This is an unedited transcript. The statements within may be inaccurate, incomplete, or misattributed to the speaker.

Diversified Reporting Services, Inc.

RPTS CARR

HIF046160

SECURING COMMUNICATIONS NETWORKS FROM FOREIGN ADVERSARIES

THURSDAY, FEBRUARY 15, 2024

House of Representatives,

Subcommittee on Communications and Technology,

Committee on Energy and Commerce,

Washington, D.C.

The subcommittee met, pursuant to call, at 10:00 a.m. in Room 2123, Rayburn House Office Building, Hon. Bob Latta [Chairman of the Subcommittee] presiding.

Present: Representatives Latta, Bilirakis, Walberg, Carter, Dunn, Curtis, Joyce, Weber, Allen, Balderson, Fulcher, Pfluger, Harshbarger, Obernolte, Rodgers (ex officio); Matsui, Clarke, Soto, Eshoo, Cardenas, Craig,

This is an unedited transcript. The statements within may be inaccurate, incomplete, or misattributed to the speaker.

Fletcher, Dingell, Kelly, and Pallone (ex officio).

Also present: Representative Schakowsky.

Staff Present: Sarah Burke, Deputy Staff Director; Nick Crocker, Senior Advisor and Director of Coalitions; Slate Herman, Counsel, C&T; Tara Hupman, Chief Counsel; Noah Jackson, Clerk, C&T; Peter Kielty, General Counsel; Emily King, Member Services Director; Giulia Leganski, Professional Staff Member, C&T; John Lin, Senior Counsel, C&T; Kate O'Connor, Chief Counsel, C&T; Carla Rafael, Senior Staff Assistant; Hannah Anton, Minority Policy Analyst; Keegan Cardman, Minority Staff Assistant; Jennifer Epperson, Minority Chief Counsel, C&T; Waverly Gordon, Minority Deputy Staff Director and General Counsel; Tiffany Guarascio, Minority Staff Director; Dan Miller, Minority Professional Staff Member; Michael Scurato, Minority FCC Detailee; Andrew Souvall, Minority Director of Communications, Outreach, and Member Services; Johanna Thomas, Minority Counsel; and Jessica Zhao, Minority Intern.

*Mr. Latta. The Subcommittee of Communications and Technology of the Committee on Energy and Commerce will come to order.

But prior to my opening statement I will take a point of personal privilege. I know the -- our chair has -- because I was there in two of the subcommittees yesterday, but on behalf of this subcommittee we want to thank you very much for your service, not only for your going on 10 terms in the United States House of Representatives, but also for your service here on this committee and subcommittee. And we have appreciated everything you have done. And you know, you are going to be sorely missed here. You know, it takes a lot of time to get the knowledge and the experience which you have gained, but you have also imparted, which has been great. You have been wonderful about having so many meetings that brings forth -- brings all of the members together, and so everyone was part of the process.

And so I just want to thank you very much for all of your hard work. And I know it was a tough decision, but, you know, for you and your family it was the right decision. But we are going to miss you. So I greatly appreciate it.

And I will yield to the gentlelady, the ranking member from California.

*Ms. Matsui. Thank you very much, Mr. Chairman. I also want to echo what my ranking member has said. You have been an outstanding leader, and being a woman I know how hard that can be because we think in many ways, and you have tried to do all of that, and personified how important it is to demonstrate, as a Member, you can do it. And we appreciate everything that you have done --

*The Chair. Thank you.

*Ms. Matsui. Your friendship and your leaning toward bipartisanship as we got to know each other personally. So I thank you very much, and we are going to miss you. I know we have some more time.

*The Chair. Yes, that is right, we still have --

*Ms. Matsui. But --

*The Chair. We have almost a year to go here, ladies and gentleman, and lots to be done.

*Ms. Matsui. Thank you, we are not going to go into that. But anyway, we --

*The Chair. Thank you, thank you.

*Ms. Matsui. Thank you for your service.

*The Chair. Thank you. It means so much, just for all the kind comments and just -- it has been such an honor and privilege to chair this committee. It really is the best committee on Capitol Hill. We all know that. We all love serving on this committee, and it really attracts the best of Congress. And I have -- it has just been extraordinary to lead this committee, such an honor and privilege.

To both the members and the staff, you know, just -- and we have done a lot, and we are going to -- we have a lot more to do to get done this Congress, and we are going to work together to get as much done as possible in the midst of a crazy time. But if it can be done, we are going to do it.

So thank you for your leadership. Thank you for your friendship. I will dearly miss you, but we are going to have some good times before I exit completely. Okay.

*Mr. Latta. Well, thank you.

[Applause.]

*The Chair. Thank you, thank you.

*Mr. Latta. Well thank you, Chair. And again, the subcommittee will come to order, and the chair recognizes

himself for an opening statement.

Good morning, and welcome to today's hearing to discuss solutions to counter the significant threats communist China poses to the United States.

Every minute China is attempting to infiltrate communication networks across the globe in its quest for global economic dominance. Whether it be unauthorized access to sensitive data, manipulating our networks, or attempting to disrupt critical infrastructure, the Chinese Communist Party does not play by the rules.

In an effort to combat this foreign influence, this committee has worked on a bipartisan basis to secure our domestic communications networks from foreign threats. In 2020 we passed the Secure and Trusted Communications Networks Act to rip and replace Huawei and ZTE equipment from our networks. That law also created a list of covered equipment and services that pose an unacceptable risk to our national security. Last Congress we passed the Secure Equipment Act to prohibit the FCC from authorizing equipment from entities on the covered list.

Today we are building on those efforts by discussing

five different legislative proposals that will help promote U.S. innovation and ensure the U.S. continues to lead the world in combating Chinese tech influence.

H.R. 2864 would amend the Secured and Trusted Communications Network Act to add equipment produced by the company DJI Technologies to the FCC's covered list due to the threat that DJI Technologies pose to the national security of the United States.

Next we will consider H.R. 820, the Foreign Adversary Communications Transparency Act, which would require the FCC to annually publish a list of entities that hold a license granted by the FCC and are owned by China, Cuba, Iran, North Korea, Russia, and Venezuela.

Both of these bills are led by my colleague, the gentlelady from New York's 21st district, and I thank her for her work on these important issues.

We are also considering H.R. 1513, the Future Networks Act, introduced by the ranking member of the subcommittee, the gentlelady from California's 6th district. This bipartisan legislation would require the FCC to establish a 6G task force to develop a report on the standards

development process and possible uses of sixth-generation technology.

The other two discussion drafts being considered today would require the Assistant Secretary for Communications and Information to study whether certain routers, modems, and drones produced by companies with ties to our adversaries pose an unacceptable risk to our national security, as well as technologies that would increase the redundancy and resiliency of Taiwan's communications networks. Taiwan's independence continues to be threatened by the Chinese Communist Party, and staying connected is crucial for economic and military security.

These bills highlight the new and evolving threat that our adversaries pose to our communications networks, and show that we must remain ever vigilant and ready to act. I am proud that this subcommittee continues its important bipartisan work to lead on solutions that protect Americans and safeguard our communications network.

I thank again the panel for appearing before us today and look forward to the discussion.

[The prepared statement of Mr. Latta follows:]

**********COMMITTEE INSERT**********

*Mr. Latta. And at this time I yield back the balance of my time, and I now recognize my colleague, the gentlelady from the California's 7th district, the ranking member of the subcommittee, for her opening statement.

*Ms. Matsui. Thank you very much, Mr. Chairman.

Today's hearing comes at a critical time. Vulnerabilities in America's communications networks continue to pose an unacceptable risk to our national security. We know our global adversaries are working tirelessly to exploit the weak links throughout our networks. Nowhere is this dynamic clearer than with the vulnerable network gear still operating in American telecom networks.

As an original cosponsor of the rip and replace bill, I believe it is a national security imperative that we fully fund the shortfall in the reimbursement program as quickly as possible. Allowing Chinese-produced Huawei and ZTE gear to operate in a communications network is like locking up the house and leaving the back door open.

Thankfully, the FCC has made progress, but our work is far from complete, and we simply cannot afford to wait. Congress must immediately explore every option on the table

to deal with this urgent threat. That is why we requested updated data from the FCC and detailing on a state-by-state basis where this gear remains on our networks.

The data the FCC provided reinforces what we already know to be true: this gear is still operating in nearly every single state in this country. It is both in red states and blue states and rural areas and urban centers. That is why funding the shortfall immediately needs to be a bipartisan, nationwide priority for all of my colleagues. I am ready to work with any of my colleagues to get this done.

I am also excited to see my FUTURE Networks Act on the agenda today. For the United States to stay ahead of the rest of the world in wireless communications, we need to be taking steps to prepare for the next generation of networks because the economic and national security stakes and the global race to 6G couldn't be higher. This bipartisan bill would make a downpayment on American leadership by establishing a 6G task force to ensure the United States is taking the necessary steps to lead.

And as networks evolve, there will be other opportunities to reassert U.S. leadership. NTIA continues to

make progress implementing the Wireless Innovation Fund to encourage the development and deployment of Open RAN systems. Open RAN gives us a chance to establish a counterweight to Huawei in the global equipment market and to capitalize on the United States' strengths in software and high-value skills.

So clearly, there is work to be done to stay ahead in the 21st century innovation race. I appreciate the witnesses for being here today.

[The prepared statement of Ms. Matsui follows:]

**********COMMITTEE INSERT**********

*Ms. Matsui. And I yield back the balance of my time.

*Mr. Latta. Thank you. The gentlelady does yield back the balance of her time, and the chair now recognizes the gentlelady from Washington, the chair of the full committee, for her opening statement.

*The Chair. Good morning. Over the past year this committee has held numerous hearings to discuss the many threats posed by the Chinese Communist Party to the U.S. These range from supply chain vulnerabilities to espionage and attacks on our communications networks. China-based companies like Huawei and ZTE have emerged as top players in the global telecommunications industry. These companies operate in an environment tightly intertwined with the Chinese Government, raising questions about their independence and potential for exploitation by the CCP.

Relying on their technology comes with significant risk. It could be used by the CCP to surveil Americans, steal people's personal information, and even shut down entire networks. Homes, schools, hospitals, our financial system, and the military are all in jeopardy as long as this equipment remains part of our communications infrastructure.

That is why in 2020 Congress enacted the Secured and Trusted Communications Networks Act to remove Huawei and ZTE entirely from our networks. That work is ongoing, and it continues to be a top priority of this committee to make sure carriers have the resources they need to remove this equipment from U.S. networks and replace it with trusted equipment.

But that is just the first step. China's aggressive pursuit of technological advancement is a direct threat to American national security and economic leadership. The Chinese Government's strategic initiatives such as the Made in China 2025 plan and the Belt and Road Initiative aim to achieve dominance in technologies that are critical to win in the future. That includes technologies like artificial intelligence, quantum computing, and advanced manufacturing.

At the recent World Radiocommunication Conference we witnessed this first hand as China and Huawei aggressively worked to undermine U.S. leadership on spectrum policy and give Huawei a global competitive advantage.

Additional actions taken by China, including intellectual property theft, forced technology transfer, and state-sponsored industrial espionage further undermine free

markets, fair competition, and American innovation and entrepreneurship.

Perhaps most alarming is the evolving landscape of cyber threats posed by China. Last month we held a hearing on cybersecurity, where we examined how foreign actors are increasingly exploiting widespread vulnerabilities in our critical infrastructure. State-sponsored cyber attacks targeting U.S. government agencies, businesses, hospitals, and our military have become increasingly sophisticated, frequent, and pose significant economic and national security threats.

Look no further than the 2017 Equifax data breach, which exposed personal information of hundreds of millions of Americans, or the 2020 SolarWinds incidents, which gave China-based hackers access to sensitive information across the Federal Government. These vulnerabilities must be addressed.

Today we will examine a number of legislative solutions to counter the influence of China and promote U.S. leadership in technology. This hearing will be an opportunity to discuss adding certain CCP control technologies and equipment

to the Federal Communication Commission's covered list, and how to increase transparency for Americans about which companies operating in the U.S. are owned by China.

We will also look at ways we can strengthen communications with our allies overseas, and establishing a 6G task force to advance American innovation and win the future.

The United States faces exceedingly complex threats from China and other adversaries that require a comprehensive and coordinated response. This response must include efforts to secure critical supply chains, protect our allies, strengthen cybersecurity defenses, and engage in strategic competition with China in key technologies. Failure to address these challenges effectively not only jeopardizes U.S. economic competitiveness and national security, but also risks ceding ground to an adversarial power intent on reshaping the global order in its favor.

I would like to thank our witnesses for being here today, and I look forward to this important and timely discussion.

[The prepared statement of The Chair follows:]

309

310 **********COMMITTEE INSERT**********

311

*The Chair. Mr. Chairman, I yield back.

*Mr. Latta. Thank you very much. The gentlelady yields back, and the chair now recognizes the gentleman from New Jersey, the ranking member of the full committee, for five minutes for an opening statement.

*Mr. Pallone. Thank you, Mr. Chairman.

Today this subcommittee continues its vigilance in protecting our communication networks from rogue national states. Fortifying our networks to better defend against these national security threats is essential, and I am pleased we will be discussing a broad range of proposals to advance the safety and security of our communications networks.

These networks are a significant driver of the American economy, given so much of our daily lives run on them. From health care to energy to public safety, nearly every facet of American life relies on these networks. So even as we work to ensure that every American can access high-speed, reliable broadband Internet, we must also recognize our efforts to do so make our communications networks and the devices that run on them targets.

In fact, foreign adversaries often see our communications networks and devices as the entry points to disrupt our daily lives and conduct espionage campaigns. Just last week U.S. officials issued an advisory stating that Volt Typhoon, a hacking group backed by the People's Republic of China, had gained access to critical water, energy, and communications systems for at least the past five years. And because of this access, there is a real risk that the information they collected could be used to launch cyber attacks on our critical infrastructure.

Moreover, the information and technology sector is increasingly seen as a lucrative way to gain worldwide influence and control. You can see this in Huawei's aggressive deployment of wireless infrastructure across the globe.

It was also reported yesterday that hacking groups linked to China, Russia, and North Korea, and Iran are turning to artificial intelligence to strengthen their spying capabilities. And what is at stake is not just the U.S. leadership on technology and innovation, but also values like free speech and expression, democracy, as well as civil and

human rights.

Fortunately, this committee has worked together on a bipartisan basis to enhance the security of our communications networks and advance legislation that furthers our national security interests. In 2020 we passed the bipartisan Secure and Trusted Communications Networks Act. This law gives the Federal Communications Commission the authority to exclude suspect equipment and services from our communications networks if the agency finds that it poses a national security risk.

This is critical, but we need to come together to make sure the FCC gets the additional $3 billion it needs to fully fund the rip and replace program to rid our networks of this equipment. And since it has been four years since this secure and trusted framework was enacted, we should also examine how it is working, and whether it needs any changes in the years ahead as these issues become even more complex.

The Biden Administration and the FCC have also taken several actions to build out our communications networks and address security concerns. Most recently, the Biden Administration successfully defended our nation's policy

interests at the World Radio Conference against aggressive moves by China to undermine the success of unlicensed technology. This is an area of innovation where the United States has been a worldwide leader.

Last March President Biden also released the National Cybersecurity Strategy. It shifts the burden of protecting cyberspace away from consumers, small businesses, and local governments to software providers who are better positioned to reduce security risks.

And finally, we cannot overlook the importance of ensuring that all Americans have access to affordable, reliable Internet service with the digital skills to use it. This not only helps Americans access health care, education, and job resources, it also helps drive our global leadership in innovation, which strengthens our nation as a whole.

Internet affordability has been a major issue, and it is why we created the Affordable Connectivity Program as part of the Bipartisan Infrastructure Law. Today it is helping more than 23 million American families in all our congressional districts afford their monthly Internet bills. Without additional funding, the program will expire in a couple of

months. We simply cannot allow that to happen. We must pass H.R. 6929, the Affordable Connectivity Program Extension Act, bipartisan legislation introduced by Representative Clarke to extend this critical affordability program, and I continue to hold out hope that our Republican colleagues would join with us in passing this bill.

And if Republicans are really serious about addressing national security threats, they would join us in demanding the House vote on legislation that has now passed the Senate that would provide funding to strengthen our national defense and ensure Ukraine can continue to protect its democracy from Russia's unprovoked war of aggression. Speaker Johnson is blocking this urgent national security funding, siding with the pro-Putin extreme Republicans. And these political games have to end.

[The prepared statement of Mr. Pallone follows:]

**********COMMITTEE INSERT**********

*Mr. Pallone. And with that I yield back the balance of my time, Mr. Chairman.

*Mr. Latta. Well, thank you very much. The gentleman yields back the balance of his time. And this has now concluded the member opening statements. The chair reminds members that, pursuant to committee rules, all members' opening statements will be made part of the record.

We also want to again -- once again thank our witnesses for being with us before the subcommittee to testify.

Our witnesses will have five minutes to provide an opening statement, which will be followed by a round of questions from the members.

The witnesses before us today are Mr. James Lewis, senior vice president at the Center for Strategic and International Studies; Mr. Craig Singleton, the China program senior director and senior fellow at the Foundation of Defense of Democracies; Ms. Lindsay Gorman, the senior fellow for emerging technologies at the German Marshall Fund's Alliance for Securing Democracy.

I would like to note to our witnesses that there is a timer light that will be on the table which will turn yellow

when you have one minute remaining and will turn red when your time has expired. If you hear me tapping the gavel, please wrap up your statement or, if you are getting a question from a member, please wrap that up.

Mr. Lewis, you are recognized for five minutes for your opening statement. Again, thanks for being with us today.

STATEMENT OF JAMES LEWIS, SENIOR VICE PRESIDENT, CENTER FOR STRATEGIC AND INTERNATIONAL STUDIES (CSIS); CRAIG SINGLETON, CHINA PROGRAM SENIOR DIRECTOR AND SENIOR FELLOW, FOUNDATION OF DEFENSE OF DEMOCRACIES; AND LINDSAY GORMAN, SENIOR FELLOW FOR EMERGING TECHNOLOGIES, GERMAN MARSHALL FUND'S ALLIANCE FOR SECURING DEMOCRACY

STATEMENT OF JAMES LEWIS

*Dr. Lewis. Thank you, Mr. Chairman. Chairman Latta, Ranking Member Matsui, and distinguished members of the subcommittee, thank you for the opportunity to testify.

Poorly secured communication networks create significant security risks, and there is an urgent need for the U.S. to address digital vulnerabilities. Progress has been made, but much more needs to be done in light of competition with China.

This will require reducing China's role in Western supply networks and its presence in Western digital infrastructures, a difficult task given our interdependence. We have built a deep, symbiotic tech relationship with China

over the years, contributing to China's economic growth and rise as a major power. However, China's authoritarian governance, espionage, human rights issues, and predatory trade behavior create unacceptable risks.

One of the dilemmas that sometimes doesn't get recognized is that China has real strengths. They have a lot of money. They have a lot of people. They have smart people. They have many problems, but they have real strengths in 5G, 6G, other technologies including artificial intelligence, quantum communications, semiconductors, satellites, and in spectrum allocation where they have, as I think some of you members have mentioned, a definite plan to displace the U.S.

China's goal is to create a dominant position globally. Chinese espionage has escalated to unprecedented levels, nothing seen even before the end of the Cold War. China's Comprehensive National Surveillance system and its 2017 National Intelligence Law, which mandates the cooperation of Chinese citizens and companies without any grounds for appeal, means that any device that connects to the Internet is a potential source of risk.

China is collecting masses of Americans' personal data. China's 2015 hack of the Office of Personnel Management is an example of its data-centric approach to espionage. China can use its position as a supplier for espionage purposes or to degrade or disrupt services, or to deny access to vital components we need for our own technology base.

So far we have only seen espionage, but recent testimony from the FBI, Cyber Command, and others shows that the disruption of critical infrastructure is a growing risk. And China, of course, has conducted extensive espionage to find vulnerabilities in our critical infrastructure.

We all know China plays a central role in manufacturing hardware due to government investment, industrial espionage, and Western financial decisions. China's role in software is less recognized, but is equally critical. There are many products that have Chinese software components in them not just in the app space, but in manufacturing devices and critical infrastructure. These software positions by China do create vulnerability. They do offer the opportunity for disruption and espionage. The U.S. can reduce risk by changing software development practices, imposing liability,

and implementing a disclosure and risk mitigation mechanism for foreign origin software and communications devices.

This is a competition between a market economy and a state-directed economy. While complete decoupling from China is not possible in the near term, managing the risks in the technology supply chains with China is crucial. Solutions include passing legislation for a national privacy law, expanding supply chain transparency, and restricting the use of Chinese technology, as well as providing incentives and subsidies to our own companies when necessary.

Many risks can be mitigated, but the subcommittee's work in building a framework of new authorities is important, essential, and I would say overdue. I thank the committee for the opportunity to testify, and look forward to your questions.

[The prepared statement of Mr. Lewis follows:]

**********COMMITTEE INSERT**********

*Mr. Latta. Well, thank you for your statement.

And Mr. Singleton, you are recognized for five minutes.

STATEMENT OF CRAIG SINGLETON

*Mr. Singleton. Good morning, Chairman Latta, Ranking Member Matsui, and distinguished members of the subcommittee. Thank you for the opportunity to testify about securing U.S. communication networks from foreign adversaries. I am pleased to provide relevant research and policy insights from the Foundation for Defense of Democracies, a non-partisan research institute where I serve as a senior fellow.

In today's era of digital warfare, the United States faces an insidious challenge as China deftly maneuvers within our communication networks, undermining the foundational integrity of our information systems and national security. Increasingly, the Chinese are not merely seeking access to our networks. They are preemptively positioning to compromise and control them.

As noted in the Defense Department's 2023 Cyber Strategy, China's peacetime penetration of U.S. networks informs its preparations for war, with the line between the two becoming increasingly blurred. China's People's Liberation Army, or PLA, has long prioritized targeting,

penetrating, and compromising our "information detection sources, information channels, and information processing and decision-making systems.'' The goal of such compromise operations, according to PLA strategists, is to "sap enemy morale, disintegrate their will to fight, and ignite anti-war sentiment among their citizens,'' all without the clamor of conventional warfare.

That theoretical framing explains why China's communications and networks attacks are focused on targeting what PLA planners refer to as vital points, or weaknesses in our communications infrastructure. These points include public-facing vulnerabilities and communications-dependent sectors we rely on daily, like energy, water, finance, transportation, and health care. By pre-positioning itself within these sectors and the communications networks that connect them, China is poised to strike at our nation's lifelines to, in the words of Jen Easterly, the director of the Cybersecurity and Infrastructure Security Agency, induce societal panic.

The U.S. Government's recent exposure of the Chinese state-directed Volt Typhoon operation is therefore not an

outlier; it is a signal. This Chinese cyber initiative compromised thousands of Internet-connected network devices in a deliberate attempt to infiltrate Western critical infrastructure including naval ports, Internet service providers, and utilities.

This and other recent examples offer a revealing glimpse into China's strategic calculus, showcasing Beijing's willingness to embrace high-risk, short-of-war operations to compromise critical U.S. communication infrastructure, even amidst an ostensible diplomatic thaw.

Looking ahead to the battle space of 6G and beyond, China is laying the groundwork to dominate these future technologies and supply chains, too. China's proactive positioning and standard-setting bodies like the International Telecommunications Union aims to advance global telecommunications norms that favor Chinese technologies and strategic interests, potentially embedding dependencies that could be exploited for intelligence gathering or to assert geopolitical leverage.

Paradoxically, even as policymakers intensify efforts to remove Huawei, ZTE, and DJI equipment from U.S. networks,

China is working to exploit open source collaborations like the Linux Foundation, O-RAN ALLIANCE, and others to reintroduce today's vulnerabilities into tomorrow's trusted networks.

The Linux Foundation counts among its members Chinese companies like Huawei, Tencent, Baidu, and WeBank, all of which maintain ties to China's government and its military. A significant portion of O-RAN ALLIANCE's members are headquartered in China. At least 16 maintain documented ties to China's security apparatus. That includes all three of China's mobile operators which are banned from operating here because they are subject to exploitation, influence, and control by the Chinese Government. Rigorous oversight is required to scrutinize these non-profit collaborations to ensure they do not serve as conduits for Chinese exploitation, espionage, or manipulation.

As China's approach evolves, so too must our own. Indictments and exposure have not deterred Beijing, nor has it meaningfully reduced China's technological leverage over us. Going forward we must embrace common-sense defensive measures, as well as deploy offensive policy tools that

impose significant costs on Chinese entities and individuals involved in perpetrating crimes against our communications infrastructure, with a goal of compelling Beijing to recalibrate its risk calculus.

On behalf of the Foundation for Defense of Democracies, I thank you again for inviting me here today.

[The prepared statement of Mr. Singleton follows:]

**********COMMITTEE INSERT**********

*Mr. Latta. Well, thank you very much, Mr. Singleton, for your statement.

And Ms. Gorman, you are recognized for five minutes for your opening statement.

STATEMENT OF LINDSAY GORMAN

*Mr. Gorman. Chairman Latta, Ranking member Matsui, and distinguished members of the subcommittee, thank you for holding this hearing and the opportunity to testify today on this important topic. My name is Lindsay Gorman, and I lead a research and analysis team at the German Marshall Fund's Alliance for Securing Democracy studying how democracies can together outcompete autocrats, chiefly the People's Republic of China, in technologies of the future.

I come at this question from the perspective of both a technologist who began my career building cryptographic protocols for IP telephony at Bell Labs, and a former White House adviser developing technology competition strategy. The opinions I express today are my own, and not that of my current or former employers.

Today the United States and its democratic allies are engaged in a technology contest with the PRC that defines our geopolitical moment. Nowhere is this competition clearer than over the struggle to define and build the future Internet, a structure I conceptualize as a connected layer --

a connected stack of layers where competitive advantages in building out one layer accrue dividends for dominance in other layers.

But so too can vulnerabilities propagate. This is particularly true for foundational infrastructure layers such as 5G or 6G telecommunications infrastructure or undersea cables. As communications networks advance in speed and data-carrying capacity, an explosion of applications and devices that sit atop those networks present new areas for competition and new vulnerabilities.

Applications in healthcare, smart cities, and connected vehicles have the potential to drive massive value creation, but also to introduce equally large cybersecurity risks. As Commerce Secretary Raimondo outlined last month, electric vehicles are "collecting a huge amount of information about the driver, the location of the vehicle, the surroundings of the vehicle. Do we want all that data going to Beijing?''

Two dimensions of cyber risk in the future Internet technology stack necessitate heightened U.S. attention.

First, PRC dominance in the foundational layer of critical infrastructure presents an unacceptable risk of

dependance. If U.S. and allied networks are controlled by companies accountable to the PRC, in a crisis scenario those networks could be held hostage.

Second, cyber espionage is a key tactic in the PRC's strategy to acquire U.S. and allied origin technology. The U.S. loses around 300 billion annually to the -- to CCP intellectual property theft alone, described by former NSA director Keith Alexander as the greatest transfer of wealth in history. And cyber intrusions continue to be exposed by CISA, NSA, FBI, and allied partners.

Looking ahead, 6G presents new areas for strategic competition and national security vulnerability through multi-sensory, mixed reality, connected autonomous systems, drone deliveries, smart services, and non-terrestrial networks. The race is on to develop 6G standards. With the PRC's identification of 6G as a top priority in its 14th 5-year plan, averting a repeat of China's global leadership in 5G will require both innovation and collaboration.

Over the last four years the U.S. policy response to this competition has ramped up significantly. The U.S. International Development Finance Corporation has made

strategic investments to prevent the use of PRC-based network infrastructure and prop up viable alternatives. And through the Next G Alliance, the Washington, D.C.-based Alliance for Telecommunications Industry Solutions Group has signed MoUs with the O-RAN ALLIANCE, Europe's 6G-IA industry group, Japan's Beyond 5G Promotion Consortium, and Korea's 5G Forum.

Yet the reality is that Huawei is still embedded in networks around the globe. In 2022, for example, PRC-based vendors still accounted for more than half of the 5G equipment installed in Europe. In my written testimony I offer five recommendations to Congress to ensure our communications networks remain competitive and secure from foreign autocratic threats.

First, analyze -- catalyze 6G development through the creation of international centers of excellence.

Second, incentivize the adoption of robust cybersecurity requirements into Open RAN and 6G standards.

Third, set roadmaps for post-quantum cryptographic systems.

Fourth, pass Federal data privacy and security legislation, including limiting the acquisition and sale of

biometric data and bulk third-party data brokerage.

And fifth, invest in the U.S.-EU Trade and Technology Council and the Quad, where much of this needed international coordination is happening for semi-permanence over the next decade.

Our global technology infrastructure must be governed by values rooted in openness, transparency, freedom, and democracy, not surveillance, censorship, and control. And Congress is critical to this work.

Thank you, and I look forward to your questions.

[The prepared statement of Ms. Gorman follows:]

**********COMMITTEE INSERT**********

*Mr. Latta. Well, thank you very much for your opening statement, and that will conclude our witnesses' opening statements. And I will now begin questions and recognize myself for five minutes.

Mr. Lewis, a major focus of our conversation today is the vulnerabilities of -- Chinese-controlled equipment pose to our networks. It is very concerning that the U.S. Government is continuing to purchase technology and equipment from foreign adversaries. What is your opinion about the Federal Government using routers that are a security risk?

*Dr. Lewis. We have boxed ourselves in in some ways, Mr. Chairman, in that, as you know from the Huawei story, there may not be U.S. sources of supply. There may not be Western sources of supply. So we have boxed ourselves in. This has been a problem for more than a decade.

And we will need to remove that equipment because it is a vulnerability that the Chinese intelligence services would exploit. So the risk is greater than we assumed, perhaps, when we started doing this, and the efforts to remove Chinese technology from Federal systems are crucial.

*Mr. Latta. You know, let me just follow up because,

again, you are talking about the information that -- from hacks that have occurred, you know, Americans read about -- from the OPM hack to information being taken on -- from -- on medical data from health systems. What is your opinion on what is the communist Chinese looking at using all that information for?

*Dr. Lewis. It is worth bearing in mind that the leaders of China are very paranoid. And so it may not be rational to collect all this data, but they are collecting this data first on their own citizens, now on Americans.

And if you visit China and they will display their internal security systems, they have programs where if you walk across the street there is a camera that goes to a police station and a little bubble appears over you with your name, your Social Security number, your criminal record, anything else they think is useful. So they are building a giant server. They have built, I beg your pardon, built a giant surveillance system, and they are putting that data into it.

It is also some of the way people do intelligence now is that if you can get, the same way as you do in sales, masses

of data that you can use for targeting, it works great for sales, it works great for spying, too.

*Mr. Latta. Thank you.

Mr. Singleton, how about CCP-controlled drone companies? Do you believe it is a good or a bad idea that these drones are being used in the United States that are linked to communist China?

*Mr. Singleton. Absolutely. You know, DJI sits at the heart of China's military civil fusion strategy, which breaks down barriers between the civilian and military institutions to mobilize the former in service of the latter. So DJI drones collect vast amounts of sensitive data, everything from high-resolution images of critical infrastructure to facial recognition technology and remote sensors that can measure even an individual's heart rate.

Compounding the DJI risk is their capacity for geofencing, so they can use GPS data. Or using GPS data, DJI can decide whether one of its drones will function in a given area, allowing the company to turn down or turn off entire fleets of drones. I think the ability to deactivate American drones shouldn't be entrusted to a foreign entity, least of

which the CCP.

*Mr. Latta. Thank you.

Ms. Gorman, in your testimony you talk about all the information that is being collected out there, especially, you know, from smart vehicles. And we are working on that to make sure that we have the cybersecurity and the privacy there. But you also mentioned about the 6G and what is happening out there.

Is the United States falling behind, especially -- we were talking about 5G technology, and then all of a sudden we started talking about 6G. Where are we in that, on the 6G race?

*Mr. Gorman. Thank you for the question. We are starting from behind because 6G technology is going to be built on top of 5G technology. The United States does not have a player in the Infrastructure Radio Access Network vendor market. Huawei leads it. So we are trying to claw our way back. I think initiatives like Open RAN help break up the market, but we are not starting from a place of strength when it comes to that network layer.

*Mr. Latta. Well, thank you.

Mr. Singleton, in my last 30 seconds, how can we better educate or, better yet, get the information out to Americans and the U.S. Government about the dangers of purchasing vulnerable equipment?

*Mr. Singleton. Thanks. It is an excellent question.

I think, when I talk to average Americans about the threat posed by DJI drones or TikTok, they are simply unaware of it. I think that there are really broad opportunities here for public partner -- public-private partnerships to better educate the public. I think the U.S. Government has to do a better job beyond the very useful and robust reports that CISA puts out on a routine basis about these threats.

*Mr. Latta. Well, thank you. My time is expired, and I will submit my other questions for the record.

[The information follows:]

**********COMMITTEE INSERT**********

*Mr. Latta. And the chair now recognizes the gentlelady from California, the ranking member of the subcommittee, for five minutes for questions.

*Ms. Matsui. Thank you very much, Mr. Chairman.

I was an original cosponsor of the rip and replace legislation because I believe, as I do now, that getting every single piece of vulnerable Chinese gear out of our networks must happen immediately. So to start I would like to ask each member of the panel a few yes-or-no questions, and I want you to answer quickly. Is this yes or no?

Starting from you, Mr. Lewis, yes or no, do you believe this network gear poses a severe threat to our national security?

*Dr. Lewis. Yes.

*Ms. Matsui. And?

*Mr. Singleton. Yes.

*Mr. Gorman. Yes.

*Ms. Matsui. Yes or no, do you believe this network gear jeopardizes the security of America's personal data?

*Dr. Lewis. Yes.

*Mr. Singleton. Yes.

*Mr. Gorman. Yes.

*Ms. Matsui. Yes or no, do you believe Congress should prioritize its immediate removal?

*Dr. Lewis. Yes.

*Mr. Singleton. Yes.

*Mr. Gorman. Yes.

*Ms. Matsui. Thank you.

Allowing this funding shortfall to persist is a gift to our foreign adversaries. They want nothing more than to see Congress come up short. We can't let that happen. I am ready to work with my colleagues to finish what we started.

I am glad my Future Networks Act is on the agenda today. My bill would direct the FCC to bring together industry leaders, public interest groups, and government experts to establish a 6G task force. The economic and geopolitical stakes in the race to 6G couldn't be higher. That is why I believe the U.S. needs to act.

Some describe 6G as a simple evolution of 5G, but I think all of you know it is not a complete picture. It is an incomplete picture. Ms. Gorman, can you describe the technological differences, and why China is so keenly focused

on winning this race?

*Mr. Gorman. China is focused on winning the 6G race for many of the same reasons it has focused on winning the 5G race, because its presence in networks around the world allows it to build leverage, allows it to collect data, allows it to create dependencies across the Belt and Road Initiative.

*Ms. Matsui. Okay --

*Mr. Gorman. And 6G technology is going to allow many of the advances that we have been hearing about with the Internet of Things in -- and really explode the information environment there.

*Ms. Matsui. Okay, and the Future Networks Act would require the 6G task force report on the current state of industry-led standard-setting bodies and the development of 6G.

Ms. Gorman, can you describe the role of standard-setting bodies and how they are being used to help or hinder U.S. values in the development of 6G?

*Mr. Gorman. International technical standards-setting bodies are these groups of largely industry-led players that

agree on the standard for the next generation of the Internet, how technology developed in one country can interlock with technology developed in another country, and we can all have the same Internet.

Now, China has prioritized putting its own patents into the standards from which it accrues revenue, from which it accrues royalties, and from which it accrues value in defining the standards. Now, at some organizations like the International Telecommunications Union, we have all seen -- also seen a values creep, where some of the standards that Chinese providers have introduced have ended up creating things like facial recognition technologies that allow for ethnic profiling, racial profiling that go against our values.

*Ms. Matsui. Okay.

*Mr. Gorman. So it is playing out in this domain.

*Ms. Matsui. Thank you.

Back in 2020 I was an original cosponsor of the USA Telecommunications Act to support the development and deployment of open, interoperable equipment. I also worked to include $1.5 billion in the CHIPS and Science Act to stand

up the Wireless Innovation Fund within the NTIA.

Open RAN presents a unique opportunity to add needed diversity for the highly consolidated equipment market. Ms. Gorman, can you talk about the role of the allied coordination to Open RAN to create meaningful alternatives to Huawei?

*Mr. Gorman. It is critical. Right now there are three, maybe four players in the 5G market, and Huawei leads them. Open RAN will allow us to add new entrants.

It is important to note, though, that Huawei too is developing Open RAN solutions, so it is not a panacea. But we need to be coordinating with our allies and partners so that they too can develop the next generation 6G equipment with the Open RAN standard.

*Ms. Matsui. Okay, thank you.

Mr. Lewis, can you discuss some of the limitations of technological decoupling with China, and the challenges the U.S. faces in managing technology supply chains?

*Dr. Lewis. Thank you. First we should note that many companies are adopting what they now call a China Plus One strategy, which is they are moving investment out of China,

or at least they are not putting new investment in because they are worried about the risk, the political risk of doing business in China and the espionage risk.

So what we have seen is a period that began in the 1980s of building this strong, interconnected economy. And so many things -- the one I think is funniest, I still don't know if it is true, but you know the little berets that Army soldiers wear? Those are made in China. We have an interdependent economy, and pulling it apart will be difficult. There is clearly risk. And that is where the committee's work is valuable.

*Ms. Matsui. Okay. I thank you very much.

And I yield back.

*Mr. Latta. Thank you very much. The gentlelady yields back, and the chair now recognizes the gentleman from Florida's 12th district for five minutes for questions.

*Mr. Bilirakis. Thank you, Mr. Chairman. I appreciate it very much. Thanks for holding this hearing. It is so important.

It is no secret that we have been competing with China for telecommunications. It is the center of the debate for

5G innovation and deployment, as well as the identification of cybersecurity threats and mitigation strategies. We have been -- we have seen some strides toward these goals. For example, we were able to sign my bill, the RANSOM [sic] Act, into law, which strengthens the Federal Government's efforts to respond to recent ransomware and other cyber attacks from foreign adversaries. But this is just a start. That is an understatement. We must remain vigilant, that is for sure.

Mr. Singleton, drones are a growing segment in society and technological advancements, and not just for entertainment. Archer First Response Systems is a company in Florida partnering with local hospitals that developed a 911 integrated drone system that deploys defibrillators and Narcan spray for 911 callers, a need when an ambulance crew could be too far away to adequately assist. It has a potential to revolutionize first response and improve health crisis outcomes.

I am happy to say that Florida statute requires that no critical components of drones may be made by any foreign country of concern, including China. I am further happy to say that all critical components of Archer are made in the

good old USA. However, the fact is most drones are made by Chinese companies, and many states do not have the same protections as Florida in combating Chinese interference.

So Mr. Singleton, how does the Countering CCP Drones Act help promote an increased U.S.-based market for drones?

And should we be looking at a national critical components ban similar to Florida's, at least in our health care space, where it is not just privacy but potentially lives in the balance?

If you could answer that question, I would appreciate it.

*Mr. Singleton. Sure, thank you.

Drones will play a critical role in the 21st century economy. There are myriad examples where drones are incredibly impactful during times of crisis, but also impacting and improving the lives of everyday Americans to buy something online and have it delivered by a drone. This is the future of where we are going.

The unfortunate reality is that China maintains more than a monopoly in this area. Over 80 percent of drones are produced by China. They have invested heavily and subsidized

these companies and industries in ways that we haven't. And there is a current lack of market competitors.

I think, unfortunately, as we have seen with ByteDance, as we have seen with Huawei, we are forced to wage a war of attrition against these companies by slowly eating into their market share. And that will require steps from, I think, Congress, but also at the state and local level to slowly weed out these companies from their supply chains and try to prop up alternatives, whether they are from the United States or allied countries like South Korea and Japan.

*Mr. Bilirakis. Thank you. I will move on, but that is worthy of more discussion.

Mr. Lewis, there are a lot of concerns about China and our telecommunications equipment, and rightfully so. However, we cannot neglect threats we face from other adversaries, as well. How are the capabilities of Russia, Iran, for instance, and North Korea developing?

And what proactive steps should we be taking to combat infrastructure equipment made by these foreign actors from entering our networks?

*Dr. Lewis. That is a great question, and it refers

back to Ranking Member Matsui's comments, which is if you took apart a 5G box, you know, from -- whether it was Huawei or Ericsson, you would find it depends on American equipment, it depends on Chinese equipment. When you look at the software, it is largely American, it is largely Chinese, but the Russians also are strong in software, and the software vulnerability is one we haven't paid as much attention to.

Weirdly enough, the North Koreans -- I think it is weird -- weirdly enough, the North Koreans have subcontracting companies that make software for Western companies. So if you are using a European product, it may have North Korean software in it, and you won't even know.

So the manufacturing side, largely China, the software side, Russia and North Korea are also involved.

*Mr. Bilirakis. Well, thank you very much. I appreciate it.

I yield back, Mr. Chairman.

*Mr. Latta. Thank you. The gentleman yields back, and the chair now recognizes the gentleman from Florida's 9th district for five minutes for questions.

*Mr. Soto. Thank you, Chairman.

The United States is gearing up for this incredible competition with countries that don't share our values, like China and Russia and North Korea.

We passed the infrastructure law with $65 billion to ensure rural broadband in areas across the nation, including rural areas in my district like Kenansville and Bull Creek and South Osceola County, as well as areas of east Osceola County.

We also have the Affordable Connectivity Act, the program that is helping make affordable Internet for, literally, tens of thousands of my constituents. And we need to fund it and continue it.

When you think about an event like the Super Bowl, how much telecom equipment and part of our system is required to make it happen, even the comments about it -- but of course, there are far more serious areas like our U.S. military, power plants, water treatment centers, traffic systems, the cloud, and other systems that keep us vulnerable, which is why I was thrilled that our Ranking Member Pallone helped put together the rip and replace program. And as he had mentioned, we need $3 billion in funding to rid our country

of Huawei and other companies from China and other countries that don't share our values to ensure a resilient system.

We also passed the CHIPS Act, which has the Public Wireless Supply Chains Innovation Fund, 1.5 billion to really boost up domestic manufacturing and capacity, and as well as the President's executive order to ensure a duty for software providers to make our systems more resilient, defend critical telecom infrastructure, dismantle cyber hackers.

And what we are looking for is trust and resiliency. We just saw recently the Chinese hacking group Volt Typhoon get access to local infrastructure. We also know that foreign adversaries are embedded in foundational layers of the Internet stacks, as well as the Internet of Things, making it even more precarious. So we have to be proactive and not reactive.

I was excited, Chairman, about the recent O-RAN hearings we had, as well as today putting H.R. 1513, the Future Networks Act by our Ranking Member Matsui, on the agenda for today, which would create a 6G task force so that we are being proactive.

Ms. Gorman, how critical is it that we develop standards

for 6G and O-RAN here in the United States in order to make a more resilient system?

And what else should we be doing in these areas to gear up?

*Mr. Gorman. Thank you for the question. It is very critical.

As we spoke about earlier, China wants to lead the future of the Internet, just like their providers have led in the 5G layer. And with 6G, the amount of data, whether it is from drones, whether it is from remote telehealth visits, remote surgeries, connections, fielding networks in space, this -- the amount of data is going to explode in ways I think it is hard for us to conceptualize.

And it is the PRC's goal to collect the world's data, in part to feed into their own artificial intelligence systems, which then yield advantages in those systems, as well. So I think it cannot be understated how much we need to make sure that not just the United States, but also our allies and partners that share our democratic values lead in 6G.

And so there is a lot more we can do in international standards bodies, but really also in that sort of pre-

standards R&D and commercialization work. Our standards process has been industry-led. We think that is generally a good thing, but I think there are steers that, as policy-makers, we can indicate and to increase the cybersecurity and resilience of our systems.

*Mr. Soto. Thank you.

And Mr. Singleton, we are defending democracy both at home and abroad in areas such as Ukraine, Israel, and potentially Taiwan. Can you briefly assess where these countries' network security is, and what the United States needs to do to help?

*Mr. Singleton. Thank you for the question.

I mean, enhancing the resiliency of Taiwan's communication networks is absolutely crucial in the face of increased Chinese aggression. Taiwan is the number-one target of hacking in the world, almost all of it perpetrated by the Chinese Communist Party.

I mean, I think, really, there is a lot that Congress can be doing to help them. We can allocate funds specifically for research into advanced communications technologies that enhance their network resilience. We can

encourage partnerships between U.S. companies and Taiwanese entities to accelerate the development and deployment of those technologies. We can work to ease restrictions on the export of certain defensive communication technologies to Taiwan, and we can also support educational exchanges in cybersecurity and I think communications technology that can help build a workforce in Taiwan that is capable of maintaining and defending its own networks.

*Mr. Soto. And they sure make a lot of our microchips, so very important to continue that relationship.

And I yield back.

*Mr. Latta. The gentleman's time has expired and he yields back. The chair now recognizes the gentleman from Florida's 2nd district for five minutes for questions.

*Mr. Dunn. Thank you very much, Mr. Chairman.

So it is imperative that Congress enables American commercial enterprise with being able to compete with China's rapid technological development. This subcommittee has worked in a bipartisan manner to address critical issues like spectrum availability, streamlining, satellite and space permitting, AI, cybersecurity, wireless, and more.

Our shared goal is to keep America at the forefront of enterprise and, of course, to remain safe. We all know China's Digital Silk Road is rapidly acquiring the building blocks for 5G and, yes, even 6G global digital dominance. We talk a lot in Congress about the dangers and threats of TikTok, which is important. However, if China wins the 5G race and develops a software that rides on top of the next generation networks, I worry that the Chinese Communist Party will leverage that innovation against us in all sectors: energy, health care, AI, and everything.

In Florida China poses real risks to critical communications infrastructures, including manufacturing equipment, secure devices. But other examples include the Port of Panama City, located in my district, or Cecil Air and Space Port, which is also in Florida, along with Cape Canaveral.

My esteemed colleagues on this subcommittee enjoy a largely bipartisan, pro-American approach to technological innovation, which is fundamental in finding solutions to interagency debate and political disputes standing in the way of America's global competitiveness. And I look forward to

finding real solutions to clear both chambers of Congress at this urgent time and this quest.

Ms. Gorman, we know the first level of communications that will be compromised during any conflict with China over Taiwan is the submarine cables and other secured network devices that supply Taiwan and elsewhere. When we look at legislation to help secure our allies' networks in Taiwan, do you believe that data systems like satellite communications might have better resilience compared to the risks associated with stationary submarine cables?

*Mr. Gorman. I do. I don't know that they are a full substitution, but Taiwan itself is looking at developing satellite networks either in low Earth orbit, they have partnerships with providers in the UK now, and elsewhere in Europe. And we have seen already vulnerabilities of Taiwanese cables. Right now Taiwan is served by 16 submarine internet cables, 4 of which have direct connections to the United States, but only 1 of which is not at least partly owned by a Chinese telecommunications provider. That is the Pacific Light Cable network. So there is a vulnerability there.

Taiwan has accused China of cutting cables about a year ago, and so we absolutely need to look at backstops. Right now --

*Mr. Dunn. Yes, so --

*Mr. Gorman. -- the backstops would not --

*Mr. Dunn. I think people sometimes don't think about those -- the vulnerabilities of those cables, specifically.

Mr. Singleton, Congress and the FCC have implemented a number of regulatory actions targeting Chinese technology utilized in the U.S. For example, the Secure Equipment Act, enacted in 2022, directed the FCC to adopt rules that restrict the Commission from approving equipment authorizations on what they have -- a covered list, so a specific list of devices and manufacturers. This affects virtually every IoT device, Bluetooth, wireless, and cell phones, radio equipment, and everything manufactured by them.

While this bill prevents these Chinese and Russian companies from selling new and updated products, these entities are -- they are not barred from selling products that were previously authorized. Do you believe the FCC should revoke or phase out existing equipment authorizations

for the entities on the covered list?

*Mr. Singleton. I do, and I think that the examples of banning China's three mobile operators and the limited blowback that was sort of measured and monitored in the U.S.-China bilateral relationship is indicative of the fact that those strong sanctions, those strong measures can be absorbed, and with little blowback to us.

I think, ultimately, we have to do -- we have to think about waging this war of attrition. As we have talked about here, these technology standards are evolving in real time. Some of these outdated systems, whether they are ripped and replaced because of action taken by this committee in Congress, or whether just because our technological development and advancement allows us to leapfrog new technologies, some of these existing tools, systems, and processes will eventually be removed from our networks. It is a long-term strategic challenge, though.

*Mr. Dunn. In my remaining few seconds, Mr. Singleton, do you think that that is something that the FCC would do as a -- on their own, or do they need statutory language either to compel them to do that or to allow them to do that?

*Mr. Singleton. As far as I am aware, it is well within their current statutory framework and authority. I think pressure from Members of Congress and increased awareness on the issue provide political top cover to FCC officials, who are keen to take broader and stronger action against these problematic Chinese entities.

*Mr. Dunn. Thank you. I will take that as a homework assignment.

Mr. Chairman, I yield back.

*Mr. Latta. Thank you very much. The gentleman yields back, and the chair now recognizes the gentleman from New Jersey, the ranking member of the full committee, for five minutes for questions.

*Mr. Pallone. Thank you, Mr. Chairman. I mentioned earlier that the Secure and Trusted Communications Networks Act provides a helpful framework for how the FCC can work with our national security agencies to determine if communications equipment or services pose a national security threat. And I also understand that China, Russia, North Korea, and Iran are starting to use AI to enhance their spying capabilities. So I have a series of questions of Ms.

Gorman.

Do you agree that directing the FCC to work with our national security agencies to evaluate the security threats posed by communications equipment or services has been an effective framework?

And if so, how should we build upon this framework, especially given the increasing capabilities of artificial intelligence, Ms. Gorman?

*Mr. Gorman. I do, and I would offer one core recommendation to build on it, which is that we need to be more proactive in anticipating threats, as opposed to reactive and only responding to them once they are already embedded in their networks. We can forecast. We can predict which markets of the future are going to drive our competitiveness and drive our networks and security.

We should be doing that across the U.S. Government, building on that framework with FCC, communicating and collaborating with our intelligence agencies to predict and get ahead of some of the threats so that we don't have to go back and untangle them on the back end.

*Mr. Pallone. Well, thank you, and last Congress Chair

Rodgers and I, with the committee, advanced the strong, comprehensive, and bipartisan American Data Privacy and Protection Act. This legislation would put consumers back in control of their data, stop aggressive and abusive data collection by Big Tech, and require data minimization to ensure companies collect only the data they need to serve their customers.

So let me ask, Ms. Gorman, in your testimony you state that passage of a national privacy law would help mitigate the risks posed by Chinese technologies and suppliers. Do you agree that passage of strong, comprehensive Federal data privacy legislation will enhance our national security?

And if so, how?

*Mr. Gorman. Thank you for the question, and thank you for your leadership on comprehensive privacy legislation.

It is crucial. Right now it is open season on Americans' data, regardless of the sensitivity of that data. Data is becoming of strategic value in training artificial intelligence systems, as well as the traditional cybersecurity threats around sensitive information and kompromat, and access as well to business data. Personal

data can be used to create more sophisticated spear phishing campaigns, and the fact that we are not attempting to secure it at the Federal level creates massive loopholes.

I don't think that is the only solution. Data security also has to be a piece of it beyond just the personal data, but we should at least be protecting our personal data from unnecessary privacy breaches, particularly from foreign countries and companies like in China.

*Mr. Pallone. Thank you. I want to ask you one more question.

But did you want to add anything to this, Mr. Lewis, quickly?

*Dr. Lewis. Sure. Thank you, Chairman.

In conversations with government officials from many other countries, they complain about the U.S. lack of an overarching national privacy law, and it would address many of the espionage problems we face.

There is one caveat. We are not acting, the European Union is acting. The problem with the European Union regulation is it really damages the ability to innovate in economic growth. So it would be better if we did it than

them.

*Mr. Pallone. Thank you. So let me go to my last question, Ms. Gorman.

We all recognize the importance of providing Americans with access to high-speed, reliable broadband connection. Without that, students can't complete their homework, vets and seniors can't see their doctors, and some of us cannot do our job. So I want to ask you, how does ensuring that all Americans can access and adopt high-speed, reliable broadband, which is necessary to participate in today's digital economy, also strengthen America's standing as an economic power and allow us to advance our national interests?

*Mr. Gorman. Well, I think there is a moral argument and a moral imperative here, as well, to be lifting up the entire country and setting ourselves as an example to the world, particularly as talent seeks to come to the United States.

But also we are building a modern industrial strategy. We have recognized that as a national security imperative, and that strategy ought to be built from the bottom up and

the middle out, and that involves involving all of the country in this competition. We need the next generation of IT professionals, the next generation of AI professionals, the next generation of professionals across the Internet of Things. And we need to be drawing not only on the best and the brightest from a few cities, but from the entire country.

*Mr. Pallone. Well, thank you so much.

And thank you, Mr. Chairman, I yield back.

*Mr. Latta. Thank you. The gentleman yields back the balance of his time, and the chair now recognizes the gentleman from Michigan's 5th district for five minutes for questions.

*Mr. Walberg. Thank you, Mr. Chairman, and thanks to the panel.

Mr. Lewis, your testimony identifies that it is very difficult, to say the least, to decouple the United States' technology ecosystem from China completely. But there have to be significant steps we should take to minimize the risk. This includes addressing egregious cases of Chinese technology use in the United States.

When I was informed by General Motors that they are not

allowed to test autonomous vehicles in China, and we allow China to test autonomous vehicles here all across our country, that is a concern. At least seven Chinese autonomous vehicle companies are allowed to test throughout this country, gathering millions of data points, as I understand it, and giving the CCP an unprecedented vantage point into our country.

Would you consider, Mr. Lewis, this as an example where lawmakers should step in and prevent this type of technology from operating in the U.S.?

*Dr. Lewis. Thank you. One word -- when you talk to Chinese officials, one word that always makes them nervous is the word "reciprocity.'' So if we can't do it there, why can they do it here?

*Mr. Walberg. Right.

*Dr. Lewis. So yes, I do think it would be useful to step in.

*Mr. Walberg. Yes, I mean, it is ridiculous to think we don't have that reciprocity because we are fearful of not having their consumers or being able to sell our vehicles there, we can't test them. Thank you.

I am co-chair of the 5G and Beyond Caucus, and the emphasis is on "beyond.'' While 5G is still being deployed across the country, it is important that we remain wireless leaders of the world and keep looking forward. Ms. Gorman, what role does sixth-generation wireless have in our economic and national security?

And secondly, how should we demonstrate leadership in these early stages?

*Mr. Gorman. Well, it will have an enormous role in our economic and national security, because the entire Internet will be built on top of it, just like we have had for 4G and 5G. And not just the Internet in our own country, but around the world. And that is where China has really succeeded in deploying 5G throughout the developing world, throughout the Belt and Road Initiative.

So there is a clear global economic and national security imperative for the United States to lead in 5G. As we were speaking about earlier, there -- we don't have a national champion in 6G. And so what we can do is we can continue to invest in Open RAN, and I am grateful this committee has held hearings on that topic and to advance our

leadership there. We can build cybersecurity standards into the 6G standard. We can look at post-quantum cryptography, which should be a part of 6G, to make sure that we are robust against future developments in quantum computers. And we should work with our allies and partners so that we together are building the research and development and commercialization activities that are going to play into that industry-driven standard.

*Mr. Walberg. Yes, that is key, allies and partners. We don't have to be alone in it, but we have to make sure that China doesn't overcome us.

The Secure and Trusted Communication Networks Act was an important step in securing our nation's telecommunications systems, and I support Representative Stefanik's legislation to expand the language to DJI. But as we are looking to expand it, I once again voiced the need to fund rip and replace so we get the job done.

Michigan has hundreds of sites where harmful Huawei and ZTE equipment had to be removed, and now the shortfall is unmanageable, especially for our small providers.

Mr. Singleton, what national security risks do Chinese-

made drones pose, and how would including DJI on the covered equipment list address those risks?

*Mr. Singleton. DJI presents, I think, a catastrophic risk to U.S. national security. I think when you look at how the company was born out of the Chinese Government through direct investments, when you look at how it is used every day to surveil concentration camps in Xinjiang Province to monitor Uyghurs, its use on the battlefield in Russia against Ukraine, these are -- there are myriad examples in which this technology, while very advanced and I know a lot of people have DJI drones, they don't quite understand the links to China's military and how data flows can be potentially exploited down the road as China harnesses all of this data, which -- Chinese, you know, Communist Party Chairman Xi Jinping refers to data as the 21st century oil.

They don't quite understand what they are going to do with all this information, I absolutely agree with that --

*Mr. Walberg. But they will have it.

*Mr. Singleton. But they will have it. And by applying big data capability on top of it, they are preparing for a future environment where they could potentially

operationalize all of this data to further their strategic interests.

*Mr. Walberg. A hundred years war, yes. Okay, thank you.

My time has expired, I yield back.

*Mr. Latta. Thank you. The gentleman's time has expired and he yields back. The chair now recognizes the gentlelady from California's 16th district for five minutes for questions.

*Ms. Eshoo. Thank you, Chairman Latta and Ranking Member Matsui, for holding this very important hearing. And to each of the witnesses, thank you for your highly instructive testimony.

The security of our nation's networks is obviously of the utmost importance. The one thing that worked seamlessly on 9/11 was our telecommunications networks, and it is critical that they are never compromised.

Unfortunately, much of America's networks, especially in high-cost areas where connection is at a premium, were built with Huawei and ZTE equipment. This is a direct threat to our national security, and something that I have been

pointing out and working to address for over 15 years. Congress finally got its act together and passed the Secure Networks Act and the Secure Equipment Act. Now we need to fully fund rip and replace and finish the job.

Congress appropriated $1.9 billion for this effort. The applications are 5 billion, so there is a shortfall of 3.1 billion, and we need to address this. We also need to be more strategic in our efforts to respond to foreign adversaries so we aren't playing catch-up, especially when it comes to our national security.

Mr. Lewis -- and I know that other members have asked this question, but I want to circle back on it -- what does Congress need to do to ensure we aren't playing catch-up to our adversaries from a network security perspective?

And what should we be doing strategically so that the U.S. response is proactive and not reactive? And Ms. Gorman spoke to that, as well.

*Dr. Lewis. Thank you, and I would say that the work and the legislation that committee has passed previously has been very helpful in moving the ball forward while we still have a long way to go.

To the direct point, one of the targets for hacking are 911 systems. You said they worked on 9/11, they did. Other people realize that. We need to think about how we strengthen 911. Removing rip and replace has to be completed.

Anecdotally, if you look at where the networks are located, if they use Huawei equipment they are very often near sensitive U.S. facilities, either research or military.

*Ms. Eshoo. Right.

*Dr. Lewis. I don't think it is a coincidence. So rip and replace would be good. Strengthening Huawei would be good.

Some of the things we have done in this Administration have been very beneficial. So the National Cyber Security Act, the -- pardon me, the National Cyber Security Strategy, looking at how to make the industry more mature by imposing liability, by creating standards for the writing of software long term, we will need to move this industry to be -- and they are doing it on their own, but it could be done more quickly -- move it to be a more mature industry that follows standards. Near-term things like rip and replace and other

activities are also essential.

*Ms. Eshoo. Did I hear you correctly that there are Western companies that are doing business with North Korea?

*Dr. Lewis. European companies.

*Ms. Eshoo. European companies.

*Dr. Lewis. Yes.

*Ms. Eshoo. Okay, not American companies.

*Dr. Lewis. Not as far as I --

*Ms. Eshoo. I was going to say, if there are, I want to go and meet with them. And I think the whole subcommittee would want to.

Following up on this, we discussed the importance of securing our networks from foreign adversaries, and Congress has -- well, we have taken steps. You just commented on that, and other members have pressed that, as well. What is the next technology or sector we should be focusing on?

Where is the threat coming -- where is the threat going to come from next? Any one of the witnesses.

*Mr. Singleton. I would chime in on EVs and lithium ion battery supply chains, another industry where China in the 14th 5-Year Plan has made clear that it wants to dominate the

sector. It already does.

Unvetted Chinese batteries are today being installed in U.S. electrical grids across the country. Most recently members of this committee wrote to the Marine Corps and the Secretary of Defense after discovering that one of those unvetted systems, Chinese systems from a company called CATL, or C-A-T-L, had been installed at Camp Lejeune, which is the military base that is going to be responsible for launching a counter offensive in the event of a Taiwan invasion.

*Ms. Eshoo. Ms. Gorman?

*Mr. Gorman. Maybe not the next one, but one that remains a huge decider would be the advent of a fault -- universal fault tolerant quantum computer if China gets there before the United States --

*Ms. Eshoo. I didn't catch that.

*Mr. Gorman. A universal fault tolerant quantum computer, which would allow whoever develops it first to break many of our modern encryption systems, including those that our defense communications rely on.

Now, the U.S. is probably a little bit ahead of China in this, but if China gets there first, all of our military

communications will be at risk.

*Ms. Eshoo. Thank you again to the witnesses. I think, again, you have been highly instructive.

And I yield back, Mr. Chairman.

*Mr. Latta. Thank you very much. The gentlelady yields back, and the chair now recognizes the gentlelady from Washington, the chair of the full committee, for five minutes for questions.

*The Chair. Thank you, Mr. Chairman. I just kind of wanted to circle back on the same question, recognizing that in 2020 Congress passed the Secure and Trusted Communications Network Act, and that was to address the immediate threat posed by having Chinese equipment like Huawei and ZTE in our communications networks.

Now, today we are discussing several pieces of legislation to address other technological threats. And in the technology space I just wanted to give each of you a chance to speak if there is anything more you want to add as far as what you see as the greatest threat to our national security today. And I will start with Mr. Lewis.

*Dr. Lewis. Thank you. You know, the prevalence of

Chinese software and Chinese apps is sort of unrecognized. And we all know TikTok. TikTok is a potential risk. It can be mitigated, and there has been good work in Congress in moving the industry in that direction.

But I think the use of software by developed by China -- and you wouldn't necessarily know, I will give you -- I won't give you an example. Some of the biggest companies in the U.S. have Chinese software built into their apps. You don't know it, they may not even know it. And that is a potential for espionage.

*The Chair. Mr. Singleton?

*Mr. Singleton. I would chime in with facial recognition technology, where the Chinese are obviously far ahead of us. They have weaponized facial recognition technology, I think as we have mentioned here, to identify the facial features and characteristics of Uyghurs and then to inter them in concentration camps.

There are companies like Tiandy Technologies that was recently included on the U.S. export control list, but whose products you can still buy on Amazon, that develop that exact genocide-enabling artificial intelligence product, so much so

that they sold it to the IRGC last year.

I think we have to start to really think about how the Chinese intend to employ facial recognition, and it is impossible to divorce China's internal repression from its broader geopolitical aims.

*The Chair. Thank you.

Ms. Gorman?

*Mr. Gorman. I am both incredibly excited, but also incredibly fearful of the combination of AI and biotechnology, and that is an area that the U.S. absolutely has to lead on.

But where I fear that China's lax concerns about personal privacy and forced collection of data on its own citizens may propel it to global leadership, China is collecting the world's largest DNA database. In addition to some of the horrific and genocidal actions and ethnic cleansing actions that that enables, those databases could also enable the future of personalized medicine.

And so, from a national competitiveness and security risk perspective, I worry about a future where we are dependent on China for advances in therapeutics and medicines

because of this AI-driven approach.

*The Chair. Thank you.

The FCC has updated the covered list twice since publishing the initial list, following the passage of the Secure and Trusted Communications Networks Act. Those updates have largely focused on services instead of equipment.

Dr. Lewis, I wanted to ask, should Congress make changes to update and strengthen this law? And if so, how?

*Dr. Lewis. Thank you. Focusing on equipment is essential. The rip and replace funding is essential for getting Chinese equipment out of the telecom network.

Some of the measures this committee has proposed that would increase transparency into sourcing would be very helpful. Where does your software come from? Where does your equipment come from? And if you don't know, you are at risk. So I think those are the -- transparency mitigation, some of the things you have seen in the discussion about TikTok include mitigation measures-- rip and replace, there is a lot of work for you guys.

*The Chair. Thank you. As a follow-up, one of the

bills we are considering requires DJI Technologies to be added to the covered list. And, you know, while it may be a good step to address the threat, I feel like we are going to start, you know, playing whack a mole with this. So as we are considering legislation, what could be a more comprehensive solution?

*Dr. Lewis. Oh -- go ahead.

*The Chair. Yes, Dr. Lewis, or any -- does someone else want to --

*Mr. Gorman. I am happy to chime in on that one.

*The Chair. Okay, great.

*Mr. Gorman. I really think we need a comprehensive risk-based framework here. We can't de-risk and de-couple from all Chinese technology at once. And so we are going to have to make strategic choices about what is the highest-level risk, what requires dedicated action. And that is something that the Commerce Department, that other agencies across the government need to put together a more comprehensive framework so that it is not only the job of Congress to select technologies and concerning companies to flag for putting on these lists.

*The Chair. Okay, thank you --

*Dr. Lewis. Maybe to build on that, if I could, quickly?

*The Chair. Yes.

*Dr. Lewis. The transparency point remains essential. In the 5G debate we worked with our Japanese and European allies to create trust criteria: How do you identify a trusted supplier? Those should be broadened from beyond 5G to other technologies.

*The Chair. Thank you. Thank you all for being here. We appreciate your insights.

I yield back.

*Mr. Latta. Thank you. The gentlelady yields back, and the chair now recognizes the gentleman from California's 29th district for five minutes for questions.

*Mr. Cardenas. Thank you, Mr. Chairman. I appreciate the opportunity to have this discussion today, and thank you for holding this committee hearing, and also to Ranking Member Matsui. I appreciate the witnesses sharing your expertise and your opinions today, as well.

We are all living in an increasingly connected world,

and Americans rely on technology daily to participate in their workplace, pursue their educational objectives, and socializing, as well. We need to know what the communication networks that we are -- we depend on pose a risk or personal safety, or -- to our privacy and to our national security. Maintaining American global leadership is -- communications technology is critical in mitigating those risks.

Some have argued that the United States should pull back from working more closely with our allies to respond to shared threats; I believe the opposite is true. Close cooperation with global partners that share democratic values makes both the United States and the world a safer place, and hopefully will allow us to be -- further our technology and our breakthroughs when China seems to be charging forward at a rapid pace.

Mr. Lewis, President Biden included forging international partnerships as a pillar of his national cybersecurity strategy. Why is it important that we work closely with our Democratic friends around the globe to set responsible standards in cyberspace?

And what is at stake if we shy away from international

engagement in this space?

*Dr. Lewis. Thank you for the question.

I would call the committee's attention to an initiative called the Counter Ransomware Initiative, which is led by the White House. And part of the reason it is called the Counter Ransomware Initiative is if you called it the Counter China Initiative no one would show up.

So counter ransomware is a problem for all countries. And currently, 57 nations have joined this effort to share information on potential threats, to share information on ways to improve your defenses. We have discovered routinely that if you try and do this as one nation, you will be out-maneuvered.

The next step for the Counter Ransomware initiative is to think about accountability. How do you create accountability for malicious action? Right now, if you do something bad, nothing happens to you. Why would you stop? So that will be a difficult step, but it is one where foreign partners will be essential.

*Mr. Cardenas. Thank you.

We generate more data today by living our everyday lives

than ever before. And for better or worse, this data helps drive our digital economy. When available to our adversaries, massive amounts of data on American people can also be used for more nefarious purposes, including undermining faith in democracy and disrupting public health. We will be holding a major election this year in the United States, and looking at the state of our digital ecosystem I am concerned about the role that widespread mis and disinformation could play in the process.

This question is for Mr. Lewis and also Ms. Gorman. When Americans' data and communications networks are vulnerable to foreign adversaries, how can it be used against them, particularly when it comes to mis or disinformation?

*Dr. Lewis. One of the things we have seen with the ability to collect massive amounts of data and process it is it allows you to improve your messaging, right? It allows you to identify people who might be more accepting of your message. It allows you to identify themes and topics that are going to have political resonance.

In some ways, the task of the foreign influence operator is similar to the task of anyone who works in politics. You

want to figure out how to persuade people to do something different from what they were thinking. And I think the Russians have proven the ability to do this.

What is interesting and worth watching -- Iranian propaganda is still terrible, but Chinese propaganda has improved in -- since 2016. So I would say Russia and China will definitely go out of their way to interfere with the election.

*Mr. Cardenas. Thank you.

Ms. Gorman?

*Mr. Gorman. Yes, absolutely. I agree with that completely, and would add that the more we know about someone the easier they are to influence. Much in the way that the technology platforms collect massive amounts of data about us so that they can keep us engaged and keep us on the platforms, a foreign propaganda operation can do the same thing, can create divisions, can identify where particular swing districts may be vulnerable and what messages would appeal to them, either to vote for a certain candidate or even just to stay home that day from the polls.

So there is an incredible amount of vulnerability,

particularly when paired with algorithms that can selectively up-rank and down-rank content, according to objectives. And I think that is really the concern around apps like TikTok.

*Mr. Cardenas. Thank you. My time seems to be expiring. With that I yield back, thank you.

*Mr. Latta. Thank you. The gentleman's time has expired and he yields back. The chair now recognizes the gentleman from Georgia's 1st district for five minutes for questions.

*Mr. Carter. Good, thank you.

I am down here. I am in time out over here. So you all -- thank you all for being here, and this is extremely important, something that this subcommittee has been working on for quite a while and it is very, very concerned with. Obviously, this is a national security issue and an economic issue at the same time. And we have to make sure that the U.S. has the capabilities to combat both of these, all of these threats.

Mr. Lewis, let me start with you. According to 2018 CISA's analysis, the U.S. has likely lost $600 billion due to Chinese cyber espionage. Do you think that is still accurate

today? Do you think that figure is probably accurate, or do you estimate that number is higher or lower?

*Dr. Lewis. Thank you. Unfortunately, the number is considerably higher. The Chinese have made borrowing American intellectual property a cornerstone of their economic growth.

*Mr. Carter. Borrowing?

*Dr. Lewis. Well, they will give it back if you ask nicely.

[Laughter.]

*Mr. Carter. Yes, right. But obviously, it is having an economic impact on our country.

*Dr. Lewis. In many ways. First, Americans are paying for R&D that the Chinese can then get advantage of. Second, in some cases -- a good example would be Nortel. Nortel, now out of business because of this, did the research, started building the products. Chinese espionage provided it to Huawei, who put the product on the market before Nortel could. And so Nortel lost the market share.

So in terms of market competition, in terms of research and development --

*Mr. Carter. Absolutely.

*Dr. Lewis. -- we are behind.

*Mr. Carter. It is really difficult to say how much economically that it has impacted us.

*Dr. Lewis. We have done a number of surveys, and other people have, as well. And it suggests that the global cost is now in the billions of dollars. A good rule of thumb is it is roughly equivalent to the narcotics trade. Still less, but roughly equivalent.

*Mr. Carter. Wow. Ms. Gorman, as you know, the countering CCP Drones Act would place DJI Technologies on the FCC's covered list. Agencies such as the FBI and CISA have built a substantial record for this ban. However, it takes a lot of time to do that and a lot of resources.

How should Congress -- how should we approach building records for other companies with CCP connections that have equipment and critical infrastructures?

*Mr. Gorman. Well, thank you for the question. I think we need to start by developing a framework for what we are really, really concerned about. And there could be many dimensions of this.

In the case of DJI, one element of it is the data collection capacity. So we need to start by laying out what are the risks that we are really worried about, and then look at industries to build those records where there are companies that clearly have a market dominant position that are violating some of these principles we are talking about, and we need a better analytical capacity across the Federal government to do that, as well.

*Mr. Carter. Fair enough, thank you.

Mr. Lewis, back to you. We know that China hackers take advantage of almost every vulnerability throughout the Internet infrastructure. If certain routers have known vulnerabilities, how does this undermine security measures of other vendors, such as hosting services or ISPs that are used to prevent unwarranted attacks?

*Dr. Lewis. Yes, our opponents in espionage are both inventive and well-resourced, and so there has recently been a series of hacks where the target of the intended hack is pretty good at defending itself, but the people who work there and their small office or home office routers and equipment may not be as well defended. So it is a useful

avenue to get into the target. I may not be able to get into your office, but there is a fair chance I can get into your basement, and that is the risk.

*Mr. Carter. Great. Mr. Singleton, we know that the Chinese collect all sorts of data, including biometric data, which is concerning. I remember that when I first got here one of the things that I learned is that some of these agents, some of these heredity agents, programs, whatever, that they get this information, and that some of them are owned by Chinese companies. What can they do with that kind of information, do you think?

*Mr. Singleton. Millions of Americans have had their DNA sequenced by certain other American companies, you know, the DNA gets sequenced back in mainland China, and the American consumer isn't even aware that their genomic data has been transferred to DNA banks in China.

The People's Liberation Army plays a key role in China's genomic research and its genomic bank. BGI, another well-known Chinese biotechnology company with links to the People's Liberation Army, also is at the forefront of thinking about research that could support the PLA's -- and

it almost sounds like a joke, but it is real -- the super soldier program that they have talked about and written about extensively, the development of targeted viruses that can target particular DNA receptors of other ethnicities.

I just don't think we fully understand and grasp how the biotechnology sector is going to impact our everyday lives in ways that are both good and potentially malign. The concern, again, is that BGI is the market champion.

*Mr. Carter. Great. Thank you all for being here.

And I will yield back.

*Mr. Latta. Thank you. The gentleman yields back, and the chair now recognizes the gentlelady from Michigan's 12th district for five minutes for questions.

*Mrs. Dingell. Thank you, Mr. Chair.

Today we are discussing various pieces of legislation aimed at addressing risks in our communication technology networks, and I believe it is absolutely critical to continue collaborating with my colleagues on both sides to tackle these issues and thwart future threats.

From critical infrastructure to 5G to supply chains and emerging technologies in the automotive center -- sector,

addressing these concerns is necessary to foster competition, drive innovation, support our domestic industry, and safeguard our data. Congress must prioritize its responsibility to secure our networks to shield all Americans from current and future threats.

Urgent action is needed to remove Chinese equipment from America's networks. However, the FCC is facing challenges in its effort to rip and replace Chinese equipment from our networks. There are significant funding shortfalls in the FCC's rip and replace program, and although Congress allocated 1.9 billion for the program, the FCC has approved reimbursements exceeding double that amount, resulting in more than a $3 billion deficit.

According to data released and made public by Ranking Member Matsui, Michigan received $14 million in rip and replace funds, but this data shows that Michigan needs more than 56 million to get all the Chinese equipment out of our networks. That is a $42 million deficit just in my state of Michigan, a quarter of the funds needed to help secure Michigan networks.

Mr. Lewis, how important is it for Congress to ensure we

remove all Chinese equipment from our networks and prioritize funding FCC's Secure and Trusted Communication Network's reimbursement program?

*Dr. Lewis. Thank you for the question.

One question I asked some of my colleagues is why do you think the Chinese subsidized the placement of telecommunications infrastructure and hardware in networks around the world and in the U.S.?

And it is as admirable as people might be. It is not because they love you, it is because it gives them a signals intelligence advantage. And for that reason we have to complete this.

And we have talked earlier about the fact that many of these networks are around sensitive areas. This is a huge potential risk.

*Mrs. Dingell. Thank you.

Ms. Gorman, how might these funding delays impact the security of U.S. telecommunication networks and our ability to lead in this sector?

*Mr. Gorman. Every day we keep this equipment in our networks is another day that these networks are vulnerable.

And it is not only about the personal data, it is also -- and data that is potentially near sensitive sites, it is also about our business data. That is also at risk. We have these, you know, multi-hundred-billion-dollar loss due to intellectual property theft. That remains a vulnerability, too.

So to our future competitiveness, as well as our present cybersecurity, this really needs to be addressed.

*Mrs. Dingell. Thank you. As a co-chair of the congressional 5G and Beyond Caucus, we need to ensure we play a strong role in leading on wireless standards and enabling advanced wireless technologies, both domestically and internationally.

Today we are discussing Ranking Member Matsui's Future Uses of Technology Upholding Reliable and Enhancing, otherwise known as FUTURE, Networks Act, which would establish a 6G task force essential for competing against China, securing our supply chains, and facilitating faster and more cost-effective deployment of services.

Ms. Gorman, can you talk about the importance both here and abroad of starting now to plan and invest in the future

of advanced wireless technologies such as 6G?

*Mr. Gorman. Well, not only do we need to start now, we really needed to start yesterday. The 6G standards development process has been ongoing for a couple of years now. These things take an enormous amount of time to plan, often on a decade-long delay between when the standard gets developed and when it is implemented in the world, as we are seeing with 5G.

And our leadership and the leadership of our allies and partners is so critical because this connected future Internet advantages in one layer, the foundational layer, create advantages on all the application layers: the artificial intelligence systems, the facial recognition that are building out on top of that layer. And China is building this out throughout the Belt and Road Initiative, propping up autocratic regimes with safe city programs that purport to be able to predict crime and arrest people before it happens.

So this is a huge compromise to our democratic values, both at home and globally, if we allow our innovation advantages to atrophy and allow China to win the day on 6G.

*Mrs. Dingell. Thank you.

Thank you, Mr. Chair, for holding this hearing. And we have really got to work together. Our goal needs to be to take steps to safeguard our constituents and our businesses for future cybersecurity attacks and risks.

I yield back, Mr. Chairman.

*Mr. Latta. The gentlelady yields back, and the chair now recognizes the gentleman from Utah for five minutes for questions.

*Mr. Curtis. Thank you, Mr. Chairman and Ranking Member.

And to our witnesses, I am impressed as I have listened to my colleagues and to your testimonies today of your expertise. And I am pleased that you are here with us.

This is an important hearing, securing our networks and the networks of our allies from China and Russia. I am especially pleased to -- by the Promote Secure Connectivity to Taiwan Act to ensure resilient layers of telecommunication networks to Taiwan.

Last March China cut cables connecting the small Taiwanese island of Matsu, and the 13,000 residents of this island went without Internet for almost 2 months. At the

same time, NATO has been warning that Russia may sabotage undersea cables in Europe. In response I was able to put language in the recent NDAA signed into law in December asking for an assessment of our ability to repair the cables of our allies if China and Russia simultaneously cut them in Europe and Asia.

This is one of many measures I have passed into law supporting Taiwan and pushing back against China's aggression. And for my work I have an arrest warrant in Hong Kong to show for it, which I am proud of. I mention this just to highlight the difference between our system of democracy and the CCP: we stand with our friends and allies. China threatens arrest to try to threaten and coerce.

Mr. Singleton, as we think through how to secure our networks and the networks of our allies in Europe and the Pacific, what capabilities do our adversaries have that we should be -- that we should take into consideration to build resiliency for?

For example, what capabilities in space and cyberspace, at sea, et cetera, that can be used to disrupt communications.

*Mr. Singleton. We often talk about the lessons that we are learning here, but I often think of Taiwan actually as a -- as the pilot for many of -- at least China's hacking and sort of offensive cyber operations against communication networks, underwater sea cables. And so what occurs there we often see beta tested in other parts of the world, as well. And so I think there is actually a lot that we can learn from Taiwan. And we are strengthening cooperation and collaboration with the Taiwanese authorities, and this is key.

I think we have to continuously expand the list of sectors that we define as critical. You mentioned space being the -- I think probably one of those next frontiers, the recent news about how Russia is examining and perhaps considering putting a nuclear weapon in space.

I think we do have to just understand that there is an interconnected layer to interoperability across these system structures and sectors. And so we do -- we are forced, I think, through our congressional committees, to work across jurisdictionally. And I think that really -- building out those lines of communication and effort across committees

where there is overlapping interests is really essential.

*Mr. Curtis. Excellent, thank you.

Anything from the other witnesses?

*Dr. Lewis. We can learn from the experience of Ukraine. The Ukrainians did a remarkable job in defending themselves against massive Russian cyber attacks accompanied by kinetic attacks. So some of the Ukraine lessons -- cloud use LEO satellites, and everyone knows about Starlink. Harden your networks before the conflict, and then develop partnerships that will allow you to respond quickly in the event of an attack. So the Ukrainian experience is something that Taiwan could usefully copy.

*Mr. Curtis. Thank you, a great comment.

I would like to just add my voice to that of my colleagues of the urgency of this issue. And with that, Mr. Chairman, I yield back.

*Mr. Latta. Thank you. The gentleman yields back the balance of his time. The chair now recognizes the gentlelady from New York's 9th district for five minutes for questions.

*Ms. Clarke. Thank you very much, Mr. Chairman. Good morning. And to our Ranking Member Matsui, thank you for

holding this hearing. And I would like to thank our witnesses for joining us today.

The growth of our national communications sector has been a major source of economic strength, and its continued evolution must be tended to, safeguarded from threats both foreign and domestic. The advancements in communications technology are undoubtedly exciting, and have the potential to bring innumerable benefits to consumers.

However, I would be remiss if I did not take a moment to note that it will all be for naught if millions of Americans are not able to access these benefits. That is why it is so crucial that we not backslide in our efforts to bridge the digital divide by letting funding lapse for crucial programs like the Affordable Connectivity Program, or ACP.

The ACP has made it possible for nearly 23 million American households to access high-speed broadband and, without action, this program may run out of funding in April of this year. For that reason I urge my colleagues to cosponsor my bill, H.R. 6929, the ACP Extension Act, which would provide the $7 billion in funding needed to ensure the ACP can continue its operations through the end of 2024 while

we in Congress hash out a sustainable, long-term funding solution for this essential program that has widespread bipartisan support on and off the Hill.

As technology continues to evolve and the collective network of connected devices grows, so too do the threats to things like servers, cloud services, IoT devices, and the full range of network components. And I am proud of the work this committee has done to secure our network from threats, particularly our work on the Secure and Trusted Communications Networks Act and the Secure Equipment Act. The FCC has done great work in implementing these bills, and we must take care to provide the funding needed to fulfill our mission and to keep our networks secure.

We, as policy-makers, must also ensure that we are providing the authorities and necessary regulatory landscape to prevent, detect, and respond to the wide range of threats our networks face.

Mr. Lewis, in your testimony you mentioned some of the potential harms of foreign open source software and legacy code, and discussed creating disclosure or reporting mechanisms as a logical first step to combat these harms.

Can you expound on that a bit, and speak to how the reporting of cyber incidents, regulatory harmonization can help us keep pace with the range of threats our networks face today?

And other interested witnesses may also respond. Thank you.

*Dr. Lewis. Certainly. One of the things that has been a challenge, really, for about the last decade is that we began by thinking of cybersecurity as a voluntary action, that people would do it out of self interest. That didn't work. We created a number of incomplete and disconnected regulatory initiatives and subsidies. Not a bad start. But coming together with a comprehensive strategy like the one laid out in the national strategy would improve our defenses.

So we need to think of this as -- it is a very complicated environment, but in general, the things we did at the dawn of the Internet to get the thing off the ground -- no taxes, section 230, other things -- light regulatory touch was the motto of the day -- we now need to reconsider that for defensive purposes, for national security purposes. It doesn't mean heavy regulation, but it means putting something together.

*Ms. Clarke. Very well.

Any other comments?

*Mr. Gorman. I would just add that, yes, we absolutely need to do a better job of removing it only from the responsibility of the individual, the implementer, when it comes to ensuring our nation's cybersecurity. So what that means, providing incentives, providing requirements, and taking this off the goodwill of actors that have not been able to, on their own, create enough security.

And also, I think it is also about building into the next generation of the Internet. The Internet, as designed, was not designed with security in mind. It is a very trusting series of protocols. I think we have to have maybe a slight bit of less trust the next go around, and bake in some of those security principles.

*Ms. Clarke. Very well.

Mr. Chairman, I have nine seconds. I am going to yield them back. Thank you.

*Mr. Latta. Thank you. The gentlelady yields back, and the chair now recognizes the gentleman from Texas's 14th district for five minutes for questions.

*Mr. Weber. Thank you, Mr. Chairman. We have got a lot of interest, obviously, in the counter-espionage law of 2014 and the 2017 National Intelligence Law.

Mr. Singleton, I want to come to you. Of the two CCP intelligence laws we have just talked about, in your mind which actually poses the greatest concern?

*Mr. Singleton. Well, I think the Chinese Communist Party, their grip on industry is really multi-faceted. You mentioned several bills and several laws.

The 2017 national security law is sort of the paramount example. It is notable because it mandates that all organizations and all citizens have to cooperate with state intelligence efforts. And the key challenge is the law's broad scope. It doesn't limit the obligation to support intelligence work within China's borders. It applies in an extraterritorial basis, as well.

The 2016 cybersecurity law is also pretty frightening, because it requires all network operators to furnish technical support to public -- Chinese public security organs. The recently updated counter espionage law is another great example.

The Chinese have built this overlapping network and framework of new laws, partnered with deeper party-state penetration throughout China's ostensible private sector such that I think it is pretty difficult these days to even say that there is such a thing as a private Chinese company.

*Mr. Weber. Is that -- Mr. Lewis, I am going to ask the same questions to you. Do you agree with that assessment?

*Dr. Lewis. I do, unfortunately. The Xi Jinping era has seen a gradual extension of the central government's control over the economy and over the population. So that means that -- we, in some ways, encourage the Chinese. It is sort of ironic now to formalize and adopt laws to -- similar to FISA to regulate how they conduct intelligence operations.

*Mr. Weber. Oh, nothing is similar to FISA. Did I say that out loud?

*Dr. Lewis. The Chinese used to do this out of their hip pocket, and we said, you know, you should build it into a structure of laws. And unfortunately, they took us at their [sic] word, and now have probably the most extensive surveillance system in the world.

*Mr. Weber. Ms. Gorman, your thoughts?

*Mr. Gorman. Yes, I agree with what has been said, and I think this stems from the fact that this is an autocratic regime. This isn't a democracy. There isn't a separation between the public and the private sectors. Ultimately, all private companies are accountable to the state and the state security enterprise. So that is what we are talking about.

You know, there is no probable cause. There is no independent judiciary when it comes to this kind of data.

*Mr. Weber. You said -- Ms. Gorman, I am going to stick with you for a minute, if I may. You said earlier that your fear was that the Chinese would get a quantum computer to erase -- then I missed the last part. Erase what? What were those? Reiterate those comments for us.

*Mr. Gorman. Yes, thanks. That is right, the -- we are -- many of these technology areas I think can be conceived of as a race. Probably fewer are -- few are as dire as the race to build a quantum computer, because these computers, a universal quantum computer, would allow whoever has it to break the basis of our modern encryption communications.

Right now the military encrypts all its communications. We have secure networks. You know, we have JWICs and our

secure systems. A quantum computer would allow us to break the mathematics that form the foundation of those encrypted communications, and so putting all of our communications at risk.

*Mr. Weber. Does AI have that same capability, or does it just not compare with quantum computing in that regard?

*Mr. Gorman. There are different capabilities. You know, AI is already supercharging cyber intruders' ability to create realistic spear phishing campaigns, to spoof websites, to spoof emails, to create emails in foreign languages, especially with generative AI, that seem really realistic. So AI is definitely supercharging the cybersecurity risk, but it is a different class of risk, I think, from a quantum computer.

*Mr. Weber. Any other countries, to your knowledge, that are even close to the kind of progress on the quantum computers China is making?

*Mr. Gorman. Well, the United States is probably leading -- I think is still ahead. So that is a good sign. But it is not a lead we can take for granted.

We also have strong allies and partners working on

quantum information and communications in Australia, some of our European allies and partners. So we have a strong basis to build off of here. We just can't take our eye off the prize.

*Mr. Weber. Are you concerned that China can hack into those systems and derive the benefits?

I think the gentleman down on the far left here says that they might give that property back if we ask nicely, but are you concerned they will hack into those other countries and get information?

*Mr. Gorman. Absolutely. I would be very surprised if those programs weren't targets of Chinese intelligence services and espionage.

*Mr. Weber. Okay. Thank you, Mr. Chairman, I yield back.

*Mr. Latta. Thank you. The gentleman yields back, and the chair now recognizes the gentlelady from Illinois' 2nd district for five minutes for questions.

*Ms. Kelly. Thank you, Chair Latta and Ranking Member Matsui, for holding this morning's hearings. I also want to thank the witnesses for their testimony.

As a member representing a district with over 2,000 farms, I find the cybersecurity vulnerabilities on our wireless networks to be troubling because our agricultural producers increasingly rely on wireless networks for monitoring their soil, crop growth, weather conditions, and operating equipment. In many cases, it is small companies of a few thousand subscribers serving these farms.

These small networks often have difficulty getting access to capital to upgrade their networks. For example, in their last upgrade cycle many bought equipment from Huawei and ZTE at severely discounted rates. Fortunately, we set up the rip and replace program to remove that untrusted equipment. But as my colleague last pointed out, there is -- well, she talked about Michigan, but there is a $3 billion funding gap. And I am not -- and I am worried that many of these companies are at risk of not being able to upgrade their network equipment.

Another network security issue involves Internet routing, specifically the Border Gateway Protocol, BGP, which, as you know, enables the Internet to exchange routing information between a sender and a receiver. This is an

essential function as it helps ensure Internet traffic arrives at its intended destination.

Ms. Gorman, first, can you please explain how our foreign adversaries could exploit BGP vulnerabilities?

*Mr. Gorman. Thank you for the question.

BGP, the Border Gateway Protocol, is the routing protocol of the Internet. If the Internet is a series of connected highways, the BGP are the road signs telling information or drivers where to go.

In a BGP hijacking attack, a malicious actor will spoof the addresses from a known address to reroute the traffic from where it was intended to go to where -- to itself. And so we already have examples, you know, numerous examples of malicious actors using this -- these attacks. Russian attackers in 2018 rerouted traffic from a cryptocurrency site to create a scam where they were able to pocket about $150,000 by rerouting traffic to them. The Pakistani Government back in 2008 actually also had an inadvertent BGP hijacking attack when it was attempting to censor YouTube, and ended up rerouting all traffic to YouTube to the Pakistan Telecom Company.

So these are challenging to get ahead of. The best we can do is kind of monitor them. But because the Internet, as I mentioned, is based on a very trusting protocol, anyone who owns one of these systems can spoof an IP address and try to reroute traffic from its intended destination to a malicious actor.

*Ms. Kelly. Well, my follow-up was going to be what can government do to help support industry-led efforts for BGP routing security and continued improvements. It sounds kind of dire.

*Mr. Gorman. Yes, it is definitely not the easiest cybersecurity problem out there. We don't have too many great tools, but certainly increasing our efforts to monitor where Internet traffic is going so that we can quickly detect when one of these hijacking attempts is taking place; there are things we can do around IP prefix filtering to better assess out, you know, understanding when there is a degraded network performance to respond; and building in that layer of security to future protocols, as well.

I was pleased to see that the FCC and CISA are holding workshops about BGP security, and there is also some

interesting work being done in the IETF, the Internet Engineering Task Force, another standards body, on more secure BGP protocols.

So I think it is about changing the mindset a little bit of the Internet, not too much, but to bake in some of those security principles in future iterations.

*Ms. Kelly. Thank you so much.

And I yield back.

*Mr. Latta. Thank you. The gentlelady yields back, and the chair now recognizes the gentleman from Idaho's 1st district for five minutes for questions.

*Mr. Fulcher. Thank you, Mr. Chairman. I have got a question for Mr. Lewis, but I need to set it up first.

In January the UK's National Cyber Security Center, the Five Eyes intelligence network, and the FBI warned about a Chinese hacking group known as Volt Typhoon that attacks older Wi-Fi routers and homes and small businesses. And the hackers drop in malware that cuts off or prepares for thousands of homes or small businesses to be cut off from power and water. That malware can infect other machines as it infects that router, as well.

So my question is to you, given that backdrop, what kinds of threats should we be considering here?

And could those be the kinds of attacks designed to create problems with various parts of U.S. power and water infrastructure?

*Dr. Lewis. It has become clear that in recent years China has begun to target U.S. critical infrastructure: water, pipelines, electricity. Telecom networks are hard, but there are efforts: logistics, railroads, airports. And when you look at the varying levels of security at these different entities, one useful option is perhaps not to go after the company, but to go after its employees using their home equipment, or to go after their subcontractors who might be smaller.

And so small office, home office routers and equipment is a useful avenue for our adversaries to gain access to their primary target.

*Mr. Fulcher. In particular, older equipment?

*Dr. Lewis. Say it again.

*Mr. Fulcher. And particularly older equipment, more vulnerable?

*Dr. Lewis. Older equipment is vulnerable. At this point I don't know if we would want to take a bet, but if it is more than three years old you probably should be nervous.

*Mr. Fulcher. I am nervous.

[Laughter.]

*Mr. Fulcher. Mr. Singleton, this is in regard to China's national security law, which is something I think you probably have good familiarity with. Could China use that national security law to hack Americans or Taiwanese or Hong Kong backgrounds to disrupt them financially, or even coerce their businesses that -- into ending up supporting Hong Kong, Taiwan, or even to get them to stop raising the issue of violation of human rights? Do you see that as a vulnerability there?

*Mr. Singleton. Absolutely. The key challenge is that the 2017 law has no end. There -- the scope is nearly boundless. And so China doesn't simply execute and institute these laws and other regulations thinking about the confines of its own border, it is thinking about how they can project those same rules, regulations, and authorities beyond its borders.

And so China already considers Hong Kong part of mainland China. The rules of the mainland apply in Hong Kong now. And so I think the key that we have to remember is that there are global implications to these laws beyond simply what occurs inside China's official borders.

*Mr. Fulcher. Okay, thank you for that. Again, I am still not comfortable.

Back to Mr. Lewis on that same general topic. Given Russia has been operating closely with China, do you see Russia as trying to be a similar type of disrupter in all this? And, look, for example, like getting into the EU or U.S. company data -- again, through that older equipment, perhaps more vulnerable. Comments on that?

*Dr. Lewis. Russia is, in some ways, more aggressive than China. And in some cases they are more skilled. And we know they have explored U.S. and European critical infrastructure for identifying vulnerabilities that they could use to disrupt. So I think Russia is an equal threat in this area to China.

*Mr. Fulcher. Thank you.

Mr. Chairman, I think we have got our -- definitely, our

work cut out for us. The other questions that I have been interested in have been asked by other members, so I yield back.

*Mr. Latta. Thank you. The gentleman yields back the balance of his time. The chair now recognizes the gentleman from Ohio's 12th district for five minutes.

Oh, I am sorry, I am sorry, I got ahead of myself. I apologize to the gentlelady from Texas -- for five minutes for questions.

*Mrs. Fletcher. Well, thank you so much, Chairman Latta, and I really appreciate you convening this hearing today. It is a timely hearing, as I think we all know, and this has been a really useful panel.

So thank you, Mr. Lewis, Mr. Singleton, and Ms. Gorman for your testimony this morning.

You know, it is really important for us to understand the threats that our communications networks face from foreign adversaries. And our reliance on the Internet and connected devices opens all of us up. I think the conversation that we were just having, Mr. Lewis talking about the threats to our critical infrastructure, also

thinking about the threats to our devices as individuals in our households, in our businesses big and small, these are really crucial issues. So I want to talk about a couple of things and drill down on a couple of things that have already been raised this morning, but I think are important.

Ms. Gorman, in your testimony you noted the development of Open RAN as a way to combat the use of untrusted equipment from Chinese providers in American networks. And last month we had a hearing on Open RAN in this committee, and we discussed some of the benefits, including greater network security. But I think it is kind of counterintuitive for a lot of folks that shifting from sort of end-to-end networks that have proprietary features to more of an open network would make that network more secure.

And so could you just take a minute to talk and maybe tell us a little bit about how Open RAN leads to more secure wireless systems, particularly in the context of our foreign adversaries?

*Mr. Gorman. Yes, thanks for the question. And I agree, it is a little counterintuitive, and perhaps also has some nuance.

But I think the conversation around Open RAN really took flight about four or five years ago. We were going overseas and trying to convince our allies and partners to rip out Huawei from their networks, to not choose Huawei to build their next generation, their 5G networks. And they would come back to us and say, "Well, what should we use instead?''

And we weren't selling a U.S. alternative because the equipment market is dominated by three or four players. We would say, "There is Ericsson, there is Nokia, maybe Samsung,'' but there wasn't a cost-competitive alternative to Huawei. And that is fine in some of the richest countries in the world. We can maybe afford to do this kind of rip and replace project. That is incredibly costly, as you know. In much of the world, that really isn't a choice.

So the Open RAN movement was really born out of a desire to provide some kind of alternative to Huawei in a shorter time-scale than would be required to build a competitive telecom giant like Huawei, which took over 20 years to build. And so that is why, from the security perspective, Open RAN helps break up that market that is dominated by three players, one of which is able to sell at much, much more

cost-competitive prices, in part due to espionage, in part due to significant state subsidies, for geopolitical reasons.

Now, we do need to do more to make sure that these open, interconnected architectures, where you can change one piece for another, you don't have this vendor lock-in, do actually still have cybersecurity baked into it. So from the foreign adversary perspective, we are not buying Chinese equipment, but if we don't build in strong cybersecurity protections, particularly at the points of connection of these interchangeable pieces, then those systems will remain vulnerable.

*Mrs. Fletcher. Thank you so much.

Mr. Singleton, you also talk about Open RAN in your testimony, and I am just hoping you can share with us your recommendations on countering this influence and ensuring that we are establishing Open RAN standards that don't give foreign adversaries a strategic advantage.

*Mr. Singleton. Thank you. I mean, O-RAN holds tremendous promise, although it doesn't necessarily increase network security.

I think it is important to remember that China's biggest

slab of tech R&D muscle have gained entry into, really, the design room of the technology touted as a Huawei substitute. Today thousands of Chinese software developers are contributing to the direct development of software dependencies in these applications that are being used in our critical infrastructure, thousands of Chinese software developers.

The complexity of RAN code provides multiple options for back doors, not only in a single piece of code, but also in combination of it. So it is really unrealistic to expect us to be able to constantly review this code provided by all the participants in the Open RAN software community. A lot of experts more well versed in this say it is impossible.

But I think we have to remember that the collective development of code requires a high degree of trust. And given that several of the Chinese members of organizations like the O-RAN Alliance and the Linux Foundation are less trustworthy than even Huawei, the initiative carries huge risks.

I think it is really incumbent upon Congress to have very serious scrutiny of the role of the Linux Foundation, O-

RAN Alliance, and others developing this next generation of software code. I think additional investigations into those issues and those relationships is warranted.

*Mrs. Fletcher. Thank you so much, and I have run out of time for my last question, so I will submit it for the record and yield back.

[The information follows:]

**********COMMITTEE INSERT**********

*Mrs. Fletcher. Thank you so much, Chairman Latta.

*Mr. Latta. Thank you very much. The gentlelady's time has expired, and she yields back, and the chair now recognizes the gentleman from Georgia's 12th district for five minutes for questions.

*Mr. Allen. Thank you, Chair Latta, for convening this hearing, and I want to thank our witnesses for being here today.

Since I have been in Congress I have come to understand the problem of Chinese espionage is staggering, particularly since the passage of China's 2017 National Intelligence Act. Every single Chinese company is an asset of China's national intelligence network, no matter where they operate.

I am currently considering a draft piece of legislation that would add foreign advisory Internet of Things module producers to the FCC's covered list through this piece of legislation. Although it has not been introduced, it is in the draft phase. Mr. chairman, I would like to submit this draft legislation for the record.

*Mr. Latta. Without objection, so ordered.

[The information follows:]

2520

2521 **********COMMITTEE INSERT**********

2522

*Mr. Allen. Thank you.

Mr. Lewis, could you explain the risk we face if we allow foreign adversary-produced Internet of Things modules to continue to be integrated into our systems?

*Dr. Lewis. There are two general risks.

The first is that the Internet of Things provides you access to the larger telecommunications network. And so, as we have been talking about with routers and home office equipment, that may not be the most important piece, but you get your foot in the door and you can go into the larger networks.

The second piece is that it would create new opportunities for espionage by the immense amounts of data that the Internet of Things would create. And most people know now that your car is sort of a rolling computer --

*Mr. Allen. Right.

*Dr. Lewis. -- It is wirelessly connected. Very often the connections are made by Chinese companies. Certainly, if you are driving a European car, it has got Chinese connectivity.

*Mr. Allen. Right.

*Dr. Lewis. So you will be generating huge amounts of data that these data analytic tools, artificial intelligence can analyze for intelligence benefit.

*Mr. Allen. Yes, I learned in conference that Google can -- knows where I have been and how fast I drove to get there. And so probably the Chinese know it, as well.

Mr. Lewis, how at risk are Taiwan's communication networks?

*Dr. Lewis. Well, Taiwan is, of course, the principal target for a lot of Chinese activities because of the Chinese Government's belief that it has some ownership over Taiwan. The target priorities for China are, first, its own population; second, the United States; and then I would say third, Taiwan. So that level of attention, that level of penetration by the Chinese intelligence service means that Taiwan is at considerable risk.

*Mr. Allen. Good, thank you.

Ms. Gorman, could you please provide an overview of the undersea cable network?

*Mr. Gorman. Specifically in Taiwan, Taiwan is served by 16 undersea cables. We have had reports of some of them

being cut, potentially by Chinese ships about a year ago, and this is how the island receives its Internet. There are four cables that connect to -- that connect Taiwan directly to the United States, a number of indirect connections.

But I think what is concerning is that many of these cables are owned by a multiple consortia of stakeholders from around the world and from around the places that they are connecting. Most of Taiwan's submarine cables do have ownership from Chinese telecom providers: China Mobile, China Telecom, China Unicom. So in an event of a Taiwan crisis scenario, I believe they would be at risk.

*Mr. Allen. Okay. And so the vulnerability there is that the Chinese Communist Party would cut these lines and cut that service out?

*Mr. Gorman. That is certainly a risk, and that the population would lose its access to the Internet --

*Mr. Allen. Right.

*Mr. Gorman. -- when that happened, when the Matsu cable was --

*Mr. Allen. So what security measures should we take to enhance the -- and, you know, provide protection for these

cables against these potential threats and disruptions?

*Mr. Gorman. Two things. One, we can have more streamlined and better monitoring of when these cables might be under risk of being cut around the cable, and better action to restore them and repair them. You can repair these things, but it is extremely expensive to do so. Better, cheaper ways, quicker ways of repairing it to get the Internet back online faster.

And then we also need to be looking in -- and Taiwan is looking -- into backstops. Right now, the backstop that has been proposed has just an incredible amount of latency. It can take hours to send a text message. So satellite communications, low Earth orbit constellations, Starlink-esque communications networks, I think, Taiwan is certainly looking to, especially given how they have played out in Ukraine.

*Mr. Allen. Okay. Well, thank you.

And, Mr. Chairman, I yield back.

*Mr. Latta. Thank you. The gentleman yields back, and the chair now recognizes the gentleman from Ohio's 12th district for five minutes for questions.

*Mr. Balderson. Thank you, Mr. Chairman.

Thank you all for being here today. For the witnesses, there is no doubt that we must secure our nation's communication networks. Whether it is fully funding rip and replace or addressing concerns about Chinese equipment being used in IoT and other devices across the nation, we need to ensure our -- ensure bad actors aren't accessing our networks.

I commend the chairman for allowing discussion on the ROUTERS Act. This bill directs NTIA to conduct a study of the national security risks posed by routers and modems manufactured by adversary countries. Last month this committee held a hearing on cybersecurity, where I posed a question about the national security implications of IoT devices using Chinese made cellular modules to connect our networks.

I know Mr. Allen addressed this issue, but I would like to follow up on this topic, so my first question is for any of the witnesses: Do you think it would be beneficial for NTIA to, along with routers and modems, study the national security risks posed by IoT devices that use Chinese-made

cellular modules to connect to networks?

*Dr. Lewis. I will go.

*Mr. Balderson. Yes, sir.

*Dr. Lewis. I am just going to --

*Mr. Balderson. Go ahead, Mr. Lewis.

*Dr. Lewis. -- answer yes.

*Mr. Balderson. Thank you.

*Mr. Singleton. I would agree. I mean, the threat from Chinese cellular modules is far greater, in my view, and more systemic than the danger posed by individual Chinese companies or even a Chinese sector.

You have to remember that these modules are small components embedded in other equipment or devices, and their goal is, right, to establish internet connections across mobile networks so you can move laterally across networks. And so they transmit, they receive, the process vast amounts of information. The Chinese are very keen to establish a market dominance, if not a monopoly in this sector.

But unfortunately, you can send through -- covertly through software updates which are, frankly, too numerous and too frequent to monitor individually over the lifetime of a

device -- hostile malware, and take over some of these systems and networks. So I think it is an incredibly important issue, and Congress should most certainly investigate it more.

*Mr. Balderson. Thank you, Mr. Singleton.

Ms. Gorman?

*Mr. Gorman. I would add my agreement.

*Mr. Balderson. I am sorry. Say that again, ma'am.

*Mr. Gorman. I would add my agreement.

*Mr. Balderson. Okay, thank you.

I would argue that an important part of shoring up any national security risks would be to ensure that the networks of our close allies are secure, and that we counter China's growing influence in this space. We have seen our ally, Taiwan, lose 2 undersea cables that disconnected 14,000 people. The Promote Secure Connectivity to Taiwan Act would counter China's ability to isolate Taiwan.

In addition to sabotage, we know that China can use these undersea cables for espionage. China is currently working on its Pakistan and East Africa Connecting Europe, or PEACE cable. This cable will be 15,000 kilometers long,

connecting several continents, adding to the vast networks of undersea cables controlled by Chinese entities. With the control of these cables, China can control the flow of information, intercept sensitive information at cable landing stations.

This question is also for all the witnesses, but I would like to start with Ms. Gorman, since you touched on this in your testimony: What can we do to ensure that China does not take the lead on constructing undersea cables, giving them vast control over global communication networks?

*Mr. Gorman. We really should be treating -- and I think we are starting to treat -- undersea cables much in the way that we do 5G and 6G internet infrastructure, because they are a foundational layer technology. The amount of information that is potentially accessible from them is enormous. And so I think we need to start and increase our strategic investments, particularly for some of these new projects.

We have had some success. There is the SEA-ME-WE 6 cable, where we have been able to kind of push the Chinese provider out of ownership of that cable. And so much in the

way that the Development Finance Corporation is trying to subsidize approaches that would exclude Huawei from 5G networks globally, we should be doing the exact same thing with the construction of new undersea cable projects.

*Mr. Balderson. Okay, thank you very much.

Mr. Singleton -- and we are down to 25 seconds, sir.

*Mr. Singleton. I would absolutely agree. I mean, we actually have to show up. There are bids and tenders that are submitted around the world for these vital underwater sea cable projects, and often U.S. companies aren't bidding, or we are severely underbid by Chinese competitors.

I think eventually we are going to have to get to a point where we -- I think, to Lindsay's point -- think about this as crowdsourcing and burden-sharing opportunities, pulling in private-sector leaders and tapping into U.S. capital markets to offer competitive bids and safer bids to countries that want to consider landing sites, or tapping into Chinese undersea or submarine cables.

*Mr. Balderson. Okay, Mr. Lewis, I have to pause. I am over time already, so I apologize.

*Dr. Lewis. Let me just add a quick point. Undersea

cables are not defensible.

*Mr. Balderson. Okay.

*Dr. Lewis. So you need to think of redundancy.

*Mr. Balderson. That is a great response. Thank you.

*Mr. Latta. The gentleman yields back. The chair now recognizes the gentleman from Pennsylvania's 13th district for five minutes for questions.

*Mr. Joyce. Thank you, Chair Latta and Ranking Member Matsui, for putting together today's hearing. And thanks to our witnesses for giving your time to be here.

Every day, down to this minute, the Chinese Communist Party and other foreign adversaries are looking for ways to manipulate our communication networks and to gain access to a plethora of valuable information. This committee has taken great steps toward combating these threats through legislation that is being presented in this hearing, and I appreciate the attention given to ensuring that we address any and all vulnerabilities that we might have with China.

The United States entered this year's World Radio Conference with three goals: expand connectivity, unlock space, and protect spectrum for national security. It is

clear that we need to be focused on expanding mobile connectivity and updating our technology to meet and combat China's aggressive approach.

Mr. Lewis, do you believe that the United States is doing everything that we can to have a competitive advantage over the Chinese Communist Party's spectrum policy?

*Dr. Lewis. Unfortunately, no. The risk for the United States is that it will become a spectrum island, where there are allocations that apply only to the continental United States and not to the rest of the world. And this has major implications for electronic warfare. So we could do more to address this risk.

The U.S. has strong advantages. We still lead over China, but they are determined to displace us. And they have gotten a better reception in many parts of the world than we have when it comes to spectrum allocation.

*Mr. Joyce. Mr. Lewis, do you think that commercial wireless can work in tandem with our national security interests?

*Dr. Lewis. I believe it is possible. In the long term, people are very optimistic about the prospects for

dynamic spectrum-sharing, which is a way of saying that two users can occupy the same space. And between artificial intelligence and other programing --

*Mr. Joyce. Do you feel that that dynamic spectrum-sharing can be safely done?

*Dr. Lewis. At the moment, yes. In limited cases by the end of the decade, certainly.

*Mr. Joyce. Mr. Singleton, what national security risks do we face if we allow the Chinese Communist Party to further lead in communication networks and spectrum bands that the United States has yet to develop?

*Mr. Singleton. I would say China's penetration of spectrum bands and broader U.S. communication networks provides China with direct gateways, frankly, to intercept and manipulate vast quantities of data traversing our networks. It jeopardizes not only the privacy of American citizens, but also the integrity of our infrastructure systems.

And so, as a result, China is really poised to impede the mobilization of American military forces, to foment a state of disarray, and to redirect national attention and

resources in --

*Mr. Joyce. Do you feel that is a national security risk as we sit here today?

*Mr. Singleton. Absolutely.

*Mr. Joyce. What policies should we adopt to ensure that the U.S. once again develops that leadership position in spectrum, and not only against the Chinese Communist Party but on the world stage?

And that is for you, Mr. Singleton.

*Mr. Singleton. I think there is often a hesitancy here in Washington, understandably so, to mirror China's behavior simply because we have radically divergent governance structures.

I think in this area in particular, the Chinese have shown a willingness to think boldly, to think about how, from a national and sort of Beijing-centric perspective, they can drive innovation, growth, and dominance as it comes to -- as it reflects just spectrum dominance and spectrum operability. I think it is something where we also need to sort of get in the game, build --

*Mr. Joyce. Okay, to get in the game what should we in

Congress be encouraging to develop that spectrum dominance, which you mentioned and I agree with?

*Mr. Singleton. No, I mean, I think we absolutely actually first have to understand what our adversary is doing and how our adversary perceives that sectoral advantage.

And then, from there, sort of assess, I think as we have mentioned here, the fact that we have to broadly understand the risks, and which are the highest-profile risks, and really focus our effort there. I think a broader conversation on spectrum is absolutely necessary and required. I think the key for that will be talking to industry stakeholders, and really understanding from them and hearing their concerns, but also what opportunities they could potentially leverage if spectrum opens up and if we are thinking more expansively about spectrum.

*Mr. Joyce. So working with industry leaders will allow our spectrum to expand and to be safer. Is that the message that we need to leave this hearing with?

*Mr. Singleton. Absolutely.

*Mr. Joyce. I thank all the witnesses for being present here today.

And, Mr. Chairman, I yield.

*Mr. Latta. Thank you. The gentleman yields back the balance of his time. The chair now recognizes --

*Dr. Lewis. If I could add one thing, Mr. Chairman, the one thing Congress could do is renew FCC's auction authorities. That would be a good first step.

*Mr. Latta. Thank you. The chair now recognizes the gentlelady from Tennessee's 1st district for five minutes for questions.

*Mrs. Harshbarger. Thank you, Mr. Chairman. I have changed my whole line of questioning since I have sat here and listen to you all. Thanks for being here today.

Mr. Lewis, I will start with you. You know, we have been talking a lot about rip and replace, and it makes a lot of sense because consumers don't have a choice, generally, in what equipment is connected to their network. And Americans deserve the right to keep themselves free from Chinese espionage. And in your testimony you say anything connected to the Internet can be used to collect information.

I guess my question is what items can consumers make their own decisions about?

*Dr. Lewis. The first case I ever looked at, by the way, was a fish tank connected to the Internet. This was about 20 years ago, and a foreign government hacked the fish tank to get into the --

*Mrs. Harshbarger. Twenty years?

*Dr. Lewis. You wouldn't think that. But what American consumers can think about -- and there has been some progress in this, it is a race, a regulatory race between the U.S. --

*Mrs. Harshbarger. Yes.

*Dr. Lewis. -- and Europe -- is some kind of good housekeeping standard. You know, that when you buy the equipment you know it has been done in some trusted way. So that is probably the best thing for consumers.

*Mrs. Harshbarger. Yes, okay. How do we educate consumers, I guess, to buy secure technology?

*Dr. Lewis. The example I have heard used sometimes is a New York City example, which is they have started making restaurants put their ratings --

*Mrs. Harshbarger. Yes.

*Dr. Lewis. -- outside on -- their Board of Health ratings.

*Mrs. Harshbarger. Yes.

*Dr. Lewis. And something like that would probably help consumers.

*Mrs. Harshbarger. You also mentioned that Chinese software was embedded in specific apps, and Americans don't even know about it. And you said in your statement you spoke about software development kits that provide portions of code for larger programs and apps. Is that what you are speaking about?

*Dr. Lewis. That is the primary concern.

*Mrs. Harshbarger. Yes, and I know that for a fact because we were briefed on that when I was on Homeland Security. And they said we can check your phone any time and see.

How do we combat that? I guess -- do we have to know the origins of those apps, or would that be enough to help?

*Dr. Lewis. A first step would be just knowing that you have the potential Chinese software on your phone, or --

*Mrs. Harshbarger. Well, somebody has got to disclose that somehow for us to know.

*Dr. Lewis. We don't have a process for that --

*Mrs. Harshbarger. Yes.

*Dr. Lewis. -- and that would be useful to --

*Mrs. Harshbarger. It would, wouldn't it? It would be useful to have a process.

*Dr. Lewis. Yes.

*Mrs. Harshbarger. Who knew? Okay. We can work on that, Chairman.

What effect do you see on Chinese companies when they are placed on the entity list or the covered list?

And we can start with you.

*Dr. Lewis. I missed the question.

*Mrs. Harshbarger. What effect do we see on Chinese companies when they are placed on the entity list or the covered list?

*Dr. Lewis. They complain a lot. They lose market share, they lose revenue.

*Mrs. Harshbarger. Yes.

*Dr. Lewis. So overall, it is a useful tool. It is not a perfect solution because it is a little bit like whack a mole, but it has effect.

*Mrs. Harshbarger. Yes, okay.

Mr. Singleton, you talked about the DJI and direct investments, and can you tell us a little bit about how that happened? Because these have been away, and then you had to -- I know this because I looked at them, and a lot of Americans have these drones, the Phantom or the DJI, but we know it is Chinese software. Tell us how that happened, and then how does this -- how does the data flow?

*Mr. Singleton. Sure. I mean, I think I mentioned a little earlier DJI is like the poster child for Chinese military-civil fusion. This is a company that received these direct infusions of capital from at least four known Chinese Government entities, and the goal was to prop up and support, through subsidies, through credits, through support, these direct capital infusions, the drone industry and to make them a market champion.

And that is because, as we have mentioned here, what you see with the Chinese is what you get. They have articulated clear strategies in their 5-year plans, the 13th and the 14th, to dominate this industry. And they understand the value of technological leverage and weaponized interdependence.

I think that the challenge is, because they are able to keep prices low in the drone industry -- but they are also doing this increasingly in the EV sector -- they can flood out other market competitors. And at this point there are very few -- almost zero -- U.S. competitors. Almost none of them are really cost effective.

And so we do have to start to think about, once again, this slow war of attrition, weeding them out of markets. And drones brake, drones fail. Technology needs updates. If we can do a death by a thousand cuts approach --

*Mrs. Harshbarger. Yes.

*Mr. Singleton. -- I think sort of cut into some of their market share, while recognizing that the FCC covered lift is not a panacea.

*Mrs. Harshbarger. Well, that was my next question. What kind of suggestions do you have to incentivize these American companies to get into that market?

*Mr. Singleton. Usually the government can lead here. I thought that the recent rules on DoD procurement bans on DJI and cattle equipment sort of set the stage. Why don't we replicate that for DHS can't buy those products, DHS

purveyors can't buy them, the State Department can't purchase Chinese batteries?

*Mrs. Harshbarger. Yes.

*Mr. Singleton. I mean, we have to sort of work cross jurisdictionally at the different departments and agencies. And eventually, industry on their own, when they recognize they can't get a government contract because they use those drones, will eventually decide to get rid of them and to buy a different product to maintain connectivity to the U.S. Government. So I actually think this is an example where the U.S. Government can drive change in the market.

*Mrs. Harshbarger. Yes, okay. Thank you.

Mr. Chairman, I yield back.

*Mr. Latta. The gentlelady yields back. And seeing there are no further members wishing to be recognized, again I want to thank our members, our witnesses for being with us today before the subcommittee.

I ask unanimous consent to insert in the record the documents included on the staff hearing document list.

Without objection, that will be the order. Without objection, so ordered.

[The information follows:]

**********COMMITTEE INSERT**********

*Mr. Latta. I remind 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 Friday, March the 1st.

And just once again, I want to thank our witnesses for being here for this sobering testimony, and I hope across the country folks can hear this because it is something that we all have to take extremely seriously, what is happening out there.

Without objection, the subcommittee is adjourned.

[Whereupon, at 12:30 p.m., the subcommittee was adjourned.]