Testimony of

Lindsay Gorman

Prepared for the

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

Hearing on
“Protecting Communications Networks and Improving Connectivity”

Wednesday, July 22, 20246
2:00 PM EST
2123 Rayburn House Office Building

Chairman Guthrie, Ranking Member Pallone, Chairman Hudson, Ranking Member Matsui, and Members of the Subcommittee, thank you for the opportunity to testify today on the essential ways we need to protect our networks and our leadership in the artificial intelligence (AI) era.

I come at these issues from a background as an AI and cybersecurity engineer with start-up companies and Defense Advanced Research Programs Agency (DARPA) initiatives, as a builder with technology-focused venture firms, as a researcher of US-China competition in AI and telecommunications, and as an advisor to the White House on emerging technology strategy.

Two years ago, I had the honor to testify before this Subcommittee on the Future Internet and risks of cyberwarfare and espionage from the People's Republic of China (PRC). I argued then that democratic allies need trusted supply chains for a projected $500 billion Internet of Things market, and that present day applications such as in healthcare, connected vehicles, and smart cities introduced new attack vectors and cybersecurity risks around dependence-building, espionage, and intellectual property theft.

Today, those risks have grown immeasurably and also transformed in character with the rapid adoption and diffusion of generative AI. Yet the U.S. policy response has largely not kept pace with the threats -- neither to ensure American global technology leadership, nor to secure our networks.

U.S. national security policymakers have to confront two intersecting risks:

(1) the actor-agnostic expanding cyber threat surface posed by AI models, agents, applications, and the networks they run on; and

(2) the risk of loss of American AI leadership to geotechnical competition from the PRC.

In developing policy prescriptions, they should be clear-eyed about which risk proposed solutions aim to target.

An Exploding Cyber Attack Surface

Whereas two years ago, the proliferation of connected devices posed growing threats to network and application security, today the landscape has shifted dramatically. The adoption and diffusion of AI risks creating gaping holes for intruders to penetrate as well as the accelerated means to do so.

- **AI risks tipping the cyber offense-defense balance in favor of the attacker**. First, AI systems have shown remarkable progress in conducting cyberattacks. In a one study published in March, Anthropic found that over the last year more cyberattacks were being conducted autonomously with AI, and threat actors were using AI in complex stages of cyber operations. In its evaluation of Claude Mythos Preview in April of 20226, the UK AI Security Institute concluded that on its tests the tool was "at least capable of autonomously attacking small, weakly defended and vulnerable enterprise systems where access to a network has been gained." AI also shows promise in defending against cyber intrusions through means such as automated threat detection, vulnerability discovery, improving incident detection, takedowns of malicious sites, and predictive analytics. But the barriers to closing vulnerabilities are often less technical ones and more matters of organizational culture or leadership prioritization. CISA and CERT, for example, already maintain a known vulnerabilities catalogue, yet they persist unpatched in US systems. Absent a coordinated public-private policy response at least an order of magnitude more

ambitious than we have seen previously, advanced AI cyber systems are likely to tip the balance in favor of the attacker.

- **Models and agents create new cyber access points.** Second, AI models and agents also themselves introduce cyber risk. Prompt injection attacks can be used to fool an AI chatbot into revealing inner workings or sensitive documents it has access to. Data poisoning attacks can corrupt training data to alter model output or create malicious backdoors. Such models are used with a wide array of personal, corporate, and sensitive data, exposing ill-designed or defended systems to attack. Model distillation attacks also open vectors for adversary competitors to tune model outputs using U.S. frontiers models in contravention of their terms of service. Moreover, the rise of agentic AI creates attack vectors intruders could only dream of as agents receive executable permission on devices on which they run.

- **AI 'World Models' incentivize physical AI data collection**. Finally, this already massive attack surface is poised to grow exponentially as well in the coming years. One movement in the AI research and investment community is the development of "world models" – taking generative AI from linguistic corpora on the screen to three-dimensional movement in the real world. These visionaries argue that in order to realize true human or superhuman intelligence, AI needs to understand, process, and engage with the physical world. The potential is extraordinary, from humanoid robots that can diffuse explosive devices on the battlefield to those that fold laundry at home. Breakthroughs in large language models came from the ability to ingest massive linguistic corpora from the

internet so that models could learn at scale patterns of human writing and speech. So too will enormous quantities of real-world data be required to train this next rung of AI's evolutionary ladder: videos of janitors cleaning office buildings, soldiers conducting reconnaissance missions, factory workers assembling complex machinery, or basketball players shooting free throws could all be sought after training data. Put simply, this requirement incentivizes increased and continued surveillance of human activity. Once developed and deployed in homes, cities, military installations, factories, and workplaces, the ability to continue to collect data and iteratively improve world models will be a competitive advantage as well. Such expanded and three-dimensional collection and data processing opens new avenues for network intrusions while also raising their stakes.

US-PRC Competition and Open Source/Open Weight AI

The United States enjoys a first-mover advantage on generative AI and a profound compute advantage. Yet PRC competitors are quickly catching up on models and pursuing sectoral AI adoption as cracks in US export control frameworks risk leveling the playing field on compute. Both espionage and competitiveness dimensions need inform US AI and cyber policy towards the PRC.

- **The United States and its Allies can benefit from leading open-source AI infrastructure**. Historically, the United States has enjoyed the benefits of leadership in building the open-source ecosystem of the modern internet. In the 1970s, global internet protocol TCP/IP emerged from early DARPA research, and major US firms such as IBM and AT&T were among its first adopters. When software engineers the world over write code in any major computer programming language, they do so in English. Private

corporations then built proprietary systems atop this architecture, leveraging it to create massive economic value for US companies and industries. Today, the US leads in frontier AI, but its infrastructural foundations are largely unfolding behind closed doors. Meanwhile, the development of the open-source architecture on which these systems were built (such as Common Crawl) has stalled in comparison to the rapid pace of proprietary AI development. In order to spur innovation and ensure US leadership in the generations of AI to come, vibrant open-source AI foundational infrastructure and ecosystems will be crucial.

- **PRC open weight models pose cyber risks as well as major challenges to US global AI diffusion**. Instead, it is the PRC that has doubled down on elements of open AI. Players like DeepSeek and Moonshot are releasing open weight models – free to use, yet difficult to find bugs. While many analysts assess this approach as a short-term strategy to catch up to US frontier labs, it carries long-term risks for AI infrastructure dependence building, particularly in third countries. Even in the United States, some AI start-ups are turning to Chinese open weight models due to cost.

As these models close the performance gap with US frontier models, AI infrastructure is emerging as a key domain of competition. The United States cannot afford to cede leadership in open architecture and ecosystem creation to China.

‘AI-Native’ 6G Networks

All of the above describes and envisions a world of massive compute, power, and network throughput needed the likes of which are nearly unfathomable today. The next generation of telecommunications networks is being designed with AI at its center. Given that major PRC cyber intrusions have come from these networks, securing them as equally important as securing the myriad AI applications that will run atop them. 6G standards envision leveraging AI for automated threat detection as well as the transition to post-quantum cryptography. Accelerating this transition and ensuring that 6G is built by suppliers from democratic allied nations will be vital for their security.

Recommendations

I offer the following recommendations to harden US cyber defense and promote US leadership in AI and the 6G telecommunications networks it will run on.

- **Modernize U.S. Cybersecurity Oversight for the AI Era**:
    - Develop mandatory, tailored obligations for the highest-powered models around safety and security testing, development, and responsible deployment with adequate controls for cyber and national-security relevant models and applications. The frameworks for frontier AI governance and cybersecurity outlined in Titles I and III of the *Great American Artificial Intelligence Act* represent a strong starting point.
    - Establish an ISAC modelled after existing cybersecurity ISACs for public-private coordination on cyber threats to the US and allied AI stack.

- **<u>Secure AI Models and Applications Against Foreign Adversarial Suppliers</u>:** Direct the FCC to develop an implementation strategy for the Covered Entity List suited to AI-era risks, including a risk-based assessment of data exfiltration and foreign control of AI models and applications. Such a framework for adversarial AI models and applications should have the following, 3-tiered structure:
    - Ban the use of PRC AI models in federal, state, government and government contracting applications.
    - Incentivize firms in high-value emerging technology areas with key intellectual property such as telecommunications, quantum computing, pharmaceuticals, new energy technology, and robotics to choose non-adversarial alternatives such as through tax credits on AI-enabled R&D and fast-track security reviews.
    - Direct the FTC, in coordination with the FBI, CISA, and relevant IC entities, to publish a risk-based guidelines and recommended mitigation measures around hosting, evaluation, and data access for corporate use of PRC AI models and applications in less sensitive fields.
- **<u>Accelerate 6G Adoption and Security as the first "AI-native" network:</u>**

  Spectrum
    - Direct the Commerce Department to fast-track the clearing and relocation of mid-band spectrum for 6G — BCG estimates 600 MHz of full-power mid-band spectrum will be needed by 2029 to maintain U.S. mobile leadership.

- Direct the FCC to publish acceleration timelines for key 6G spectrum auctions in coordination with Commerce and the Pentagon.
- Facilitate spectrum-sharing between 5G and 6G bands for accelerated initial deployment via accelerated R&D and crash pilot programs specifically on spectrum-sharing techniques.

Security and Deployment

- Establish a 6G Accelerated Deployment Initiative to coordinate spectrum, security, and R&D priorities across the federal government, industry, and allies and partners.
- Set up 6G pilot projects and testbeds across federal agencies, prioritizing deployment speed to maintain global competitiveness.
- Fund translational R&D to move 6G innovations from lab to market and incentivize trusted 6G components via grants, credits, and expedited public procurement.
- Designate 6G as critical infrastructure.

Allied Cooperation

- Reconstitute the 6G Standards Contact Group under the aegis of the GCOT to guide US and allied standards strategy and serve as an early-warning system for undue PRC coordination and influence
- Fund and build allied 6G testbeds and pilot projects to coordinate deployment of trusted 6G infrastructure globally as part of Pax Silica.

- Harness the DFC, EXIM Bank, and financing mechanisms to support secure 6G choices globally and join up these digital development efforts with key allies and parters.

- **<u>Secure and Compete on Open-Source AI:</u>**

Secure

- Direct the FTC, in coordination with the FBI, CISA, and relevant IC entities, to publish a risk-based guidelines for corporate use of PRC AI models and applications in less sensitive fields.
- Establish an FTC-NIST-FBI AI consumer safety initiative that runs technical analyses of PRC open weight models, publishes risk assessments, and conducts targeted threat briefings to universities and research labs on risks.
- Include an open-source component to the White House cyber clearing house and task IVOs to evaluate open weight models above popularity thresholds towards mandatory cybersecurity standards for open source models hosted on key US cloud providers.
- Direct the Commerce Department to develop security standards for open weight models

Compete

- Incentivize domestic low-cost competitors to PRC open-weight models and open-source AI infrastructure consortia, provide dedicated compute resources to open-

source model developers from academia or nonprofits, and codify the National AI Research Resource (NAIRR) in statute.

- Build an explicit open-weight track into the American AI Exports Program with the goal to create low-cost rivals to PRC models. Such an initiative would unlock cooperative financing mechanisms to promote open weight model development and contracts.
- Create an Allied Open-Source AI Consortium as part of Pax Silica to promote and coordinate open-source development with key allies prioritizing open source such as the European Union.

- **Rebuild tech trust with U.S. allies and partners.** The global movement towards sovereign AI poses risks to US AI diffusion and leadership. In European capitals, for example, debates about a US 'kill switch' animate an impetus to move away from US technology as a matter of sovereignty. Rebuilding trust is necessary to capitalize on US strengths – its alliances.