Testimony of Lindsay Gorman

German Marshall Fund of the United States

Prepared for the

U.S. House of Representatives
Committee Energy and Commerce
Subcommittee on Communications and Technology

Hearing on
"Securing Communications Networks From Foreign Adversaries"

Thursday, February 15, 2024
10:00 AM EST
2123 Rayburn House Office Building

G | M | F Alliance for Securing Democracy

Chairman Latta, Ranking Member Matsui, Chair McMorris Rodgers, Ranking Member Pallone, and Members of the Subcommittee, thank you for the opportunity to testify today on securing our networks from foreign adversaries.

My name is Lindsay Gorman, and I lead a research and analysis team at the German Marshall Fund's (GMF) Alliance for Securing Democracy, studying how democracies can together outcompete autocrats – chiefly the People's Republic of China (PRC) – in critical and emerging technologies of the future. The ideas in this testimony reflect a body of work at GMF on the one area in which this technology competition is playing out: over the future internet.

I come at this question from the perspective of a technologist with training in quantum physics and artificial intelligence and first-hand experience working on the technologies critical to U.S. national security. I recently had the privilege of serving at the White House, where I crafted technology and national competitiveness strategy for the U.S. government. I also developed initiatives to implement that strategy, including through the US-EU Trade and Technology Council and Quad Critical and Emerging Technology Working Group. Both during my time at GMF and in government, I have had the opportunity and privilege of engaging extensively with officials, policy, and technology communities across the Atlantic on PRC technology matters from 5G and digital infrastructure to AI and international standards setting. I began my career building cryptographic protocols for IP telephony at Bell Labs, as well as cybersecurity tools and autonomous vehicle prototypes in connection with DARPA projects. The views I express in this testimony and before you are my own and should not be taken as representing those of my current or former employers.

I. The Future Internet: A Connected and Contested Cyber-Physical World

Today, the United States and its democratic allies and partners are engaged in an existential technology contest that is rapidly becoming the defining arena of geopolitical competition with the PRC. At issue is whether the technology systems that citizens around the world rely on will continue to be governed by values that are rooted in openness, transparency, freedom, and democracy, albeit imperfect, or surveillance, censorship, autocracy, and control. Nowhere is this dichotomy and competition of value systems clearer than over the struggle to define and build the Future Internet. In a report for the Alliance for Securing Democracy at the German Marshall Fund, I defined this Future Internet as:

> The suite of technologies and the standards for how they operate that will define and shape digital connectivity over the next 30 years, including: infrastructure technologies and internet protocols; application layer technologies that run atop this infrastructure, harnessing data often with artificial intelligence; and the governance frameworks this technology stack imputes.[1]

The picture is one of a connected stack of layers, where competitive advantages in building out one layer of the stack accrue dividends for dominance in other layers. This is particularly true for foundational infrastructure layers, such as 5G or 6G telecommunications infrastructure or undersea cables, which is why competition and security requirements in these layers have been so acute.

---

[1] Lindsay P. Gorman, *A Future Internet for Democracies: Contesting China's Dominance in 5G, 6G, and the Internet-of-Everything* (Washington, DC, German Marshall Fund, 2020), https://securingdemocracy.gmfus.org/wp-content/uploads/2020/10/Future-Internet.pdf.

As communications networks advance in increased speed, improved data-carrying capacity, and decreased latency, an explosion of applications and devices that sit atop those networks present expanded opportunities for access exploitation, espionage, and intrusions.

By 2030, the IoT suppliers' market is projected to reach $500 billion with a full potential for the IoT market value as high as $12.6 trillion.[2] Applications in healthcare, smart cities, connected vehicles are already springing up and have the potential to drive massive value creation, but also to introduce equally large cybersecurity risks. As Commerce Secretary Raimundo pointedly outlined, 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?"[3] Smart vehicles that can allow for traffic light optimization, collective route planning, or thermostat adjustment on an approach home can also provide a nefarious actor with information on visits to the doctor or therapist, where children play soccer, or trips to the local watering holes.[4] The same can be said of wearable health monitors, telehealth visits, and one day remote surgeries. Managing the exploding attack surface these cyber-physical connections imply will determine how much of this value is successfully captured by the US, and how much may be lost due to lack of trust or due to determined PRC cyber espionage.

II. Securing the Future Internet and Steeling Against PRC Cyberwarfare and Espionage

One dimension of the cyber risk that animates the need for trusted supply chains that remain free from the threat of significant autocratic control is that of dependence-building in critical infrastructure: if US and allied networks are controlled by companies accountable to the PRC, in a crisis scenario or time of heightened tension, those networks could be held hostage. This risk is not theoretical. The PRC has a history of using infrastructural dependence and cyberattacks to exert leverage and achieve its geopolitical goals. The case of Vietnam's rejection of PRC territorial claims in the South China Sea is illustrative here. Since 2014, Chinese investors have frozen energy infrastructure projects in Vietnam and cyber groups linked to China have launched cyberattacks on Vietnamese airports and government officials in response to disagreements over China's maritime claims in the South China Sea.[5] The very threat that the PRC could wield critical infrastructure control represents an unacceptable national security risk.

A second dimension of the necessity in securing critical layers of the technology stack is the persistent threat of PRC espionage and disruption from state-sponsored and linked cybercriminals. In addition to run-of-the-mill disruption and threats to the US economy and society, cyberespionage is a key tactic in the PRC strategy to acquire US and allied origin technology critical to its global data and emerging technology leadership ambitions.[6] The Office of the Director of National Intelligence's 2023 Annual Threat Assessment assessed that "China probably currently represents the broadest, most active, and

---

[2] Jeffrey Caso, Zina Cole, Mark Patel, and Wendy Zhu, "Cybersecurity for the IoT: How trust can unlock value," McKinsey & Company, April 7, 2023, https://www.mckinsey.com/industries/technology-media-and-telecommunications/our-insights/cybersecurity-for-the-iot-how-trust-can-unlock-value.

[3] Mackenzie Hawkins, "Raimondo Warns Chinese EVs Pose National, Data Security Risks," *Bloomberg*, January 30, 2024, https://www.bloomberg.com/news/articles/2024-01-31/raimondo-warns-chinese-evs-pose-national-data-security-risks.

[4] Future Internet, Data of the Daily Commute, p.10.

[5] Gavin Bowring, "Vietnam yields cautionary tale over Chinese investment," *Financial Times*, November 27, 2014, https://www.ft.com/content/6ea71dd6-ccea-3779-87be-d4654fc9379b.

[6] Lindsay Gorman, "China's Data Ambitions: Strategy, Emerging Technologies, and Implications for Democracies," The National Bureau of Asian Research, August 14, 2021, https://www.nbr.org/publication/chinas-data-ambitions-strategy-emerging-technologies-and-implications-for-democracies/.

persistent cyber espionage threat to U.S. Government and private-sector networks. China's cyber pursuits and its industry's export of related technologies increase the threats of aggressive cyber operations against the U.S. homeland, suppression of the free flow of information in cyberspace—such as U.S. web content—that Beijing views as threatening to the CCP's hold on power, and the expansion of technology-driven authoritarianism globally."[7] The United States loses around $300 billion annually to CCP intellectual property theft, a phenomenon that has been described by former NSA Director General Keith Alexander as "the greatest transfer of wealth in history."

Even as the United States has recognized and taken steps to counter this threat, PRC cyber intrusions have not abated. This month CISA, NSA, and FBI along with interagency and Five Eyes partners released an advisory warning critical infrastructures that "People's Republic of China (PRC) state-sponsored cyber actors are seeking to pre-position themselves on IT networks for disruptive or destructive cyberattacks against U.S. critical infrastructure in the event of a major crisis or conflict with the United States." The operation, conducted by state-sponsored group Volt Typhoon positioned hackers in US networks for up to five years.[8] The motives outlined should make any US citizen deeply skeptical of PRC-based providers of any critical information infrastructure, especially communications networks.

Securing the Future Internet will require increased coordination among public and private sector actors, stronger education of critical infrastructure providers on the threats of state-sponsored espionage, and continued and increased outreach by the FBI and CISA to private sector technology providers to raise awareness and expertise on the types of state-sponsored actors they are likely to be targeted by. Required reporting of intrusions to CISA will help build a picture of state-sponsored activity.[9] This picture then needs to be communicated back to the critical infrastructure and technology providers that are on the front lines of defending the nation's technology and infrastructure assets. Moreover, a risk-based approach to IoT component certification that delineates smarter and more central IoT components, and standards that create true incentives for the adoption of secure components will also be needed.

III. Winning the 6G Race

While the transition from 4G to 5G is characterized by increasing IoT applications, the upshot of which is a new generation of consumer and industrial technologies, 6G promises to realize this vision more fully. Described as the end of the smart phone era, 6G is the stuff of science fiction: multisensory augmented, virtual, or mixed reality, connected robotics and autonomous systems, drone-delivery systems, autonomous drone swarms, and vehicle platoons. [10] The emergence of smart surfaces and environments, wireless brain-computer interactions, blockchain and distributed ledger applications, holograms, and virtual remote control will again revolutionize the economy.[11] 6G will also send parts of

[7] ODNI 2023 Threat Assessment
[8] "PRC State-Sponsored Actors Compromise and Maintain Persistent Access to U.S. Critical Infrastructure," Cybersecurity & Infrastructure Security Agency (CISA), February 7, 2024, https://www.cisa.gov/news-events/cybersecurity-advisories/aa24-038a.

[9] "Cyber Incident Reporting for Critical Infrastructure Act of 2022 (CIRCIA)," Cybersecurity & Infrastructure Security Agency (CISA), accessed February 13, 2024, https://www.cisa.gov/topics/cyber-threats-and-advisories/information-sharing/cyber-incident-reporting-critical-infrastructure-act-2022-circia.
[10] A Future Internet for Democracies.
[11] Laurens Cerulus and John Hendel, "Hologram wars: The race to 6G," *Politico*, April 11, 2021, https://www.politico.eu/article/6g-race-eu-united-states-china/.

the network into space, constructing non-terrestrial networks of low-Earth orbit satellites and unmanned aerial vehicles to enable cost-savings from 5G's ground-based fiber optics and cell towers.[12]

Given the economic opportunity and geopolitical import of leading 6G, the race is on to develop the standard or set of standards that will power next generation networks.[13] In its 14th Five-Year Plan, the PRC identified 6G as a top priority, and like with 5G will hope to shape global 6G standards under development in bodies including 3GPP and the ITU.[14] The PRC's IMT-2030 (6G) Promotion Group has signed an MOU with European 6G Smart Networks and Services Industry Association (6G-IA), even as the European Commission's 6G flagship initiative Hexa-X-II is led only by European companies. Through the Next G Alliance, the Washington, DC-based Alliance for Telecommunications Industry Solutions has signed MOUs with the O-RAN alliance, 6G-IA, Japan's Beyond 5G Promotion Consortium, and Korea's 5G Forum.[15]

Averting a repeat of China's leadership in 5G and achieving 6G dominance requires both dedicated investment in research, development, and commercialization; the rapid fielding of spectrum; attention in advance to cybersecurity requirements, including for post-quantum cryptographic protocols and algorithms; and sustained international collaboration and engagement in the standards process. Both the US-EU Trade and Technology Council and Quad Critical and Emerging Technology group have made strides in driving allied coordination on 6G and Open RAN technologies. Congress can help sustain these plurilateral initiatives and insulate them from changing political winds so that allied 6G and future internet development becomes a mainstay of US foreign and technology policy.

IV. US Policy Responses

Over the last four years, the U.S. policy response to this competition has ramped up significantly across two dimensions. First, efforts to prevent the use of PRC-based network infrastructure providers in the United States and globally. And second, efforts to shake up markets and create viable alternatives to PRC providers.

The U.S. International Development Finance Corporation (DFC) has made strategic investments in lower income countries on the condition they eschew PRC-made 5G gear, including committing to pay off or finance billions in sovereign loans in Ecuador and committing up to $500 million to an initiative led by Vodafone in Ethiopia to establish an alternative telecommunications operator without equipment from Huawei or ZTE. On subsea cables, DFC has committed to loan Trans Pacific Networks $190 million to support a telecommunications cable connecting Singapore, Indonesia, and the United States. DFC has involved been in the Blue Dot Network effort to develop high-standards for infrastructure investments.[16]

While these efforts are important, the reality is that Huawei is still embedded in networks around the globe. PRC-based vendors still accounted for more than half of the 5G equipment installed in Europe in 2022, for example. The US cannot take its foot off the gas when it comes to 6G or to the security of its communications networks. In addition to domestic rip-and-replace efforts, international cooperation to

---

[12] Tyler Carroll, "New 6G Networks Are in the Works. Can They Destroy Dead Zones for Good?" *Scientific American*, October 3, 2023, https://www.scientificamerican.com/article/new-6g-networks-are-in-the-works-can-they-destroy-dead-zones-for-good/.
[13] Mercator Institute for China Studies (MERICS), "Fragmenting technology – 6G mobile could divide the world," February 22, 2023, https://merics.org/en/comment/fragmenting-technology-6g-mobile-could-divide-world.
[14] Rogie Creemers et al., *Translation: 14th Five-Year Plan for National Informatization* (Stanford Cyber Policy Center, 2022), https://digichina.stanford.edu/work/translation-14th-five-year-plan-for-national-informatization-dec-2021/.
[15] https://www.rcrwireless.com/20230113/open_ran/atis-inks-deal-oran-alliance-boost-cooperation
[16] https://crsreports.congress.gov/product/pdf/R/R47006

create alternatives to Chinese providers has leaned into the promotion of Open RAN, such as in the Quad Critical and Emerging Technology Working Group, and a 6G industry roadmap in the US-EU Trade and Technology Council. Congress is critical to ensuring this work continues.

V. Recommendations

I offer five recommendations to Congress to ensure our communications networks remain competitive and secure from foreign autocratic threats into the future:

1) **Catalyze 6G development**

   Congress should fund the creation of international centers of excellence for Next G research and development, such as through the Next G Alliance, with an aim to deepen allied coordination on 6G innovation hubs, looking to Finland's 6Genesis Flagship Project as an example.

2) **Plan for 6G security**

   6G builds on the promises of 5G networks and involves the incorporation of intelligent technology and smart devices into all societal niches. As this technology integrates into daily life in higher volumes and with greater sophistication, a 6G future will amass sensitive data at a larger scale than ever before. In response, Congress require the DNI to conduct a cybersecurity risk assessment for emerging 6G frameworks, incentivize the adoption of robust cybersecurity requirements into Open RAN and 6G standards, and set timelines and roadmaps to plan for post-quantum cryptography systems.

3) **Pass federal privacy and data security legislation**

   The US has largely failed to secure protections for sensitive personal data through federal legislation and must take concrete steps to enact legislation that will ensure American data is not subject to misuse by foreign adversaries in the name of gaining strategic advantages. Regulations must begin with provisions that limit the agency of third-party data brokers, requiring brokers to register with the FTC, pay annual registration fees, disclose ties to foreign entities, and create guardrails on data that can be sold without user consent. Lawmakers should also consider legislation that limits the acquisition and sale of biometric data to exclude covered foreign entities; requires companies that collect citizen data to implement cybersecurity requirements; and supports small business cybersecurity tax credits.

4) **Address IoT security**

   The IoT—the suite of physical technologies and applications that rely on the Internet as groundwork for functionality—has grown rapidly over the last decade. As a consequence, this network of connected devices has amassed massive amounts of data (by 2025, it will reach the scale of zettabytes). This aggregation of data will only continue to skyrocket with the advent of 5G and 6G networks, which will buttress even greater numbers of technological devices and applications—and this data is currently entirely vulnerable. The United States needs both a

robust federal framework that secures IoT data and the incentives and means to implement it. Lawmakers should consider enacting standards that obligate enhanced cybersecurity and breach notifications in IoT devices, offer incentives for providers that choose certified IoT vendors, and center cybersecurity requirements in emerging 6G frameworks to secure vulnerable data at the application layer.

5) **Invest in the TTC and Quad for semi-permanence**

Finally, our international leadership on 6G and creating alternatives to PRC-based vendors has made progress, but more work is clearly needed. Congress should build a budgetary line-item to support the US-EU Trade and Technology Council and Quad over a 5-10 year timescale. Connective tissue is important, and bureaucratic mechanisms take time and effort to stand up and to build trust. Congress can help insulate this mechanism from changing political winds in the United States, while providing the means for its strategic evolution and adaptation over time.

Thank you and I look forward to your questions.