commerce.

Subsea cable security is part of broader global infrastructure resilience. Foreign adversaries tampering with these systems could destabilize communications and economic systems, posing serious national security threats. Protecting them ensures the stability of global infrastructure, cross border data flows, and supports both economic and security interests.

I would equate the importance of subsea cable systems to the importance of commercial vessels travelling the seas to carry goods from port to port. As I said in my testimony before the subcommittee, 99% of cross continental internet traffic is carried through these subsea cables. As advanced digital technologies continue to emerge, such as artificial intelligence (AI), xreality (XR), and the Internet of things, subsea cables will continue to become even more essential to the U.S. economy as they connect U.S. innovation to global markets.

I have concerns about the Team Telecom process causing delays in the cable landing deployment process. I worry that these delays in deployment are working against our national and economic security interests. My understanding is the review process has gone from taking 6-9 months under the first Trump Administration to now taking 2-3 years.

2. ***Can you explain the challenges within the Team Telecom review process? Do you believe there is sufficient representation of our economic security interests on Team Telecom?***

Response: The Team Telecom review process suffers chiefly from three challenges: redundancy, transparency, and predictability. A comprehensive subsea cable review begins anew each time a licensee applies, regardless of whether Team Telecom has already reviewed the applying entity. This redundant process often leads our members to submit the same information multiple times. The combination of redundancy and a lack of information sharing between Team Telecom agencies is unfortunately cumulative, requiring the same information to be submitted across multiple applications and then to multiple agencies. The Team Telecom risk assessment process is also opaque, with little economic input, and little insight into how the agencies measure threat, vulnerability and consequence. With little to no consistency over similarly situated projects, and limited regulatory predictability, there is a constant risk of stranded investment for applicants. This results in a process that is harmful for builds that can take decades to result in a return on investment. While the Team Telecom process is important for our national security, the resulting regulatory uncertainty that this process is creating may hamper innovation in a way that results in more harm than good

Telecommunications Industry Association
1201 Wilson Boulevard, Floor 25
Arlington, VA 22209 | www.tiaonline.org

as we begin to cede our subsea cable leadership to China.

When entities like the Departments of Commerce and State, the United States Trade Representative, and the White House Office of Science and Technology Policy are relegated to the role of "advisors" to Team Telecom instead of being "members" and actively part of the risk assessment and deliberative process, there is a lack of representation from those agencies responsible for protecting economic national security interests. That is why we believe that the Department of Commerce's National Telecommunications and Information Administration should play a leading role in running the Team Telecom process.

3. ***Mr. Stehlin, what is the cause of this increased timeline, and how does this delay impact the planning and laying of subsea cables? Given the limited number of manufacturers that make these cables and the few ships available for laying and servicing cables, are there also supply chain implications?***

Response: As mentioned above, the duplicative nature of the Team Telecom process often leads to multiple rounds of back and forth between an applicant and any of the Team Telecom agencies. This delay dramatically increases the costs of a subsea cable system. On top of delaying a realization of increased capacity and redundancy, each day the application is delayed pushes the return on investment period further into the future, while also introducing risks related to availability of ships, suppliers, weather, terrain, and permitting. Additionally, any purchased materials begin to depreciate and plan modification may be needed in order to successfully deploy the cable.

The Honorable Doris Matsui

1. ***Open RAN increases supply chain diversity – which has significant economic, network performance, and national security benefits.***

Mr. Stehlin, how can Open RAN and secure-by-design principles help our networks be more trusted and resilient?

Response: Open RAN and secure-by-design principles play a vital role by supporting supply chain diversity, increasing resilience, and encouraging innovation in the trusted nations' tech ecosystem. Although these principles raised in this question are possibly related, they are two distinct items. Open RAN's interoperable architecture potentially reduces dependency on foreign adversary controlled equipment manufacturers by creating a marketplace for interchangeable equipment made by trusted manufacturers. From a resilience standpoint, Open RAN potentially improves the ability of operators to integrate components from multiple suppliers, avoiding single points of failure and enabling quicker recovery from disruptions, assuming that the systems integration is successful. But like any network architecture, Open RAN solutions must be proven from a security perspective and need to be shown to meet secure-by-design principles.

The secure-by-design approach reinforces resiliency by ensuring that systems are built with layered defenses, limited attack surfaces, zero-trust, and robust monitoring from the outset. TIA strongly believes that security must be built into our networks, which is why we created SCS 9001, our supply chain security standard, to allow ICT industry to certify that their products and networks are built with a defense-in-depth approach to network technology. We feel SCS, and similar secure-by-design principles create a foundation for agile, trusted, and future-ready networks that are better equipped to serve national interests and protect against emerging threats. Security starts with the processes an organization uses to build a product or service.

2. ***California is a major landing site for undersea cables, which connect us to the rest of the world and are a part of a global system carrying 99 percent of international data traffic.***

Telecommunications Industry Association
1201 Wilson Boulevard, Floor 25
Arlington, VA 22209 | www.tiaonline.org

Mr. Stehlin, what role does redundancy play in both preventing and mitigating the effects of deliberate or accidental disruptions to our subsea cable networks?
Mr. Stehlin, your testimony indicates that regulatory delays have reduced cable redundancy. Could you explain how these constraints increase national vulnerability and what reforms might help improve resilience?

Response: As in any communications system, redundancy plays a critical role in both preventing service outages and mitigating the effects of disruptions. Subsea cables form the backbone of global internet connectivity. If one cable is damaged or cut, subsea cable redundancy enables traffic to be automatically rerouted with minimal downtime. By spreading traffic across a diverse set of cable routes, physical geographies, and landing points, networks become more resilient to localized incidents or targeted attacks. As capacity demands on cables increase due to an uptick in the use of advanced digital technologies, it is critical to have redundant cables to avoid bottlenecks and slowdowns and to quickly and efficiently reroute traffic destined for diverse global endpoints.

As industry is rushing to increase the redundancy of our subsea cable infrastructure, regulatory uncertainty and delays slow down and raise the cost of deployment. When the PEACE subsea cable system crossing through the Red Sea was cut it took approximately three weeks to get the cable back online. Even if the Federal Communications Commission ("FCC") were to grant an emergency license to deploy a subsea cable system, it would be too late for the system to act as a backup. We need to work quickly to deploy cables now, so we can increase our cable route diversity and minimize disruptions to essential global communications and data flows. This can be done with an expedited Team Telecom review for trusted vendors; increased cooperation and information sharing between Team Telecom, the FCC, and trusted providers; and standardized mitigation and security measures, providing much needed regulatory certainty.

The Honorable Robin Kelly

1. ***Mr. Stehlin, many of our global communications travel across subsea cables. To protect these cables and the data, we need to address both the physical security and the cybersecurity of these cables. Regarding cybersecurity, how do you suggest we protect the actual data traveling across these cables?***

Response: The Federal government has a variety of cybersecurity requirements across all sectors of industry. In developing cybersecurity requirements in this area, it is important to recognize that the responsibility of subsea cable operators should be limited to ensuring the resiliency of the physical infrastructure they operate. Ensuring the confidentiality and integrity of data in transit across the Internet is typically the responsibility of the data's ultimate owner and the communications service provider, which can be a different entity than the subsea cable owner. Ensuring the infrastructure owner does not have access to data flowing over the cables is critical for privacy and civil liberties purposes, and the majority of traffic flowing over cables is protected by end-to-end encryption. Additionally, each network element in the subsea cable system should be purchased from trusted suppliers.

In many cases, communications providers must already develop cybersecurity plans that align to the National Institute of Standards and Technology ("NIST") Cybersecurity Framework under other appropriate and complementary regulatory regimes. Adopting a cybersecurity plan that adheres to the NIST Framework ensures that service providers have the flexibility and agility necessary to respond to a highly dynamic cyber threat environment.

Jamil N. Jaffer, Founder and Executive Director, National Security Institute
George Mason University Scalia Law School

Attachment —Additional Questions for the Record

The Honorable Russ Fulcher

Mr. Jaffer, on the issue of undersea cables, we have seen repeated incidents to cut or damage undersea cables that disrupts service on communication, data for business and government, as well as power and energy flows. We all know the critical role undersea cables play – $10 Tri in finance and commerce; 99% of the world's data flowing through them – most of which impacts the U.S. Several European countries around the North Sea have signed an agreement to protect critical infrastructure, Baltic countries, Finland, and others have stepped up patrolling in the Baltic Sea, and NATO is now coordinating.

1. **What do you see as next steps we can take from this Committee to ensure data flows are not interrupted?**

Jaffer Response:

There are a number of immediate steps the United States might take to ensure data flows over critically important cable infrastructure are not interrupted, some of which this Committee might work others to help accomplish. First, in the near term, our adversaries need to know that, to the extent they are engaged in efforts to intentionally cut or otherwise damage undersea cables that are critical to our national and economic security, we and our allies will take action both to protect those cables and to impose costs upon those responsible for such interference.

This Committee could support efforts to protect such infrastructure by working with other committees to authorize federal programs, through the Department of Defense and other appropriate departments and agencies—and provide incentives or funding to private entities, whether undersea cable owners and operators, insurers, or other third parties—to protect those cables, make them more resilient to attacks, and have the resources available, including repair ships, supplies, and skilled personnel, to rapidly identify attacks and reconstitute these capability, including installing devices to detect such attacks as they are underway, as well as to respond to such attacks, when directed by the President.

Likewise, this Committee could work with other committees in Congress, as well as with the President, to impose direct costs on adversaries engaged in cable attacks including but not limited to sanctions and perhaps even more aggressive responses. Given the importance of these cables, for example, it would not be out of the realm of the possible for the United States to determine that an attack on a critical cable (or cables) are the equivalent of a physical attack on the United States itself and its critical infrastructure.

Members of this Committee could also, for example, encourage the President to publicly state our nation's policy on such cable attacks, including concretely and specifically describing our plans for responding to such attacks, and also could provide the funding, support, and authority necessary to permit the President to rapidly respond, should he or she choose to do so. For such a policy to have a real deterrent effect, however, our adversaries must assess that we are both able and willing to respond. This is because without real credibility, no amount of bluster about responses will actually deter our adversaries. That means if we threaten to respond when our redlines are crossed, and those redlines are in fact crossed, we must act and we must do so publicly. For far too long our adversaries have seen an America willing to talk a big game but unwilling to actually bring it. Such behavior—which has been a problem under Presidents of both parties for well over a dozen years—does not create fear in our adversaries nor the confidence in our allies needed to achieve effective deterrence.

Finally, in the longer term, this Committee could work with industry to ensure we have backup capacity and resilient capabilities—whether using undersea cables, alternate routes, dark fiber, or satellites, among other things, to handle critical communications and to ensure that we don't suffer—once again—from a major strategic surprise when it comes to these very important capabilities.

2. **Can we look at different routes? For example, Delegate Plaskett of the Virgin Islands and I have a bill[1] that studies whether we need a new undersea cable connection between U.S. territory and Africa.**

Jaffer Response:

Certainly, alternate cable routes are a key part of building a resilient cable infrastructure that can keep communications effectively flowing, notwithstanding either intentional and inadvertent efforts that result in a cut or damage to critical infrastructure cables. Specifically, such alternate routes can help ensure that communications between the United States and our allies (and trading partners) can robustly continue even in times of natural or man-made crises.

In this case, a study of alternate cable routes like the one you and Delegate Plaskett have proposed make good sense, particularly if such a study can be completed at a reasonable cost. It may be worthwhile, while undertaking such a study, for those who either have—or are able to develop—a real knowledge base (whether prior to or as part of such a study), to look at other critical cable routes as well, and assess whether other alternatives based on cost, necessity, availability, immediate usability, and the like, might be helpful for those cable routes as well.

Of course, additional cable routes alone are not a panacea for the challenge posed by our adversaries in this domain, for a variety of reasons, including cost and time to completion, and the ability to attack those routes as well. This is why other long-term measures, including strengthening our defensive capabilities and engaging in real deterrence are also critical. Nonetheless, evaluating and establishing alternate cable routes, where appropriate, are a critical part of ensuring the resilience of our communications infrastructure and must therefore be a key part of the discussion going forward.

The Honorable August Pfluger

Multiple TP-Link Routers have been added to the NIST National Vulnerability Database for hardcoded backdoors, allowing unauthenticated remote access.

1. **Mr. Jaffer, could unsecured routers with remote access backdoors pose a national security threat to the United States? Should Americans be concerned about the security of their personal data?**

Jaffer Response:

There is no question that unsecured routers with hardcoded remote access backdoors are a massive national security—and economic security—threat to our nation and its people. And there ought be no debate whatsoever that this threat should raise significant—and immediate concerns—amongst the American people. This is particularly true given the data-hungry nature and aggressive actions already taken by key American adversaries, like the People's Republic of China.

[1] https://www.congress.gov/bill/119th-congress/house-bill/1737?s=7&r=15.

The Chinese have been for over a decade—and continue today to be— engaged in a massive spree to acquire as much data on American citizens and our allies—not just government agencies, but ordinary Americans—and to steal as much intellectual property as they can from our private sector companies. Indeed, when it comes to our people, the Chinese are building massively powerful capabilities to acquire, store, and mine the data of Americans and our allies as they seek to spread their autocratic rule and influence around the globe. These capabilities, in part powered by new and rapidly evolving artificial intelligence capabilities, require massive amounts of data to make them highly performant. Likewise, the modern Chinese economy has largely been built upon the theft of American and allied intellectual property to the tune of trillions of dollars globally.

One very effective way to acquire both data on Americans and our allies—and to steal intellectual property at speed and scale—is to own and operate the infrastructure that our communications transit over. And, if you are able to successfully build hardcoded backdoors into that infrastructure, as the Chinese government has done at scale, you have essentially written you own path to success. These Chinese have not only done this with the home and business routers you reference, but also by putting its technologies and those of its largest most capable telecommunications companies, at the heart of western telecommunications networks.

Indeed, today, our communication networks and home and business facilities are intimately laced—often to their core—with Chinese capabilities and systems that, at a minimum, could be made inoperable in a crisis, and, at worst, could serve not only as highly capable intelligence collection platforms but vehicles for the delivery of cyber weapons as well.

We must root out these systems and deploy capabilities to defend against such attacks whether targeted at our government, our private sector companies, and our citizens, and those of our allies, and we must do so rapidly.

We have seen a disturbing trend in consumer electronics coming out of China, especially when it comes to critical infrastructure technology. From ZPMC modems installed on cranes at U.S. ports, Huawei and ZTE telecommunications equipment in U.S. networks, Contec CMS8000 patient monitors in hospitals, DJI drones in our skies, and so on.

2. **What should the United States' position be when it comes to trusting technology, especially for critical infrastructure, that comes out of China? Is there a way we could tackle this issue BEFORE this technology enters our country and creates a national security risk?**

Jaffer Response:

We should not trust technology that comes out of China for any mission-critical use case, including deployment into American or allied critical infrastructure. Nor should we tolerate its use by any government agencies, whether federal, state or local, nor key private sector companies and actors particularly in critical infrastructure or related sectors. And this should be true whether those technologies are being used for law enforcement or public safety uses (e.g., in the case of DJI drones) or more ostensibly mundane uses like monitoring crops or moving cargo.

The first and most obvious way to avoid the deployment of such technology is to build robust and resilient supply chains for such technology here at home and in allied countries. This Committee can help with this effort by incentivizing investors and innovators to identify these needs in this space—partnering with the U.S. government and industry—and to build those capabilities at home and in friendly countries. This means that we must raise up our technology companies—large and small alike—and ensure they remain the envy of the world, built by the free market and free from overregulation by federal, state, and allied governments.

If we fail to offer alternatives to low-cost, often slave-labor produced, stolen-IP developed goods, that are made with government subsidies in a command-and-control economy like China, then we will continue to face a significant national security—and economic—threats from these goods and their purveyors.

But building alternative capabilities isn't enough. We have to incentivize nations around the globe as well as governments and private companies and citizens here at home to buy these capabilities, rather than investing in the cheap Chinese knockoffs or technology that come with Chinese backdoors baked in from the jump. That is, we must ensure there is broad and deep adoption of allied technology versus that of the Chinese government and its wholly owned subsidiaries in the notional private sector.

And finally, we must harden these domestic and allied technologies—from the outset and during the entire lifecycle for which they are deployed—against attacks by our adversaries, and we must also be prepared to defend ourselves, our nation, its private sector companies, and our citizens, again all manner of adversaries, including China, in both the cyber and physical domain.

The U.S. needs to do more to strengthen its position in standard-setting bodies such as the ITU. Several GAO reports have outlined issues regarding the preparatory process for forming a consensus leading up to the World Radiocommunications Conference.

3. **What changes need to be made in the preparatory process between NTIA, FCC, and the State, leading up to CITEL and the WRC? What legislative fixes should be made to streamline this process, reach a consensus earlier, and maximize the U.S. ability to deter our adversaries using the ITU to the detriment of the United States' national and economic interests?**

Jaffer Response:

There is no question that the U.S. government needs to partner more tightly with the American private sector, as well as with key private actors and governments in allied nations to make sure we get our stories straight and speak with one voice.

All too often, the federal government, or individual representatives of the federal government, are internally divided on policy, and these internal divisions—even when authoritatively resolved by the White House—breakout into the open on the international stage. This ought not be tolerated by our government, not just the White House and the President, but by Congressional leaders and key committees as well.

And even when the federal government has its act together, all too often, private sector actors are a second thought—or at least are treated as such—even in sectors like telecommunications, where the private sector plays a central, if not lead, role in key areas.

These issues are often even more of a problem for our allies. First, they often believe themselves (sometimes accurately) to be playing second fiddle to the United States, and they often have a hard time corralling or effectively coordinating with their own private sector. Moreover, they often assess the threat from key adversaries—whether China, Russia, or Iran—quite differently than we do. One only need look at the long-term reliance of Europe on Russian gas or the willingness of our allies to continue to buy obviously problematic Chinese technology, to see the very real risks in play. As a result, the United States and allies sometimes find ourselves at odds in specific policy debates even where we agree on the outcomes we seek.

If we are to effectively prevent the organizations like the ITU from becoming China-dominated and from making the same mistakes we made with certain recent technology evolutions, we must get on the same page

here at home—public and private sector alike—and we must join forces closely with our allies, convincing them to come to our view, not simply acceding to theirs.

There is no doubt that legislation might help in this domain by requiring agencies to work better together, to work more effectively with industry and allies, and requiring agreed consensus before hitting the world stage. And supporting funding for such efforts could be valuable as well. However, at the end of the day, what is critical to achieve is a shared understanding of the threat, the methods for addressing it, and accepting the reality that every day we and our allies are divided—whether the public sector from private sector or between America and European or Asian nations—we make our adversaries' work that much easier.

Laura Galante
Principal, WestExec Advisors
Former Director, Cyber Threat Intelligence Integration Center
Office of the Director of National Intelligence

August 5, 2025

Noah Jackson
Legislative Clerk
Committee on Energy and Commerce
2125 Rayburn House Office Building
Washington, DC 20515

Dear Mr. Jackson:

Thank you for the opportunity to appear before the Subcommittee on Communications and Technology on Wednesday, April 30, 2025, to testify at the hearing entitled, "Global Networks at Risk: Securing the Future of Communications Infrastructure."

I am submitting the following answers below to Member questions submitted after my testimony.

Sincerely,

Laura Galante

Questions for the Record:

The Honorable Robin Kelly

1. Ms. Galante, Recent breaches have shown that vulnerabilities in our communications networks can stem not just from telecom infrastructure, but also from compromised end devices including IT hardware. How should Congress address the risk posed by companies controlled and owned by the People's Republic of China that make critical devices, such as computers, given their potential as threat vectors into critical communications systems?

There is significant and well-documented risk in incorporating PRC-manufactured devices in US telecommunication networks. In 2020 Congress passed the Secure and Trusted Communications

Networks Act which established the FCC-managed "covered list" of communications services and products that pose an unacceptable risk to national security. Numerous Chinese companies are included on the list including Huawei and ZTE.

Congress can take steps to strengthen the FCC's covered list work. This could include expanding the definition of 'risk' to include supply chain components, pursue accelerated removal timelines ("rip and replace") for covered list tech still in use and fully fund the program, and also coordinate with allies (i.e. EU, Japan, Australia) to develop shared covered lists that promote trusted network alliances to establish an ecosystem of trusted vendors in 5G/6G, edge, and critical infrastructure.

The Honorable Kathy Castor

1. *Ms. Galante, can you please elaborate for this committee what government-industry collaboration looked like in response to this attack? How is the government able to help companies identify Salt Typhoon activity into their networks, and what can we do to be more effective in the future?*

In response to the discovery of a multi-victim PRC-sponsored campaign against multiple US telcos, industry-government collaboration occurred primarily through law enforcement (FBI victim assistance and investigative support) and the sector risk management agency for the telecommunications sector–CISA (including the relevant ISAC). Intelligence agencies coordinated their support of these efforts primarily through the Unified Coordination Group which was established to respond to these breaches. Conducting a thorough review–such as the review process designed by the recently disbanded Cyber Safety Review Board–will identify a more effective intelligence sharing process between telecoms' security and intelligence teams and US government.

2. What vulnerabilities or gaps did Salt Typhoon's intrusion demonstrate to us regarding the US telecommunications structure?

The PRC-sponsored campaign against US telecoms highlighted the need for improved identity management practices in complex, critical networks. It also demonstrated the PRC's increasing willingness to target Americans' communications at both a personal level (for intelligence gathering purposes) and an ability to hold major parts of American telecommunications networks at risk for wider disruption.

3. What actions can we anticipate the PRC to be taking next to grow their own capabilities, and what should we be doing to combat this and enhance our national security?

The PRC's intelligence operations against US telecoms and the People's Liberation Army (PLA)'s deep access to US water, energy and transportation networks–both demonstrate President Xi's focus on developing digital leverage points against the US. We can expect this activity to continue as the PLA, Ministry of State Security and other PRC government entities seek options and intelligence that can have military, political, and economic consequences on US decision making.

4. Can you speak to what cybersecurity risks Elon Musk's so-called "efficiency" operations, specifically its unlawful access of personal data, have on our national security? What signal and opportunity does it present to adversaries like the CCP?

I do not have firsthand knowledge of these activities. As a general matter, PRC cyber actors closely follow the coverage of specific databases, systems, and vendors associated with government networks and will use any information they can gather to inform their reconnaissance efforts for future operations.

5. *What do these actions indicate to our allies? How will it impact our cybersecurity partnerships with them?*

As a general matter, our allies' cyber partnerships provide critical tactical and strategic intelligence about our common adversaries. Efforts that appear to undermine the information security or integrity of these relationships will undermine these partnerships and negatively impact US national security.

○