HEARING ON "TAKING A BIGGER BYTE: CHINA'S EXPANDING STRATEGY FOR DATA DOMINANCE"

HEARING BEFORE THE U.S.-CHINA ECONOMIC AND SECURITY REVIEW COMMISSION

9:30 a.m.

Thursday, April 30, 2026

Dirksen Senate Office Building, Room 430, and Webex

U.S.-China Economic and Security Review Commission

444 North Capitol Street NW, Suite 602

Washington, D.C. 20001

U.S.-CHINA ECONOMIC AND SECURITY REVIEW COMMISSION

HON. RANDALL SCHRIVER, CHAIR

MICHAEL KUIKEN, VICE CHAIR

COMMISSIONERS:

Hal Brands

Taylor Budowich

Joshua Hodges

Leland Miller

Reva Price

Livia Shmavonian

Chris Slevin

Hon. Jonathan N. Stivers

CONTENTS

CONTENTS (continued)

HEARING ON "TAKING A BIGGER BYTE: CHINA'S EXPANDING STRATEGY FOR DATA DOMINANCE"

Thursday, April 30, 2026

U.S.-CHINA ECONOMIC AND SECURITY REVIEW COMMISSION

Washington, D.C.

The Commission met in Dirksen Senate Office Building, Room 430, and Webex at 9:30 a.m., Commissioner Leland Miller and Commissioner Chris Slevin (Hearing Co-Chairs) presiding.

OPENING STATEMENT OF COMMISSIONER LELAND MILLER,
HEARING CO-CHAIR

COMMISSIONER MILLER: Good morning and welcome to the fifth hearing of the U.S.-China Economic and Security Review Commission's 2026 annual report cycle. Thank you for joining us. We welcome our witnesses and are grateful they are here today to share their expertise.

I would also like to extend our appreciation to the Senate Committee on Health, Education, Labor, and Pensions for use of their hearing room, as well as the Senate Recording Studio for their assistance in livestreaming this event.

For those attending in person or watching online, witness testimonies are available on the Commission's website and a transcript of this hearing will also be posted to the website.

Today's hearing will examine China's motivations and strategies for acquiring data, both domestically and abroad, and how Beijing is working to integrate this vast collection into a unified, state-directed framework.

Chinese leaders view data as a strategic asset, a driver of economic growth, indigenous innovation, and industrial policy, but also as a tool to shape and control global information flows in support of military and national security objectives. This approach reflects a deliberate, top-down effort to embed data dominance at the center of China's economic and geopolitical strategy.

It also underscores Beijing's intent not just to compete in the digital economy but to set the terms by which data is governed, accessed, and exploited globally. While Washington continues to debate and deliberate on this issue, Beijing has spent the better part of a decade building a comprehensive, regulatory and operational architecture designed to do two things simultaneously: hoard its own data and systematically vacuum up ours.

The asymmetry is stark. China's regulations, such as its cybersecurity law and data security law are instruments of strategic data accumulation. Beijing identifies what constitutes important data and compels its companies to share such data with the

state. China stockpiles software vulnerabilities reported within 48 hours of discovery and is under no obligation to disclose those vulnerabilities to foreign organizations, all to bolster its own offensive cyber capabilities.

Meanwhile, Chinese scientists have legally accessed data from U.K. biobanks, reported as recently as last week, U.S. genomic databases, and global data markets with relative ease, while China's similar data remain firmly off limits to foreign researchers and companies.

Beijing also seeks to gain data advantage through state-sponsored cyber operations. China's advanced persistent threat groups, or APTs, have spent decades burrowing into U.S. networks and critical infrastructure across the defense, health care, telecommunications, and energy sectors. The 2015 Office of Personnel Management breach alone exposed sensitive personal and security clearance data on 22.5 million Americans, and more recently the APT known as Salt Typhoon has been conducting a years-long campaign against U.S. government agencies. In just one year,

from 2024 to 2025, cybersecurity firm CrowdStrike reported a 150 percent surge in espionage attacks and a 300 percent increase in targeted industrial cyberattacks. These are campaigns that are state-orchestrated, persistent, and increasingly AI-enabled.

None of this is new. What is new is the scale, the sophistication, and the sobering reality that the vectors of threat are likely more comprehensive than anything we can fully imagine today.

I look forward to the insights of our panelists today on both the scope of this challenge and the policy actions required to address it.

Thank you to the panelists for being here today. We will start with Dr. Lohn. Oh, sorry. Commissioner Slevin.

[The prepared statement of Commissioner Miller follows:]

OPENING STATEMENT OF COMMISSIONER SLEVIN

HEARING CO-CHAIR

COMMISSIONER SLEVIN: Thank you, Commissioner Miller. Good to be here. Thank you to our witnesses for being here this morning and to our staff at the Commission for the preparation that has gone into this hearing.

Data has become a foundational input to modern economies, enabling technological breakthrough, driving innovation, and improving quality of life. The digital economy represents over 15 percent of global output, a figure that continues to grow, but data collected and used without appropriate safeguards is also a national security vulnerability. We have seen these risks materialize repeatedly through large-scale data breaches, the opaque practices of data brokers, and the collection of sensitive user data by foreign-owned apps.

Over the past two decades China has developed a comprehensive strategy to acquire, aggregate, and exploit data as a strategic resource.

Individual datasets may appear low sensitivity in

isolation, but when telecommunications metadata, geolocation data, financial transactions, biometric records, and travel histories are aggregated and processed with advanced AI capabilities the result is something far more dangerous -- the ability to identify, track, profile, and potentially coerce U.S. military personnel, intelligence officers, and policymakers.

Some responsive steps have been taken. The Justice Department has moved to restrict both data transfers to foreign adversaries. The FTC issued warning letters to 13 data brokers earlier this year. These are meaningful signals that the legal tools exist and that enforcement agencies are beginning to act. But we are, at present, documenting this problem more effectively than we are solving it.

As the United States and China compete across artificial intelligence, quantum, biotechnology, access to large-scale, high-quality data has and will continue play a determining role in shaping which country will lead global technology development. The United States, alongside our allies, remains at the

cutting edge of science and technology.

But our lead grows more tenuous by the day. Now is the time for us to ensure that Congress and U.S. policymakers realize the scale of the challenge we face concerning China's data strategy to forge a long-term approach to curb China's problematic activities and address our own vulnerabilities.

Our witnesses today will help us better understand the rationale behind China's data acquisition strategy, how it is implemented, and its implications for the United States, by examining both the why and the how. We aim to identify actionable recommendations that Congress can use to more effectively address China's acquisition and misuse of U.S. data. I look forward to their testimony. Commissioner Miller.

[The prepared statement of Commissioner Slevin follows:]

PANEL I

INTRODUCTION BY COMMISSIONER MILLER

COMMISSIONER MILLER: Now we will turn to Dr. Lohn for his testimony.

STATEMENT OF ANDREW LOHN, SENIOR FELLOW, CENTER FOR SECURITY AND EMERGING TECHNOLOGY, GEORGETOWN UNIVERSITY

DR. LOHN: I would like to open by thanking the Commission for this opportunity. It is an honor to be invited to this forum to discuss such an important and rapidly evolving topic.

I lead a small team of researchers at Georgetown University's Center for Security and Emerging Technology. My team's focus is on the intersection of AI and cybersecurity. We also study what is required to create and deploy advanced AI systems in terms of finance, semiconductors, models, and other underpinnings of the technology. These are all intense areas of competition with China.

This testimony will briefly discuss Chinese acquisition of American AI technology and how AI can enhance their cyber operations going forward, and I'll conclude with a few policy recommendations to limit those risks.

China's cyber teams have been targeting American defense contractors, technology companies, government

agencies, and citizens for decades, but their approach and our views have evolved over time. I remember optimism 10 years ago, such as following the Obama-Xi meeting that China might agree not to use cyber espionage for commercial gain. Today I hear less optimism about any ideological restraint, and it seems that the CCP views cyber as one tool among many for acquiring U.S. technology. They buy compiled datasets from data vendors, they use their positions in markets such as autonomous vehicles or commercial drones to enhance sensor coverage, they siphon off data in transit around the world as it passes through their telecommunications infrastructure, and they poach specialized knowledge of talented individuals such as through the Thousand Talents and related programs.

Now, the technology of the day is AI, and American companies developing it are often relative upstarts who have little experience as targets of sophisticated espionage campaigns, and whose business models often rely on providing access to their technology at extreme scales.

Our AI companies are becoming even more enticing

targets as their models and services become more capable, especially in the cyber domain. The company XBow topped the bug bounty leaderboard last year, finding more vulnerabilities than any human, and Anthropic's new Mythos has the cyber world buzzing.

But China does not view AI technology exactly as we do. While U.S. AI technology giants block their services from going to China, China also uses its great firewall to block those services on their side. And despite loosening export controls on U.S. AI chips last year, China has not purchased any of those chips yet.

Their reluctance is due to several factors. One is to support their domestic industry. Another is to avoid reliance on American models or services that could be restricted in a conflict, that could disseminate an American world view, or that could even be poisoned to subvert Chinese interests.

Contrasting that reluctance, China is also aggressively stealing all aspects of AI technology. Chinese companies are smuggling billions of dollars of U.S. AI chips. The CCP is tempting or coercing AI

researchers to China, using both carrots, such as the Thousand Talents programs, and sticks, as in Operation Fox Hunt. And all three U.S. AI leaders -- Alphabet, OpenAI, and Anthropic -- have accused China of using American outputs to train Chinese copies using techniques known as adversarial distillation.

The various forms of theft, along with their own inventiveness, have kept Chinese companies near the American frontier. The American lead is often estimated at only around six or seven months, so we should expect that the AI-induced cyber advances we see today in America will come to China soon. Already we have seen Chinese attackers string together many separate AI models to conduct complex, if relatively unsophisticated, cyberattacks in ways that threaten to upend our strategy of layered defenses.

At the same time, software maintainers are already being overwhelmed by the number of vulnerabilities that AI is discovering. It is not clear yet whether AI will help them close those gaps or if it will find too many holes for them to manage.

We should also expect the impacts of theft to

become even more damaging as AI enhances digitization. Twenty years ago there was far less to steal online. Now, with AI becoming people's therapists, and as agentification forces companies to digitize their workflows, the severity of coercion and the risk of intellectual property theft will continue to grow.

Defensively, setting aside the many technical steps to take and the role that industry must play, there is plenty for federal regulators to do. As a starting point, much of the burden of preventing theft falls on the Critical Infrastructure and Security Agency, CISA, which is understaffed from layoffs, has had leadership uncertainties, and has been plagued by intermittent shutdowns as part of the Department of Homeland Security. They are a focal point for security guidance, for informing industry of threats and vulnerabilities, and they are the sector management agency for information technology.

Information sharing among AI companies and the intelligence community will also be crucial as the threats continue to grow and attackers attempt to hide themselves. Much of that falls on the National

Security Agency's AI Security Center and the Cybersecurity Collaboration Center. Staffing and funding CISA and those information sharing efforts is necessary to secure American AI software from theft.

As for the hardware that is being smuggled, the Bureau of Industry and Security is responsible for preventing and interdicting those shipments, but they have historically been underfunded, so boosting their funding would help.

Identifying smugglers remains difficult, though, so Congress can mandate location monitoring for restricted chips. Those techniques face many limitations, but the value of the chips is large and growing, so helping to find even a small fraction of illicit shipments could help make up for the cost and difficulties.

Finally, and most broadly, the United States, and Congress in particular, should be cautious with the sacrifices it makes in pursuit of AI, given the alerts raised by American labs that China is freeloading off American investment. If America is to reallocate energy and water infrastructure, to finance or

backstop corporations, or to provide regulatory relief for construction, privacy concerns, copyright infringement, or psychosocial harms, then the benefits should not accrue to China. Congress and the American taxpayer should demand assurances that AI developers can protect the technology as a precondition to receiving our support. Thank you.

[The prepared statement of Dr. Lohn follows:]

COMMISSIONER MILLER: Thank you, Dr. Lohn. Mr. Lin.

STATEMENT OF JOSEPH LIN, CO-FOUNDER AND CEO, TWENTY

MR. LIN: Chairman Schriver, Vice Chairman Kuiken, distinguished members of the Commission, thank you for the opportunity today to testify.

In my written testimony I document how the PRC has undertaken a systematic, state-directed effort to convert data into intelligence advantage, economic leverage, coercive influence, and wartime decision superiority. In the time that I have before you today I want to focus on just one point.

The United States is still treating this challenge far too defensively. We treat breaches, privacy, and critical infrastructure as separate issues. Beijing does not see it that way. The PRC treats data as a strategic resource, it treats commercial networks as intelligence collection platforms, civilian logistics systems as potential military targets, and persistent cyber access as a form of pre-conflict positioning. And that is the core problem. China is not merely stealing data, it is doing so to build an AI-enabled intelligence and targeting architecture for economic competition,

political coercion, and wartime advantage.

Over the last five years, the threat has changed in three key ways.

First, China's cyber operations feed intelligence, military, and political objectives. That is not just traditional espionage or intellectual property theft. Campaigns associated with Volt Typhoon and Salt Typhoon show at the PRC is targeting the systems the United States would depend on in a crisis -- telecommunications providers, transportation networks, and civilian critical infrastructure systems that support our military modernization. In other words, a future conflict over Taiwan would not begin only in the Taiwan Strait. It would begin at home. This is all part of China's plan to coerce, deter, and defeat the United States.

Second, China has built an ecosystem that facilitates industrial-scale cyber operations. Let me repeat that again -- industrial scale cyber operations. The relevant actor is not only the PLA or the MSS, it is also a wider ecosystem of contractors, hacker-for-hire firms, access brokers, and even

commercial technology companies. This ecosystem gives Beijing reach, deniability, and surge capacity, letting Chinese state organs acquire access and data at a scale government operators alone could not generate.

Third, AI raises the strategic value of everything that China is collecting. Data that might once have set unused in a repository can now be fused, searched, modeled, and operationalized. Telecommunications metadata can reveal networks of associations, location data, movement patterns. Health, financial, and family data can reveal personal vulnerabilities. Logistics, maintenance, and supplier data can reveal mobilization bottlenecks, weaknesses in weapon systems, and weaknesses in the defensive industrial base.

The result is a fusion problem that we have. Bulk commercial data, persistent cyber access, and AI are converging faster than U.S. policy is adapting. That convergence is equally dangerous for U.S. military and national security personnel. The Defense Intelligence Agency has warned about ubiquitous

technical surveillance, which is the aggregation of data that links people to devices, locations, transactions, relationships, and patterns of life.

This is not just a theoretical problem that we have. Public reporting on Israeli operations against Iranian military and political leaders illustrates what can happen when systematic intelligence collection, cyber penetration, and data analytics are fused effectively. Senior officials can be tracked, located, targeted with a precision that would have been much harder to achieve in an earlier era.

The implication is clear. Commercial data is now operational data, civilian networks are now military relevant terrain, and privacy exposure is a force protection risk. While we have taken important steps, including DOJ's Data Security Program and public actions against Chinese cyber actors and infrastructure, it is not enough. The overall U.S. response remains too focused on defense, compliance, and resilience. Those things are necessary, but they are not sufficient. If the expected return on Chinese cyber operations remains high and the expected costs

remain manageable, Beijing will continue. That is Deterrence 101. China will not stop because we issue advisories, patch faster, or even write better compliance rules. We have to change the cost calculus.

So I would emphasize three recommendations.

Number one, Congress should support sustained offensive pressure against Chinese cyber operators and the infrastructure that enables them. The objective should not be episodic retaliation after major incidents. It should be continuous campaigning against adversary infrastructure -- access brokers and contractor-operator intrusion platforms. We must force Chinese operators to spend more time building access, more money defending their infrastructure, and more effort protecting their tradecraft. Right now, China has been able to impose persistent costs on us while bearing too little reciprocal burden.

Two, the U.S. should target the ecosystem, not just the government operators. Chinese cyber power is scalable because contractors, data brokers, technology vendors, and other commercial actors provide access,

deniability, and surge capacity. The United States should use sanctions, criminal charges, export control, and public exposure to make participation in that ecosystem commercially dangerous and strategically costly. Message should be simple: If a company helps the MSS or PLA cyber operators target the United States and its allies, it should lose access to U.S. capital, U.S. technology, and U.S. markets.

Three, Congress should treat strategically relevant data as national security infrastructure. That means codifying a national security data control regime, creating telecommunications and core network security requirements, and passing secure-by-design requirements for edge devices and networking gear. And it means protecting military-adjacent commercial data.

Now, I am not suggesting that we copy China's model of state data control, but we have to recognize that openness without guardrails is being converted into adversary leverage. China's data acquisition strategy is not just about stealing secrets. It is

about building decision advantage. It is about mapping the people, networks, infrastructure, and dependencies behind U.S. power projection. It is about accelerating Chinese AI and military modernization, and ultimately it is about creating options to delay, disrupt, or deter U.S. action in a crisis.

Defense alone will not restore deterrence. We need to put China's cyber ecosystem under pressure, force Beijing to spend more defending its own networks, and deny it the ability to convert American openness into strategic leverage.

Thank you, and I look forward to your questions.

[The prepared statement of Mr. Lin follows:]

COMMISSIONER MILLER: Thank you, Mr. Lin. Mr. Cory.

STATEMENT OF NIGEL CORY, DIRECTOR, CROWELL GLOBAL ADVISORS

MR. CORY: Good morning, Chairman, Vice Chair, Commissioners. Thank you for the opportunity to testify here this morning.

My core point today is simple: China has spent over a decade building a coordinated, state industry response to what it sees as the foundational input of the digital and AI economy, data. The United States has not made an equivalent adjustment. The United States still has the world's most innovative firms, but they are competing in a global market, shaped by a competitor that treats technology policy as a coordinated national project, while the United States treats it as a portfolio of separate regulatory and trade questions. Data governance runs on parallel tracks, at Commerce, State, Treasury, the FTC, Justice, and others, each handling a slice, none really responsible for the whole.

We have many of the pieces but we do not really have a data policy layer in the U.S. tech policy stack. The gap in action between the two matters

because of where we are in the global, digital, and AI market, and the competition for market share at the moment. The competitive architecture of the next decade is being set now, in procurement rules, national AI and data laws, and standards bodies.

China treats data as a factor of production, on equal footing with land, labor, capital, and technology. President Xi has said this repeatedly since 2021, and Beijing has since built the legal, regulatory, and institutional machinery to act on it. The Data 20 article sets the economic framework, the National Data Bureau, established in 2023, is operationalizing it, and the World Data organization, launched only last month in Beijing, may well become the platform to try and export it.

You can see this same pattern apply in specific sectors, such as physical AI. China has built more than 40 state-funded, robot data collection centers nationwide, and has issued a unified data collection standard to ensure every robot generates training data in interoperable format. Leading firms are releasing open datasets under state pressure to build shared

industry infrastructure rather than proprietary moats.

And you can see it in standards, with the role of China's TC260, translating Cyberspace Administration of China policy into technical standards in these specific sectors, and then aiming to take those same standards to international standards bodies.

Now, compare this to the United States. We withdrew from the WTO digital trade negotiations in 2023, ceding the field to both Beijing and Brussels. The Trump administration is partly correct at this but not broadly or consistently enough. We have no national equivalent robotics data infrastructure initiative, by example, and national security-driven actions targeting data are similarly haphazard, fragmented, and often delayed.

The U.S. thankfully continues to stand behind the global cross-border privacy rules system, and likewise the Trump administration has launched the Genesis Mission to put federal scientific datasets to work training AI models, and is obviously pushing ahead through the AI Action Plan and AI Exports Program. And in Congress, there is bipartisan legislative

proposals that are worth considering, such as the Digital Trade Promotion Act and the National Commission on Robotics Act.

But there is still no data policy layer in the U.S. tech policy stack. We have the firms, we have some of the policies, we have some of the ideas, but we do not have the strategy that pulls it together.

This brings me to Southeast Asia and the compounding effect of early entry in data collection, the flywheel. In digital markets, more users generate more data, which trains better products, which attract more users, which generates more data. Once a platform reaches critical mass in a market, displacing it becomes very difficult. In digital markets, early wins compound. And right now, flywheel either spins for you or against you, and in Southeast Asia it is increasingly spinning out for China.

Chinese platforms hold roughly half of e-commerce gross merchandise value across several major markets. Chinese firms are laying the undersea cables and building data centers that move the region's data. Chinese cloud providers are increasingly aggressive

and successful in winning contracts at prices that reflect state subsidy, not commercial cost recovery.

And under China's data security law and national intelligence law, that data is legally accessible to the Chinese state, with no independent judiciary to constrain access and no transparency requirement that would allow anyone outside Beijing to know when access occurs.

This is a structural difference. U.S. firms operate under rule of law. Chinese firms operate under the rule of potential compulsion. Both compete in Southeast Asia, which is a critical market for U.S. and Chinese firms. Only one carries a home country governance regime that turns commercial data into state-accessible data and an input into its national project. The difference is that the U.S. private sector is competing abroad, largely without a coherent government strategy and talk yet behind it.

Let me close with three categories of recommendations.

First, codify U.S. digital trade priorities. Congress should pass the Digital Trade Promotion Act

to codify protections for cross-border data flows and other critical pro-digital trade provisions so they survive administration turnover. And re-engage WTO digital trade negotiations with a clear and strong position.

Second, make Southeast Asia a priority theater. Back the U.S. ASEAN Digital Work Plan with real funding and staff at State and the Development Finance Corporation, and explicitly prioritize it under the American AI Export Program. The administration should continue to push the Global Cross-Border Privacy Rules expansion. Bringing Vietnam, Indonesia, and India would change the balance of data governance in the Asia-Pacific. And it should also try to operationalize the OECD trusted government access to data principles so partner countries have the legal tools to distinguish trusted from untrusted providers on grounds beyond price, which is what, obviously, Chinese providers excel on.

Third, emulate some of the institutions China has built that we obviously haven't, such as a national industrial robotics data foundry to give U.S.

manufacturers, especially SMEs, the shared training data infrastructure that China is building at scale. The administration should push for a trusted cloud initiative with Five Eyes partners, Japan, the EU, and others, to give allied governments and commercial buyers a common framework for distinguishing trustworthy and untrustworthy cloud providers.

Finally, they should institutionalize the analytical framework that Commerce used in the connected vehicles rulemaking so that we can identify genuine data-related chokepoints across critical technologies, systematically and proportionally, rather than reactively.

And with that I thank you again for the opportunity to testify this morning, and I look forward to your questions.

[The prepared statement of Mr. Cory follows:]

PANEL I QUESTION AND ANSWER

COMMISSIONER MILLER: Thank you, Mr. Cory, and thank you all for all your testimonies. We will do questions in alphabetical order, but I am going to take the prerogative of the Chair to kick us off.

Mr. Lin, you highlight in your testimony that biotechnology and health data deserve special attention as Beijing deems this a strategic resource, not just a purely privacy issue the way it is often viewed in the U.S. Can you dive into that issue a little bit more and tie it into why we should care about China's ability to access things like the U.K. Biobanks, our American genomics databases, and other key health and bio databases in the West? And by the way, anyone else who would like to contribute to this after Mr. Lin is welcome.

MR. LIN: Thank you, sir. You know, I think it's important to note the sheer scale of what China is trying to accomplish in the genomics space, especially through institutions like the Beijing Genomics Institute.

It's important to not just focus, I think, just

on the genomics or even the health data part but to look at that as simply one slice of an overall data aggregation, processing, and computing strategy, where what they want to be able to do is they want to, obviously, be able to leverage this for medical and health benefits for research, but also, undoubtedly, they are doing so in order to be able to do genetic-level targeting. Ultimately, that is the objective.

And so when we think about that we have to think both in terms of what is China doing, what sorts of data are they making accessible, what other types of data are they trying to collect from a personal health records perspective, not just within China but outside of it. Presumably this is so that their database has an increased amount of diversity, as well.

And so thinking through what are the types of protections that we have to put in place, and also that certainly applies to our own policies within the United States, how do we govern things like genomics information, how do we ensure that only the right researchers, only the right hospitals, providers have access, and how do we make sure that we have the right

protections in place.

MR. CORY: I think biodata is a really interesting case. It's obviously been sensitive and important in China for decades, going back to 1998. And it is one where they have institutionalized domestic controls around it the earliest, in that there are rules that require genomic data to only be stored in China, to only be accessed by authorized personnel. So they have set up the mechanism to control it, to aggregate it, and then they are now operationalizing it as a part of their industrial policy.

DR. LOHN: This is not my expertise but I, anticipating this question, discussed it with a colleague, Dr. Steph Batalis yesterday and her answer struck me, so I'll try to pass it here. She explains pretty clearly and convincingly that targeted bioweapons is not a real risk here, but that deidentification is, that we have lots of people who want to be not identified as they're walking around, Special Operations forces or military who don't want to have their identity in those locations tracked

back. And if even their family members or distant relatives have been collected with their DNA then they can be identified and then coerced in other ways.

COMMISSIONER MILLER: Thank you. Let's move back to Mr. Cory. One of your recs was for Congress and the administration to establish a National Robotics Industrial Foundry. Can you explain that concept in a little more depth for us?

MR. CORY: Basically, the data required to train physical AI is different from large language models, and so they can't obviously just access it publicly or off the internet. So it comes through the repetitious creation or monitoring of robots set up doing particular functions and capturing that. So that, obviously, happens in individual silos, in firms across America. And that lack of sharing is exactly what China has addressed by creating and forcing everyone to use a standard format. So the use of certain robots in certain scenarios can be equally applied to another firm elsewhere.

So similarly, getting NIST and working with industry on what that equivalent standard would look

like here and then setting up pilot projects for that within existing sort of arm institutes would be essentially a way for the U.S. to respond and start that same aggregation of common data, to allow U.S. robotics firms to benefit from what everyone else is doing, essentially.

COMMISSIONER MILLER: Thank you. I'm going to stick with you, Mr. Cory. In your testimony you gave us a fantastic overview of China's data supervision, government's landscape, explaining how certain agencies oversee regulatory aspects, some data governance aspects, some are offensive, some are defensive.

So big picture, how would you characterize the structure of China's entire state-driven data framework, and is there any similarity here with how the U.S. does or does not structure its various data-related government entities?

MR. CORY: Big picture. I think it's hard to find any comparator to what China has created institutionally in the role and the power of the CAC, the Cyberspace Administration of China, which is a

regulatory and party body. And you cannot distinguish in what it does what is a regulatory decision and what is a political decision. And it has created an apparatus and a mechanism around data on the domestic aggregation and sharing of it and the activation of its value, which it does through standards and sectoral bodies, but then, obviously, enacting on the other side, strict controls on who can access that data and where that data can go.

So, I mean, as is always the case with China, they have created a central institution that acts in a way, in a central coordinating function that there is no equivalent, I don't think, anywhere else in the world.

And I think it's particularly interesting the new National Data Bureau is under the National Development and Reform Commission. And that's important because that gives it an industrial policy lens as it looks at what it does. Like don't confuse the National Data Bureau for some data protection authority. Its lens is how do we activate the value of data in China, in a centralized, coordinated manner, obviously involving

all the relevant sectoral regulatory authorities and such.

COMMISSIONER MILLER: Thank you, Mr. Cory. We will move next to my esteemed Co-Chair, Commissioner Slevin.

COMMISSIONER SLEVIN: Thank you, Commissioner Miller. Thanks for each of your testimonies. I think you each illustrated well the scale and ambition, speed with which China's cyber operations have been targeting against the U.S. and allies over the last few years, and that you have each hinted, in your own way, and suggested that congressional response has been muted compared to the scale.

I want to ask also maybe a little bit of a big picture question around just China's risk tolerance and how you've seen that change. Previous intrusions, attacks showed some effort of concealment, in a way. That seems like that has evolved.

And so maybe beginning with Mr. Cory, just your sort of assessment of just the risk tolerance changing, and with that is it changing methods, is it changing the types of targets, civilian versus

military? I invite you to begin and then your colleagues also.

MR. CORY: I think I'll begin and focus on the commercial side of things and then my co-panelists can look at the intelligence and defense aspect. But basically China is creating an apparatus that obviously seeks to maximize the domestic accumulation and use of data in alignment with its strategic industrial policies. But akin, there is a central tension as it does that, in that it wants to strictly control where that data is and who uses it, in that it is, I think as you mentioned, the top line of control the outflow, expand the inflow, as well as, obviously, maximizing everything they generate domestically.

The central part of my testimony, vis-à-vis the Chinese legal apparatus providing broad, opaque state access to commercial data, is at the heart of what could potentially come, that my co-panelists have spoken about, in that there is no meaningful constraints on Chinese government's ability to access data and use it in any way, shape, or form, whether that be for a commercial, industrial policy goal or

intelligence or defense purpose. And that is baked in, foundationally, to the operating environment that these Chinese firms are in, whether they are operating at home or abroad. It's just that the question of the role of that opaque power has changed with the rise of AI and the increasing value of data.

I mean, in final, it gives them broad authority to act however they want, whenever they want, and that is quite arbitrary. I'm sure the Commission has heard the stories over the years, there is action and reaction. As the U.S. targets one thing, with export controls or the Clean Network Initiative or whatever it may be, and then China will take a corresponding action. So they retain freedom of movement as it relates to controlling data whenever they want, essentially.

COMMISSIONER SLEVIN: Thank you. Mr. Lin?

MR. LIN: Commissioner Slevin, let me start with answering the first part of your question, which is have we seen any change to how the PRC has looked at risk in terms of their cyber operations. And I think, unequivocally, the answer is yes. What we see is that

China has become increasingly emboldened over the years, and unfortunately, we have ourselves to blame for that. If you go back with me to your Thomas Schelling 101, and you look at things like signaling, you look at concepts like retaliating. And what we have done, effectively, is by not responding in any meaningful way we have encouraged China to go up the escalatory ladder. What has our signal been? What have the consequences been to their increasingly egregious compromises of American networks?

We started by saying, by justifying, by rationalizing that, well, this is just state-on-state espionage, this is classic intelligence, we do it too, so there's really no difference. So what have we done? We have indicted a handful of PLA officers who probably have no intention ever of coming to the United States. We have filed some démarches, and that's kind of it.

So the message to the PRC is have at it, right. There are no consequences to your actions. So ironically, even though we view offensive cyber operations as potentially escalatory -- this has

always been a concern of ours for a very long time, and we can have a separate conversation about how it's actually not -- our lack of response, our focus only on defending our networks, our obsession with resilience, has actually been highly escalatory and is encouraging them to now embed themselves into critical infrastructure in the United States, critical infrastructure networks, to start targeting Middle America towns, water treatment facilities in Western Massachusetts. These are the types of things that they are doing now, and they think that there is no consequence to it.

COMMISSIONER SLEVIN: Thank you, Mr. Lin. Dr. Lohn, anything you would like to add?

DR. LOHN: Just quickly, I think that's mostly true, but there have been some red lines. I don't know that they are ready to turn off power or mess with a water grid because our response will go outside of the cyber domain and maybe outside of the policy domain, and I think that's maybe where the red line hits. And I'll provide you your time back.

COMMISSIONER SLEVIN: Thanks. Commissioner

Miller.

COMMISSIONER MILLER: Thank you. Commissioner Brands is up next. He will be joining us virtually.

COMMISSIONER BRANDS: Thank you. Maybe I could start with Mr. Lin. I'd like to pick up kind of where that last discussion left off. You laid out an array of measure the U.S. could take to be more effective in terms of sustaining offensive pressure against Chinese cyber operators. What would you say the obstacles to doing this thus far have been? Is it risk aversion? Is it authorities issues? Concerns about escalation? All of the above? You mentioned in particular that you thought that the last issue, concerns about escalation, is overblown. So I'd just be curious to hear you talk a little bit more about what has stood in the way so far.

MR. LIN: It's always a little daunting to be discussing deterrence theory with the Henry Kissinger Professor at Johns Hopkins SAIS, but I'll try to hold my own.

You know, what have been the impediments? I think certainly a misguided perception about

escalation and just how escalatory cyber can be. For a very long time, if you think about the origins of offensive cyber, how we governed it, how we organized it, how we tried to control it, we put the predecessor to what is now U.S. Cyber Command, and actually initially U.S. Cyber Command, under the umbrella of U.S. Strategic Command. For a long time it was believed that cyber weapons were potentially as dangerous as escalatory, as uncontrollable as nuclear weapons, so we had to be extraordinarily cautious. That's what defined our thinking early on.

And I think the very best evidence of how non-escalatory offensive cyber operations and cyberattacks are is by our lack of response to all of the attacks that China has been throwing our way. What have we actually done? Not much, right. So that's part one.

Number two, your question around policies, your question around authorities. The authorities are there. I think there is a question, historically, around willingness, but I think starting with the first Trump administration's approach towards delegating decision authority to U.S. Cyber Command,

through NSPM-13, that's been a very welcome push in that direction to make it easier to lower the barriers to using offensive cyber capabilities. And I think what you're seeing now with the second Trump administration, as well, is a willingness, a far greater willingness, to use non-kinetic and especially cyber capabilities as part of joint military operations. So I think that willingness is now there.

In terms of authorities, the authorities are there. We have the authorities, whether we're talking about Title 10, 50, 18, we have them. It's just a matter of are we willing to actually use them, to put them to use.

And then number three, one of the things that you didn't mention but I would hammer is on is have we approached this problem of force generation from the right perspective. Because ultimately that's part of what we're talking about, is this is a force generation problem, and do we have the right capabilities in place, do we have the right people in place, do we have the right models in place, where we are also able to conduct industrial-scale cyber

operations. For a very long time, we have approached offensive cyber operations through an artisanal lens, and we have to change that. We can no longer rely on just a handful of extraordinarily talented, committed cyber operators to be the tip of the spear. We have to figure out how do we mobilize the entire force and ensure that they are equipped with the right capabilities to do so, rather than simply continue to try to throw more people at the problem.

COMMISSIONER BRANDS: Thank you. And while I have you, you referenced the ability to use data to target senior officials. So maybe you could just expand a bit on what we've learned about this from recent military engagements. And perhaps you could just kind of paint us a little bit of a picture of what this might look like if China were to try to do something similar to the United States in a crisis or conflict scenario?

MR. LIN: Yeah, sure. So let me talk about this both in the abstract and then to go back to the example of, at least reportedly, what the Israelis have been able to do against Iranian political and

military targets.

The sheer amount of data that every single one of us generates, even right now, in this very moment, is extraordinary. The amount of data that is being generated by our phones, which are attached to us by our smart devices that we are wearing, all of this can be used to track pattern of life. All of this can be used to track our movements, our biodata.

And so you can imagine that if a foreign adversary wanted to use this data to coerce individuals, to track individuals, to gain leverage over them, or in the case of, at least reportedly, what's happened in Iran with what the Israelis have been able to carry out, they have been able to do highly targeted precision strikes, simultaneously against entire layers of Iranian military and intelligence leadership. This is something that, you know, going back 200 years, our military thinkers probably would have thought, or even 100 years, would have thought impossible, but this is extraordinary.

So I think we're in a brave, new world, and for ourselves what this means is twofold. One, we have to

get much better at protecting that data, certainly, but we also have to think about how do we use that to our advantage, as well.

COMMISSIONER BRANDS: Thank you very much.

COMMISSIONER MILLER: Commissioner Hodges.

COMMISSIONER HODGES: Thank you. Picking up on the conversation that just took place with Commissioner Brands, I just want to kind of clarify a little bit here. On the issue of what we've seen publicly available and sort of the increasing capabilities and access into data into the United States, would you agree that we're seeing the Chinese sort of expanding their domains? And can you speak a little more about how they may be pre-positioning here inside the United States? That is of concern to us.

Mr. Lin, this ties back into the sort of deterrence theory and the conversation that you were just having. But I guess I'm just curious, just to help us understand, help the public understand, how is that pre-positioning actually taking root, not just potential like for threats, but where specifically are we seeing them pre-position in ways that they

previously haven't?

MR. LIN: Yeah. I'm happy to lead off. To abstract up a little bit, the best way to think about the pre-positioning that the PRC is doing now in the cyber domain is during the Cold War what we called counter-value targeting. For a very long time, we viewed what China was doing to us from the lens of purely intelligence collection, IP theft, things like that, and then that started to broaden out where they would target our government and military networks. But we said, of course, that's what they would do.

But now they are going after broad swaths of American society. I mentioned earlier in my remarks that they're going after things like water treatment plants in rural Massachusetts, that have zero military or political value. So ultimately why are they doing that? Well, I think it's pretty obvious. It's to be able to hold American society at risk so that in time of war they can start to turn up the pain. How much pain are we willing to tolerate at home? How much are we willing to risk?

This goes back to the old question of are we

willing to trade Los Angeles for Paris? Are we willing to trade rural America water treatment facilities for coming to the aid of Taiwan or some other East Asian ally? And I think they believe that this is a way in which you can undermine political support for otherwise popular national security decisions that the United States would make.

COMMISSIONER HODGES: Perfect. Thank you. Just to expand it out a little bit to the rest of the panelists, if I'm sort of combining what each of you has said, you've sort of framed this as a comprehensive, systematic approach across multiple domains, with far-reaching consequences to national security here, within the United States, as well as to nations overseas.

And I guess one of the questions I'm constantly sort of grappling with and hearing as I sort of make the rounds with folks is how much of this is nation-to-nation versus business-to-nation? So recognizing we are here to talk about U.S. and what we can do to pre-position or stop against the pre-positioning here, but I'm curious to get your thoughts on how much of

this should be driven from a business side versus a nation side. Mr. Cory, if you don't mind leading off.

MR. CORY: Interesting question. I mean, because when you're facing Chinese firms you're not just facing them alone. Chinese tech firms operate in an ecosystem and a market where they're able to essentially, partially socialize the development costs of what they've had to go through to come to market overseas, through preferential financing, discriminatory procurement, compute support, AI, and data and power support, and then, obviously, external market support through the Digital Silk Road and others.

And so when U.S. firms who are competing on the basis of commercial operations and price and such, and they need to recoup their costs, their considerable costs, by how they operate, I mean, they're facing an entity that is not playing on the same field. I know for a fact that there are U.S. cloud operators in Southeast Asia facing Chinese competitors that are providing free onboarding for new clients and are providing 60 to 80 percent price discounts up front.

And that's just not commercially viable, and that reflects the state-supported nature of these Chinese cloud firms overseas. So it's a different dynamic in terms of their relationship with their home government and what that means when they compete abroad.

DR. LOHN: I would say that I agree with all of that, and the Chinese theft to support their companies is industrial espionage that we would draw a different line on. They support their companies in all sorts of ways like that.

I would also say that our companies, we might not be defending as well as we could be, in lots of cases. There are several cases where their technology is being siphoned off, and we need to help identify in which ways and where the defenses are. Some of the distillation attacks that are happening right now are difficult to detect at the company level. Kyle Miller, who is here, walked me through some of that yesterday. The bottleneck where we might be able to have the most focus, leaning on what Joseph Lin is suggesting, is more upstream in a defense-forward standpoint.

COMMISSIONER HODGES: Thank you.

COMMISSIONER MILLER: Vice Chair Kuiken.

VICE CHAIR KUIKEN: Thank you very much, Commissioner Miller. You snuck up on me. It's been great hearing all your testimonies. Thank you very much.

I have this sort of moment where you all triggered me a little bit this morning. Congress is debating the 702 Rule right now, which I'm sure most folks in the room are tracking. I used to work on these issues when I worked for Leader Schumer, and it was always amazing to me how spun up folks got about 702. And one of the reasons that I always reacted in sort of an odd way was that if anyone has ever downloaded their Amazon data, or their LinkedIn data, or their Twitter data, or whatever data is associated with any of their accounts, it is absolutely incredible the amount of data that is available on Nigel, on Joseph, and on Andrew, let alone me and my beloved Chair, Randy Schriver.

People always get fired up about Palantir and license plates, and I understand why. And at the same

time, you're driving down the road and it's publicly available, and Palantir basically took information that was already in the public space and just put it in one spot, which is essentially what Amazon is doing, LinkedIn is doing, and all these other folks are doing.

I wrote an op-ed a few months ago in the *Financial Times* saying that data should be an asset that people are able to put on their balance sheet. They are doing this in China right now. And the reason that they're doing it is basically to get their way out of the debt crisis that they're in. So if I have my assets on one side of the balance sheet and my liabilities on the other side, it looks really bad. I'm in the red. And all of a sudden all the data that I have, I can put on the asset side of the balance sheet and things change quite a bit.

The thing that people always talk about is the frontier labs and all the cool stuff that they're doing. The really cool stuff is what the companies that are at the infrastructure layer of the AI ecosystem are really doing. How do we start tapping

into all of the data that we actually have? And one of the things that I realized is that the United States has absolutely no data strategy whatsoever from a U.S. government perspective. I mean we have got data lakes, data ponds, data rivers, whatever sort of body of water. We probably have a data ocean, in reality.

As I'm listening to you guys talk about the way that the Chinese are approaching data I sort of want to look inward. One of the things that we do at the end of the year is make recommendations to Congress on what the United States should do to sort of address this issue. You guys have said a lot of things, but the thing you haven't sort of said is should the United States government think about getting its own data house in order? We can talk about no data to Europe, no data to China, no data to all these places. Well, until we figure out what our strategy is or what we're actually going to do with the data, it seems we have some work to do.

I'd welcome your reactions to that. There's not really a question embedded in that other than a whole

bunch of things to hopefully get you a little bit fired up. Andrew, you are first.

DR. LOHN: Thank you for selecting me first.

VICE CHAIR KUIKEN: You're welcome.

DR. LOHN: I'm fired up about it also. You might have noticed, in my written testimony, memory palaces. These things scare me, where people are recording all of their interactions. It's not a lake. They have it segmented off by rooms. Everything that they're written with an AI system is recorded to be used further. And the types of things that people are putting in these are different, more personal, more important to their operations, their businesses, and their daily lives than what we've recorded in the past. We've recorded so much in the past that I'm not sure how much more impactful it is, but I'm fired up about it, as well.

VICE CHAIR KUIKEN: All right. That's one.

MR. CORY: You're exactly on point, and it raises a critical point and theme in my testimony in that there are elements of what China is doing that the U.S. should emulate in terms of the U.S. government

identifying priority sectors where there is a coordination challenge or a conflicting challenge that prevents their industry from coming together to figure out how do we develop the standards and the platforms and the pilots and the supportive infrastructure that allows us together, collectively, to do better.

Because that is essentially what China has done, in many regards, and they have the power of compulsion. They can force their industry to organize and open their datasets and open their models, not for commercial reasons but for strategic reasons.

So that is why, again, in my testimony, focusing on robotics data infrastructure, it's just such a clear example where U.S. industry suffers from this coordination challenge, and the U.S. has this amazing organization, NIST, that has a proven track record of working with industry to develop the standards and mechanisms that allows the industry to get on the same page as it relates to data and data sharing, that supports them all.

So it's about emulating elements of it, where there are, obviously, not market values or

coordination values in the U.S. industries in these critical sectors, and then with the right institutions setting about the process of getting everyone at the table and figuring out, okay, this is a shared challenge, how do we get at this together, which NIST has done repeatedly in the past.

MR. LIN: I think my co-panelists said it well. I have nothing more to add.

VICE CHAIR KUIKEN: Okay. Then I've got a second round before Commissioner Miller comes after me for going over. The Commission recently put out a report on China's open source ecosystem, sort of two pieces to it that we emphasized. One, China is doing a fairly effective job of deploying open source models. I think the assessment that, at least I personally came to, was that China needed to leverage the open source community basically to catch up and to slingshot their way either closer or sort of side by side.

The second thing we talked about is data and all of the data that just comes out of their effective deployment of these open source models, and sort of

the robotics environment that you just talked about, Mr. Cory.

One of the criticisms that I got, you know, the love letters that you get after the Commission puts these things out, is that we were a victim of the Chinese propaganda machine, and they're actually not doing this well, and how dare the Commission go down this road and fall victim to it.

I've tried to wire-brush this assessment, and I'd love for you guys to tell us the Commission is dead wrong. I don't really want to put you in that place, but what's your assessment of where China is on the open source ecosystem and the data that they get out of the deployment of their models, and sort of what we talk about is the two loops in the reinforcement cycle, that Mr. Cory just talked about. Just give me your assessment on where the Chinese are in their open source ecosystem, what's your read on it, and then just go back to the data piece, as well, and that embodied AI part.

MR. CORY: I can lead off. I think you're exactly right, and the Commission's prior reports have

been exactly on point and right. And again, referring to robotics is a great example of that, because it combines the power of Chinese ability to subsidize deployment with creating an industrial data infrastructure layer. Because with every robot deployed you thereby generate another load of data. And by then imposing an open model system on that and then accompanying that with a unified data-sharing template or standard, you create a whole different industry ecosystem.

China already leads the world in robot deployment, and they have coerced them to use a single standard, and they are forcing them to use an open model. Like it's industrial-scale data generation in a strategic technology. So I think robots, the case is really clear, in that the Commission's prior work is exactly on point.

MR. LIN: The first thing I'd point out is -- well, first of all, I love the report.

VICE CHAIR KUIKEN: Thank you.

MR. LIN: But number two, China has adopted a deliberately open source approach when it comes to

building artificial intelligence models. And the debate that we're often having around model performance I think is a little bit of a red herring here, because that's ultimately not the discussion that we should be having. The discussion we should be having is around the speed and pace of AI adoption across Chinese society, across Chinese research institutions. And what we see there is that this open source approach actually makes AI adoption far easier. It lowers the barriers.

And also let's just not make any mistake about it. If you want to talk model performance, unfortunately, open source Chinese models outperform open source models everywhere else. They're very, very good.

And you see a far warmer embrace of artificial intelligence, in general, across Chinese society. There have been reports of frontier labs setting up tables outside of supermarkets to sign people up for AI accounts, again, right. So what you see is wholesale embrace and adoption of artificial intelligence, and what that means is you have a

society, therefore, that is going to be transforming and adapting far faster than we are.

DR. LOHN: Thank you. I agree that the Chinese models are at the top of the line. I know that some major U.S. companies use Chinese open models in their systems. The reason they do that is to protect their data, though, because they don't want to ship that data off to Alphabet or OpenAI or Meta, and having an open model allows you to do that.

But when I was in the White House a couple of years ago, when we were going around trying to convince the world to tear out Chinese telecommunications infrastructure, it was because we could offer this model, they could offer that model. And so their prominence in open source models allows them to distribute their infrastructure that they can siphon data off with.

So I think it's not the models directly, but the influence they get around the world as a result of those models that allows them to support their data acquisition.

VICE CHAIR KUIKEN: Thank you, Mr. Lohn, and

thank you, Commissioner Miller, for your forbearance.

COMMISSIONER MILLER: Commissioner Price.

COMMISSIONER PRICE: Thank you, and thank you all for your really excellent testimony today. I keep flipping back and forth through my notes on what you've all said and what you've submitted to us, on different questions. And it keeps coming back to the role of government and where we should be on that. And several of your policy recommendations I feel like tinker with it, but there's no bigger, broader discussion. So I was hoping each of you could comment on that. Maybe start with, any of you. Okay, Mr. Cory.

MR. CORY: A big picture question or request. I mean, in my opening remarks the U.S. is doing elements of what it needs to do across various agencies, but it lacks the central coherence and coordination. So I think what that inevitably leads to, as a starting point, is situating it in the White House with the OSTP and NSC and NEC, in designating data policy, or however you want to phrase it, as a national priority. And then, obviously, bringing the respective agencies

together under a clear vision, clear strategy, and a clear breakdown of who is doing what and where and how, and then obviously doing that in concert with Congress across sectoral priorities -- national security and critical infrastructure priorities.

Because I think, I mean, as a former government official it may be a bit of a bland recommendation, but it starts with the institution and the agency arrangements to enable a more effective response. Because at the moment it's very ad hoc, it's often reactive, and the sum is not more than the whole of pieces.

So the U.S. needs to get its act together, from an institutional perspective, and then the tasking perspective, and then obviously working with Congress on like, well, what are our marching orders on post-quantum, on AI robotics, on whatever issue it is. There is a central coordination challenge problem there lacking, in my view.

COMMISSIONER PRICE: Thank you. Mr. Lin?

MR. LIN: I'm not a political economist so I don't have an especially strong opinions around things

like wholesale industrial policy. But I will say this, which is it's important, obviously, to recognize the challenge and the threats that the Chinese system presents to the United States and to its allies, but we have advantages, as well, that come from our free and open system. We have certain competitive advantages. Let's make sure we don't give those up.

My focus, what I would talk about, is on the national side, on the military and on the intelligence side, where the role of government is front and center. So what I would say is we should have a strategy and an objective of campaigning in the cyber domain and getting to a place where we are not just capable of carrying off one-off operations but we're able to approach the problem from a perspective of multiple continuous operations on our end that feed off of each other.

So the question then becomes what are the types of capabilities and resources that institutions, organizations like U.S. Cyber Command, NSA, CIA, FBI, and even DHS, need to have in order to get to a place, to a posture, where we are able to campaign against

our adversaries and put them on the back foot.

That will require a whole-of-government effort -- let's not make any mistake about it -- and hopefully that's something that we can get to within the near future.

COMMISSIONER PRICE: Go ahead.

DR. LOHN: I tend to look at this as a whole bunch of different issues, like the biodata is being scooped up, there is implantation in the critical infrastructure, there's siphoning off data from the telecommunications infrastructure. Well, why? There's the distillation attacks. There's the smuggling of chips. And I think that as you are pointing out, me looking at them as each of these individual pieces is a problem. We suffer from a death by a thousand paper cuts or a boiling frog situation.

So I think if we're looking big picture we have to decide at what point would the aggregation of these be a red line of its own, and can we communicate those. We need to collectively think, what is the set of data that, if acquired, would be a problem for us,

and how can we communicate that that set should not be taken? Within AI that might be easier. It's a central focus of a technology, and it's got a handful of different aspects to it. But you might be able to say you cannot have all of these things or we will. Now, we'd have to be ready to act on our "or we wills," and I'm not sure exactly how strongly we want to do that.

COMMISSIONER PRICE: And on the AI side, aren't we relying on companies to police themselves?

DR. LOHN: Yes, we have been. I think that we should move away from that. California and New York have both tried to step away. S.B. 53 has some "thou shalts" for cybers and the RAYS Act also does.

When I was in the White House we tried a little bit to push in a couple of different directions to make companies that had highly capable AI systems meet some cyber standards, but it was maybe a little bit early. And now as we are seeing these companies develop capabilities that are really practical, that are finding vulnerabilities in software, and that have really clear military dual-use or economic

applications, it might be time for us to step up and put in some, you must meet these cyber standards if you have models that are this expensive, or if you have this much revenue.

COMMISSIONER PRICE: Thank you. Thank you all.

COMMISSIONER MILLER: Over to Chair Schriver.

CHAIR SCHRIVER: Thank you, Mr. Chair, and let me also extend my thanks to the witnesses. Really fantastic testimony, and I appreciate your comments thus far. I'm learning a lot.

I could take this in a lot of different directions just based on things I'm hearing and learning, but I think I'll use the time to drill down a little more on something that's already been raised, I think primarily by Commissioner Brands and Commissioner Hodges, and, Mr. Lin, your presentation depicting China as pre-conflict positioning and being able to hold things at risk.

And I want to sort of try to drill down from the conceptual to potentially to the very practical. I mean, we're just a year out from 2027. 1 August 2027 is the be-ready-by date, not necessarily the go-by

date. But if you could sort of best guess what is D-Day or D-Day minus 1 or 2 in terms of prepping the battle space, what might we expect?

And I might ask Dr. Lohn to also contribute to this, because I sense maybe a little bit of difference. I don't know if you all want to explore that or start taking swings at one another. Dr. Lohn, you suggested that there are red lines that China has respected, and I think you mentioned they wouldn't do water plants for fear that retaliation might be outside of cyber. Do you think that the red lines would apply in the case of conflict? I think you mentioned red lines a second time just now. Is it worthwhile communicating to China, through official channels, in advance, what those lines might be from our perspective?

I mean, I was not one of the optimists in the Obama administration when they had the deal. I took some heat from friends in the Obama administration when I said I thought it was foolish and not going to work. But presumably if you think the Chinese are open to setting red lines from themselves then they

would be open to receiving our communication as related to that.

Mr. Lin, maybe begin with what you might actually expect in the very sort of concrete, if there were a kinetic action how might this particular capability contribute or augment to the kinetic activity in the Taiwan Strait.

MR. LIN: Absolutely. Let me start there and then I'm also happy to chime in on red lines and enforceability and all of that fun stuff.

I think in the run-up to a conflict and then on D-Day itself, China really would have two objectives. One is to be able to disrupt our ability to project force. Ultimately there is the tyranny of distance that we have to deal with that they do not. And so being able to field forces, whether that's from Guam, from Hawaii, from the Continental United States, that is the American way of war. And so anything that they can do to disrupt mobilization on that front, they will almost certainly do.

I would expect them to go after our logistics networks. We rely extensively on commercial

providers, commercial logistics providers, even today. And we do all of that oftentimes on unclassified networks, understandably so. They're not going to be doing this on SPIR or JWICS. So if that is the case then we have to take a very close look at the resilience of those networks, the strength of those networks, ensuring that they are not compromised, that they cannot be compromised.

That is probably the most effective way to disrupt the actual military component of anything it is that we do, in addition to the social and political warfare that they would be waging against us at home, in order to sap public support for our actions.

And we know that this is what they'll do. They have written about it, publicly, going all the way back to *Unrestricted Warfare*, which at the time, I think for a very long time people dismissed as hyperbole, it was just the work of two senior colonels, it was a thought project that their version of the NDU, and people were debating for a very long time, well, it's published by China's NDU Press, not by the Academy of Military Sciences, and so we don't

have to take it too seriously. I think at this point that debate is over. That is how they think. Those ideas continue to permeate throughout Chinese military strategy and what they talk about. So that's the first part.

The second part, I think, comes down to red lines. I like the idea of red lines. I'm not opposed to them, in theory. The problem with red lines is that you have to be able to enforce them. And one of the key, distinctive qualities of the cyber domain is that it is very, very, very hard to enforce red lines. And part of this has to do with the deniability of actions and also, quite frankly, if we wait until they actually carry out the actions, it is a little bit too late for us to enforce the red lines.

So the red line should have been, well, you cannot pre-position malware in our critical infrastructure networks ever, in civilian critical infrastructure networks, and if you do there will be punishments. Because what they have done is effectively strapped explosives, the digital equivalent of explosives, to critical infrastructure

and said, "Oh, no, no, no. Don't worry. We're not going to set it off." Why would you even do that if you have no intent of using it?

DR. LOHN: I'm not sure that we actually disagree that much, but I'll play it through. I'm maybe a little bit skeptical that we can prevent them from taking these cyber actions purely on a cyber basis of our own. The red line I was thinking of is at what point would their incursion or attack cause us to go outside of the cyber domain and come back with missiles or something like this. So, yeah, I think cutting off our power infrastructure would get us out of that, so they won't cross that unless they are really motivated to.

Now, if we're in a crisis -- maybe I'll step back before that. Before crisis, I think that they already have achieved some deterrent effect against us, and some other countries have, because we would think about whether they would turn off things if we were to do stuff. So I think that already exists, and we should recognize that is the case.

Now, if we're at the crisis standpoint, where

missiles are already flying or people have already been sent around, then they have less of a reason not to turn it off, and they might be a step on a ladder. It's like we can flash your energy infrastructure.

I would also like to go back historically to try to set this in the context. I don't think that it's exactly a China problem. That's not where we fail the deterrence on this. Russia has been in our grids for well over a decade, and they pulled power twice on Ukraine long ago.

So I think that's where we fail to set this as a boundary that shouldn't be crossed. But on the optimistic side, if we're talking about a short duration leading up to a crisis, we can also look to how challenging it was for Russia to implement their cyberattacks in the Ukraine invasion in 2022.

So if you have to keep them out of a network for eternity, that's a difficult problem. If you just need to turn off their ability to attack you over a one-week period, I'm more optimistic about our ability to do that.

COMMISSIONER MILLER: Next up will be

Commissioner Shmavonian, who is joining us virtually.

COMMISSIONER SHMAVONIAN: Thank you. A really eye-opening discussion, and I appreciate everyone's time.

One of the benefits of going at the end is most of your questions have been asked already. So I'm going to pull this back a little bit and just ask the panel more broad-based questions. One, what, in your view, is the biggest blind spot, defensively, for the United States, either government or industry? And then two, what are our largest gaps, offensively? And we can just go down the panel.

DR. LOHN: I think that we have a variety of blind spots in how large or effective the theft is in the AI domain. I don't know what we have a good understanding of how many chips are being smuggled, and I think that will be a challenge that we can try to address, perhaps with more BIS, perhaps with location verification measures.

And I think that we don't have a good understanding yet of how effective this distillation attack is, how much is the gap between our leading

performers and Chinese leading performers a result of them stealing our data, compared to their own indigenous ability to keep up.

And then I think that we also have perhaps an enduring gap about how capable are we at defending against these distillation attacks. These models need to be served in order to be profitable. The attacks themselves look very similar to normal operations and don't require that many accounts in order to pull them off. So understanding what is the scale of theft and how much of an uplift it is and where we can inject ourselves to upend their operations are our biggest gaps today.

MR. LIN: As somebody who spends most of my waking hours thinking about cyber warfare, one of the things that I think is not necessarily a blind spot that the government has but I think more broadly American society has, is around the sheer speed, scale, and sophistication of Chinese cyber operations in the United States.

This is obviously a highly technical matter. It's a complex subject. But I think we have to do a

far better job of communicating the scale of the threat and the implications of what this means for the American public. And we have to do it today, and I think that this is something that should prompt Congress to hopefully take far greater action in this space.

MR. CORY: Rounding out from my commercial, trade, and security perspective, I think the biggest blind spot as I see it, vis-à-vis U.S.-Chinese tech competition, is on the foundational issue of Chinese government access to data, and what that actually looks like in practice, and what is the nature of the relationship in practice between the Chinese government in these tech firms and providing greater information and transparency about that, because that is foundational to our efforts to counter them as it relates to concerns about resilience and trustworthiness.

I think from an offensive perspective, from a commercial, trade, and security perspective, the biggest gap we have at the moment is having a coordinated strategy and set of tools to counter

China's ability to leverage price as their key differentiator to enter and seize market share overseas, and doing more with capacity building and technology and such with these foreign government officials and procurement officials who just don't have the expertise or the capacity to assess non-price factors. In that Chinese firms succeed because they can come in with a really low, upfront price, low investment cost, and highly visible training commitments, but then the longer term risk, resilience, ecosystem lock-in, state access things are much harder to measure in cost.

So we need to do a better job of highlighting what the full sort of lifecycle costs of choosing a Chinese provider is before they just get suckered by the upfront, visible cost differentiator that the Chinese excel at using.

COMMISSIONER SHMAVONIAN: Great. Thank you. One quick follow-up, changing topics a bit. We have a number of ISACs, Information Sharing and Analytic Centers. Do we have an ISAC for data? Do we need an ISAC for data? Do the existing ISACs get information

to them related to data mining and data risks? I would love some insights, to the extent you have it, with respect to how the U.S. government is supporting our industry in just the information-sharing piece, if you have any.

MR. CORY: I'm going to refer to one of Andrew's colleagues, Helen Toner's testimony last week, which I think got to, I think, the critical issue in the context of adversarial AI distillation attacks, in that there clearly needs to be more thought put into the ability for public-private coordination and information as it relates to this form of attack. In that this may be taking place now, to some degree, but I understand that there's uncertainty of whether existing authorities are broad enough to allow them to share the type of information they want and for the industry itself to coordinate amongst itself. And I should mention both of these issues were flagged in the White House memo that came out last week in relation to the adversarial AI distillation attacks.

So I still think there's more for the U.S. government to do to ensure that there is clear, open

communication and information sharing amongst the industry and with the government.

COMMISSIONER SHMAVONIAN: Great. Thank you. And thanks to the Chair for letting me go a little over.

COMMISSIONER MILLER: It was my great pleasure. Last, but never least, Commissioner Stivers.

COMMISSIONER STIVERS: Thank you. I'd like to delve back into kind of the heart of your testimonies regarding China's acquisition of data system. Mr. Cory, in particular, you stated that there are no restraints to the Chinese government access to Chinese companies' data, and I think you all agree with that. We know China's legal framework, whether it's the Data Security Law, the Cybersecurity Law, the National Intelligence Law, all compel Chinese companies to provide data when asked for it.

So my question to you all is, is this system a well-oiled machine that works with precision, or are there weaknesses that can be exploited? And maybe, Mr. Cory, we can start with you.

MR. CORY: I mean, it goes to the love that I would have for the request for the U.S. government to

delve into this, to bring some transparency to the nature of how this works in practice. You all, I'm sure, have heard many debates and discussions about the nature of the National Intelligence Law and the Data Security Law and the standing provisions it provides the Chinese government, but what we still really lack is sort of a comprehensive assessment of, well, how do we think this actually works in practice.

And we are seeing anecdotal datapoints over time come out regarding Chinese government and ByteDance relationships and what data is shared there. But these anecdotal datapoints point us towards what we think is happening, but we just don't have a comprehensive view of that central sort of relationship and process. And I think that's critical.

I mean, it's funny, ironic, right? The U.S. government being a champion for safeguards and protections around government access to data, vis-à-vis, obviously Schrems and Snowden and such, but, ironically, the U.S. government's reaction to all of that is to actually put it in the top tier of models,

vis-à-vis transparency, safeguard, and redress around government access to data. So it's ironic that Europe, obviously, has not stepped into this gap, but it's incumbent for U.S. tech companies who are facing slander, essentially, in foreign markets, because Chinese firms are pointing at the U.S. and going, "CLOUD Act, government access to data," even though that's not how it works, while no one is pointing at them and the legal black hole that they operate in, vis-à-vis Chinese cloud companies and how they work with the Chinese government.

COMMISSIONER STIVERS: Mr. Lin?

MR. LIN: I think it's indisputable at this point that things like the Data Security Law, the National Security Law, these are valuable strategic levers for the Chinese government to pull on, and they do. As to how successful holistically all of this is, how, in your words, is this a system that is a well-oiled machine, I think it's hard to say.

But I will say there is valuable empirical evidence that we can look at. If you look at the data compromise and leaks of a mid-tier defense cyber

contractor called iSoon, that happened about a year and a half, two years ago, you start to see some evidence of not just how the National Security Law has been used to support them as a defense contractor but also looking at things like military-civil fusion, where you've got one of their key backers being Qihoo 360, which is a sanctioned company but is effectively like the Chinese version of Kaspersky, and the type of support and assistance that they're able to receive, both from an otherwise commercial provider, and then use that to be able to support their military and intelligence apparatus.

I think evidence like that is valuable, and it suggests that, again, we shouldn't underestimate the extent to which they will pull on these levers.

COMMISSIONER STIVERS: Okay. We also shouldn't overestimate it either, right? Mr. Lohn.

DR. LOHN: You asked about vulnerabilities in their well-oiled machine, and I don't know about in the machine itself, but as they pull in data maybe we can recognize that the CCP is more vulnerable to information than we are. So AI is very difficult to

control and to contain. It says things, whatever is in there, and people can grab it out. We have an opportunity to shape a little bit of the narrative worldwide, or even within China, as we distribute them. That's partly why they are blocking our models from being accessible there.

They also would have noticed, in the Anthropic leak recently, that there was some code written in there to try to poison models that were trying to do distillation. So there is at least one flag that they would have noticed that the companies are taking offensive action to disrupt the data that flows into their systems.

COMMISSIONER STIVERS: Okay. Thank you.

COMMISSIONER MILLER: We have a few additional minutes for any Commissioners that have questions, some final questions. I'm going to kick us off, because I want to keep going down that line about distillation.

We know it's a problem. The U.S. government has called out companies like DeepSeek for doing this to our large AI companies. But I thought, Dr. Lohn, you

had a very interesting section in your testimony where you said we may not know how to deal with it. "It is not certain whether it is prohibited by the Computer Fraud and Abuse Act," related to cyberattacks. "It's not certain whether it's prohibited by the Digital Millennium Copyright Act, and it is not certain whether it amounts to economic espionage, according to Title 18."

I'd like to ask each of the panelists what do we do, what should the U.S. Congress do, about the growing problem of distillation?

MR. CORY: I'll start. I mean, talking to a frontier lab earlier this week about the issue, they recognize it's obviously a growing interest on the Hill. Their reaction was that we should, obviously, ease into our response of it to fully understand the scope, scale, the nature of the risk, in order to avoid mis-reacting and thereby undermining sort of U.S. AI.

And it comes back to the point, I think -- and again I'm going to quote Andrew's colleague here, just because I thought her testimony last week was so good

-- but looking at his holistically in terms of what can be done about preventing distillation as part of protecting the full pipeline of U.S. AI IP, and that countering distillation should just be one measure amongst many, to protect the AI ecosystem.

But I think the starting point for all of this, back to my prior point, is deepening and expanding security, focus, collaborative arrangements between the U.S. government and the AI companies, making sure there's a legal architecture for that, so everyone is clear exactly that they can do that, and then providing antitrust guidance to enable U.S. AI companies to collaborate on defensive measures as another sort of current gap.

And then combining that with law enforcement and intelligence collection tools to improve our understanding of Chinese efforts. Again, just to get a better understanding of the threat picture. And from there, more substantive legislative and policy changes will likely come, but that's the sort of foundational starting point, as best I understood it.

And the final comment from the frontier lab was

like, this obviously is going to get worse, this is obviously a major concern, but we need to sort of slow our role in how we react to it and do it systemically and coordinated, so that we get it right.

DR. LOHN: Kyle Miller, who is back here, and I have been talking about this a bunch. He has been leading our efforts at CSET.

There are a couple of things. One, he scoured the academic literature and the answers are uncertain. So we don't know how big of a threat this really is, so if you can support research at large scales on newer models, that would be helpful.

But it struck me that in these calls from the companies they were asking for investment to build larger models, but they weren't saying, "We can defend this in these ways." And so I'm questioning whether they can, and I'm trying to look at how big of a problem is that, or how challenging is the defense.

And we were doing back-of-the-envelopes yesterday, actually, to see what fraction of the total user base is being used for distillation, what fraction would you need, how big is the haystack, how

small is the middle, and differentiable are the queries? And it came out less impossible than I anticipated, but very challenging.

So I think that I would ask for you to push on the companies and say, "Can you pull this off? Can you actually defend this?" Because it's not Congress' job to come up with the technical defenses, but maybe it is to say are these sufficient for us to justify our investments.

Separate from that, if that's a challenging case then at the trillions of tokens standpoint, the haystack is too big on the endpoint, then you might have to look more at the front point, defending forward to say where are these attacks coming from and can we disrupt them using our national technical means.

COMMISSIONER MILLER: Okay. Commissioner Slevin.

COMMISSIONER SLEVIN: Thanks. This is going to be brief, probably, but last month China launched the World Data Organization -- I think it was referred to in at least one of your testimonies -- intended to shape global data governance, maybe establish norms.

It is very early, obviously, but what would you look for to see if this is the kind of thing that gets any traction, and how should the U.S. respond or try to compete?

MR. CORY: An interesting development, and I was talking to some U.S. and other foreign government officials about it. They are obviously taking a keen interest in it. It is interesting because of its lack of context. Quite often China announces these major initiatives, the Global Data Security Initiative, and it launched a Cross-Border Data Flow Initiative a couple of years ago, and they are all generally in a context. This one is sort of weirdly not.

So it's unclear just how much emphasis and how important it actually is. But it's certainly gotten everyone's attention for what it could potentially be, as a platform for international engagement. And it's even unclear as to whether it's government and private sector, or is it only private sector, is it civil society? It's unclear what its membership will be made up of and what its actual work agenda will do.

So I think, for the Commission and for the U.S.

government, it's obviously something to watch very closely, how it evolves, how they use it, how extensively they draw folks into it, how connected it is to their domestic apparatus in terms of getting them to focus on standards and laws and regulations, that obviously reflect Chinese preferences.

But I think one way to look at it is that it's China's effort to change the normative discussion around global data governance in a way that reflects their preferences. And in talking to folks that deal with Chinese officials in many more intellectual bodies, it's something China has really struggled with. They are far stronger on a restrictive, defensive basis, because that lends to their strengths of sovereignty and control, but in terms of setting a constructive, positive vision for how China wants to see global data governance, they obviously really struggle because they love control, and that's at odds with it.

So it will be interesting to see whether they pick up and run with it, whether they see it at U.N. discussions and other regional bodies, like how sort

of comprehensive the push around the World Data Organization is. And if, in 12 months' time, we see they have ceding it across multiple forums and they have held many meetings, then it's like, okay, this is a real thing that they are operationalizing.

COMMISSIONER SLEVIN: Thanks. Any additional comments?

DR. LOHN: Not much. I would just say that maybe it fits in as part of a larger campaign that I'm hearing about, where they are trying to influence standards across a wide spectrum of areas, and we're ceding a lot of that by withdrawing ourselves at the same time.

COMMISSIONER SLEVIN: Thank you, Commissioner.

COMMISSIONER MILLER: Vice Chair Kuiken.

VICE CHAIR KUIKEN: Thank you very much, Commissioner Miller, and thank you. I heard Commissioner Schriver thank you for your testimony. I want to make sure I do it too. It's been an absolutely fantastic panel, so thank you.

Commissioner Slevin decided to go after the World Data Organization question, so I appreciate that one.

One of the things that Commissioner Schriver and I have been talking about when we do various events is this idea of convergence and adoption. So what I've been saying is the watch word for 2026 is convergence, and the reason I say that is there is this incredible sort of amount of accumulating data. We now have embodied AI, creating more data. And we have these models that are becoming increasingly effective. So over time more data, better models. These things are going to start converging with biotech, advanced materials, quantum science, whether it's compute, communications, or sensing.

How should we think about convergence and adoption here in the U.S. Is it just better data strategy, going back to what we were talking about earlier? Is it trying to prevent the Chinese from doing convergence and adoption? I don't think that's feasible. Is it more money for the sciences that are not AI, because the AI flywheel is going and now we need to think about how we can think about biotech and pharmaceuticals and all these other areas? I would just welcome your views on this. Anyone who wants to

answer can go, and then I've got one more question.

MR. CORY: I mean, it is the flywheel, and it is the nature of network effects, just being supercharged in the age of AI.

There's been a longstanding debate about, obviously, China's natural sort of data resource, domestically, and the fact that they have long put up walls around it. So from a quantity perspective, they have always had a lot. But quality matters more so in terms of AI model training. So that's why I think their restrict outflows, maximize inflows is important for their strategy, because they need that diversity more so than U.S. firms, so we're just naturally global, and building a more comprehensive representative dataset for training.

I think from a U.S. government perspective it's about where there are conflicts to or barriers to convergence in specific sectors. Then that should be something to take a specific look at, so the individual firms are operating in a vacuum, that they can work with partners, they can work with NIST, they can work with Commerce to figure out, okay, how do we

aggregate and share and maximize the value of the data we have, to some extent. I think, again, that's a common theme in my advocacy for a U.S. data strategy and such, taking a far more targeted approach for U.S. government intervention.

I mean, again, but it's also doing everything the U.S. government can to support its firms competing for market share around the world, because the future dataset they use is in play now, and ensuring that Chinese firms aren't able to use the unfair advantages they get at home to seize market share over U.S. firms, using all their tips and tricks. So it's about ensuring the U.S.'s data lead, for lack of a better phrase, is that they maintain that in foreign markets.

VICE CHAIR KUIKEN: That was helpful. I have one more question, but go ahead.

DR. LOHN: I might add quickly that I don't think convergence means centralization necessarily. We look at these big AI model providers and think that they're the whole story, but I think that a lot of the convergence will happen at lots of very small players who figure out how to use that model for their

application. Now, the types of defenses you would implement, those are different. You can't just target the big one and say thou shalt. You need to uplift the whole level. A lot of that happens at places like CISA, doing what are the Known Exploited Vulnerabilities list, and the CBEs list, and NIST lifting up regulations and guidance overall.

VICE CHAIR KUIKEN: Mr. Lin, Dr. Lin, you are one of the first witnesses I've heard talk about Title 10, Title 18, and Title 50 all in the same breath. It was refreshing to hear. So you definitely know the nuances of the American government and cyber operations.

I was listening to the conversation about distillation, and I was remembering one of the first accounts I worked on when I was on the Armed Services Committee was the IED Defeat Organization. And of the things that I learned over the years of working on that account was there is a measure-countermeasure cycle that goes very quickly when you're in conflict. And distillation is a countermeasure to some of the measures that the U.S. government deployed to sort of

constrain the Chinese ability to accelerate in AI. So as we continue to do export controls, they will continue to pursue distillation. Until we find a counter to distillation, there will not be sort of the next cycle.

So as we think about distillation I do think we have to get after that problem, but I also think we need to be thoughtful about how we do it, and make sure that whatever we decide to do is effective.

And on that point, Dr. Lin, one of the things that I've heard you talk around, and Commissioner Miller just talked around it a little bit, as well, is at what point does the U.S. government just need to decide that we're going to conduct cyber operations against Chinese companies?

MR. LIN: I mean, I think the time should be now. A lot of what we're talking about, I think we're still wrestling through, is how do we better protect ourselves, and I think that's obviously very important, and I don't want to discount that. But I think, again, at the end of the day cyber is one of these things where, so far at least, the curve has

been we spend more and more on cybersecurity and on data protections year over year, and somehow the results get worse and worse. And that's a cost curve and we're on the losing end of that cost curve.

So I think the question that we should be asking ourselves is what is it going to take to change that. Because at some point we will just spend ourselves into oblivion, while not necessarily improving the results. So when we look at, ultimately, thinking very simply about how do we change adversary behavior, protection, defense alone is just not enough. We have to be thinking holistically across the entire spectrum of capabilities that we have.

Now, to be clear, I am not suggesting that we don't conduct offensive cyber operations. I think the key point here is that when we think about the types of operations that we're conducting they simply cannot be done in a one-off fashion. We have to be thinking holistically, how do we build a system, with both people, organizations, authorities, and capabilities, that enables us to campaign offensively, and "campaign" being the operative word here.

COMMISSIONER MILLER: Commissioner Hodges will bring us home.

COMMISSIONER HODGES: Thanks again to everyone. So building off a couple of the questions that were asked by Commissioner Slevin and Commissioner Kuiken, earlier, Mr. Cory and Mr. Lohn, you spoke about efforts to set the architecture framework on tech, data for the next 10 years -- I think it was you, Mr. Cory, who used that time frame -- specifically with the idea of setting standards that are favorable towards the Chinese preferences.

What's the time frame on this? Is it a year, two years, three years? Are we looking at a matter of months here? Because I've had conversations that kind of seem quite alarming to me, so I'm interested in your perspective.

MR. CORY: That's a good question. I do a lot of work on technical standards, and it's something that China has prioritized and supported for some years now, but through somewhat ineffective measures, subsidizing engagement, and providing prizes for submissions, so the quantity over quality. But as

soon as they submit it to the standards body, wherever it may be, in Switzerland they're out shopping the next day because they've gotten their bounty and they've got back.

They are increasingly sophisticated and better at it, and in sectors where they are closer to the leading edge, like in physical AI, they will be the ones at those bodies having real impact on standards. So I imagine it is happening now.

The closer they are to the edge, where they have that technical, tacit knowledge is where they will be having the greatest influence on the setting of technical standards, and that's just going to be happening across the board.

But, I mean, standard setting is America's sort of superpower, that is unrecognized. American firms are incredibly good at it and have been doing it for decades, and they remain good at it. China recognizes it's something they are weaker at, but there is a concerted, ongoing government effort to support Chinese engagement and influence.

The easiest thing that most researchers focused

on is Chinese leadership of standards bodies, because that's an easier measure. But that doesn't equate to influence, and what matters is the technical merit of the submissions they make, and in a growing range of technologies they're getting better at that.

COMMISSIONER HODGES: Thank you. What would you say, and I guess this is a question for all of you, sort of the gap between the U.S. lead when it comes to 6G technology and Chinese technology? How far apart are we in that regard? Mr. Lohn?

DR. LOHN: I would have to get back to you. I haven't gotten up to recently on 6G. We can get back to you.

COMMISSIONER HODGES: Thanks.

MR. LIN: That's outside the domain of my expertise.

COMMISSIONER HODGES: Okay. Thanks.

COMMISSIONER MILLER: Okay. Well, thank you very much to our three witnesses. We are going to take a 10-minute break and return at 11:25 for Panel II.

[Recess.]

PANEL II

INTRODUCTION BY COMMISSIONER SLEVIN

COMMISSIONER SLEVIN: Welcome back, as Panel II gets seated. We'll begin shortly. This next panel is entitled "China's Data Acquisition in Practice -- Vectors, Targets, and Implications for the United States."

With us this morning, Dr. Gregory Falco, Assistant Professor at the Sibley School of Mechanical and Aerospace Engineering at Cornell University. We have Dr. Chris Miller, Professor at The Fletcher School at Tufts University. We have Diane Staheli, Senior Staff Member, Cyber Security and Information Services Division at MIT's Lincoln Labs. And finally we have Mr. Edward You, Founder of EHY Consulting. Thank you to our witnesses for being here.

We can get started with Dr. Falco.

STATEMENT OF GREGORY FALCO, ASSISTANT PROFESSOR, SIBLEY SCHOOL OF MECHANICAL AND AEROSPACE ENGINEERING AT CORNELL UNIVERSITY

DR. FALCO: Commissioners Miller, Slevin, and members of the Commission, thanks so much for the opportunity to testify today.

As an engineering professor, we build defense and aerospace systems for our national security ecosystem, and my testimony is based off of some of the threats that we have discovered as we build new secure-by-design systems, that others are doing to us.

The central point that I want to make is that China's data strategy is moving from stealing information to modeling behavior. China is not only trying to collect high-value data but they are very interested in low-level telemetry -- power traces, system log files -- that becomes interesting only at scale. So the target is not really our behavior, but it is our data in concert with the context of our behavior.

Let me start with some examples of the tactical edge, so drones. The most valuable data from a drone

is actually not the imagery you might grab. It's not from the payload itself. The metadata from the drone tells you about how the system lives, how it operates. GPS positioning, RF transmissions, power consumption, and motion data can really reveal what we are intending to do with these systems. So for example, a system that holds position with a stable power draw can indicate persistent surveillance of an operation, whereas burst movements and fluctuating power can indicate evader pursuit or testing regimes.

The patterns are not really theoretical. These are observable and they are repeatable, and that is what makes them interesting. So at scale, they allow our adversaries to interpret what our capabilities are and what we want to do.

We are generating the data on a regular basis that adversaries are interested in, just because we're using our systems, just because we're going through our operations. And what's really changed is the ability to analyze this data at scale. Historically, the bottleneck was the human operator, the human interpreter, but now we have machine learning

algorithms that are able to ingest massive amounts of data, and then we can contextualize that data with things like LLMs, that would help us to really interpret what's being used and why we care about these systems.

The systems that they are collecting on do not require perfect data. They could be very messy, but they could still extract patterns and insights, and that is where the concern is. AI is starting to turn data exhaust into actionable intelligence.

And the same pattern we see appears outside the tactical edge in scientific infrastructure. Now, don't get me wrong. As a scientist I'm not arguing that scientific collaboration is inherently malicious, and the risk is not the science itself. But there is risk in that persistent scientific infrastructure is persistent sensing infrastructure, in locations that might be geopolitically interesting.

So China is really heavily investing right now in research stations in places like the Arctic and in the South China Sea, where they would like to have persistent sensing and surveillance. And they are

framing these as, oh, we want to do ionospheric monitoring for space science. But what are really looking at. You're looking at when rockets are launching and when we're doing maneuvers on orbit. They might be looking at subsea mapping to say, oh, we want to know where mining operations are or how the climate is changing. But no, they are trying to look at where our cables are, so they can cut them at the right time.

The issue here is control of this data and who stores it, how it's released, and who they are collaborating with, at what time, and we need to be on top of this.

The logic that I'm presenting is sent into space, as well. China is not just tracking our spacecraft, but through proximity operations they can observe how our spacecraft respond to different stimuli. A system approaches our spacecraft, it triggers a response, and then it gets to observe what happens. It reveals operational thresholds that we care about and our system behavior.

And at the foundation of all of these

technologies are our semiconductors, and every semiconductor will generate electromagnetic emissions, power traces, and timing behavior. And these signals, when a system is active, we know what it's doing based off of these emissions. The risk is not about the compromise of the chips. It's about the observability of the chips, to be able to interpret what's actually happening. And we've been spending decade and billions of dollars trying to secure access to things, but we're not necessarily obfuscating observability.

So this leads to the central concept that I want to present, which is China really care about pattern of life. By observing behaviors over periods of time, they can infer purpose and our roles and our future actions. And this is about anticipating what we can do and what we will do, not just about observing things at the current state.

It represents a much broader shift in intelligence gathering. And historically, intelligence gathering was based off of human intelligence, classified collection, direct compromise, but that's not how we do it anymore. We

can do this by derived data flows from aerospace and defense systems, that are pretty freely observable.

To respond effectively I'd like to highlight a couple of priorities.

First, we need to strengthen restrictions on high-risk foreign components. We've already done this through the National Defense Authorization Act from December, where we've seen limitations of Chinese components in drones. We need to double down and do this for more sectors.

But we also need to pair these with viable alternatives that will not compromise our existing supply chains, which we kind of are seeing as a result of the December restrictions. We have a long way to go.

Second, we need to reinvest in dual-use science and global presence. The reason why is because China is filling gaps that we have left. They are populating remote research environments, and we need to expand international partnerships so we have access to the data that they would have had if they jump in there.

Finally, we need to promote secure-by-designs through standards and procurement. We have to build these systems secure from the start and prevent observability, not just access.

In closing, I'd like to present three core takeaways. First, data exhaust is now about intelligence gathering. Second, AI has removed the bottleneck to exploiting data at scale. And finally, this is a competition about data aggregation, not specifically about access. Thank you.

[The prepared statement of Dr. Falco follows:]

COMMISSIONER SLEVIN: Thank you. Dr. Miller.

STATEMENT OF CHRIS MILLER, PROFESSOR, THE FLETCHER SCHOOL AT TUFTS UNIVERSITY

DR. MILLER: Thank you very much for the opportunity to join the Commission today and testify on a topic of connected cars. And I commend the Commission for tackling this topic right now, given the extent to which connected cars and foreign investment is in the news just this week.

What I'd like to suggest here today is that we should see modern automobiles not just as forms of transportation but as sensor platforms that are gathering a wide variety of data, storing it, and transmitting it in ways that create risks, both of espionage but also of sabotage.

Most people think of cars as just the device that gets them to and from the place of work or the places that they're going, but modern automobiles can't function without dozens of different types of sensors. Traditionally, most of the sensors inside of a car were analyzing the car's own operations -- monitoring the engine, for example -- but over the last decade we have seen a proliferation of sensors across cars, both

to monitor the drivers themselves and also to map the external world. And this has brought to the fore a series of data governance concerns that I believe the automotive industry is not on its own properly grappling with and requires government action to monitor and to address potential risks.

First, to lay out the types of sensors that we ought to be worried about, we all know that cars have GPS sensors that track location, and this alone could be a valuable asset for a foreign adversary. But more interesting are the sensors that look inside and outside of cars. Many cars, for example, have camera sensors and audio sensors that monitor the driver, listen to a driver giving voice commands to the car, for example, or notifying the driver when it looks like they're no longer paying attention to the road. But, of course, cameras and audio sensors inside of cars could also be valuable sources of intelligence for a foreign adversary.

In addition to this, there are an increasing number of sensors outside of cars -- lidars, cameras, radars, and other sensors -- that are mapping the

external world. And this is a very important development. It is driving increasingly autonomous capabilities in the automotive sector, but it raises questions about where this data is going and who has access to it.

I certainly wouldn't support any limitations on the gathering of this data by companies, but we must ask questions about who has access to the data once it's gathered. It could be very useful, for example, to a foreign intelligence service if they had almost real-time visibility into who is driving by certain types of critical infrastructure, for example. It has been reported by some cybersecurity researchers that certain types of automotive cameras cannot only see the world, they can identify license plate numbers or have facial recognition capabilities. So the intelligence implications of this data is, I think, increasingly significant as more and more cars are deployed with a larger number of sensors.

And just reading the news we see many examples of this type of data being used by different governments around the world for intelligence purposes. It has

been reported just in the last couple of weeks that Israel hacked into Iranian traffic cameras to track the movements of senior Iranian leaders. Both Russia and Ukraine are alleged, in media reports, to have undertaken similar types of cyberattacks against each other, and if these countries are doing it we should assume that China is doing it, as well.

Which raises the question of what are the steps that we could take to mitigate against these risk. And it is worth nothing that our European allies, as well as Israel, have been increasingly taking steps to examine the cybersecurity implications of connected cars and to mitigate against them by imposing data protection rules or by not allowing certain types of critical components to be sourced from foreign adversaries.

It has been reported, for example, that multiple European governments have advised military personnel not to drive Chinese-made cars onto military bases or near sensitive military facilities. And China, itself, has, over the last several years, restricted where certain American-made cars can drive within

China, evidence that Beijing takes seriously exactly this type of risk.

So I think it is high time that we take seriously the espionage implications, as well. Listening to my fellow panelists talk about China's data aggregation strategy, automobiles are certainly an important part of this effort.

If the first risk is espionage, the second risk, I think, is sabotage, because cars today are increasingly software defined, which raises questions of who can update the software. This is important both for the operating systems of cars but also, in particular, for the software that manages the battery, the battery management system. And in particular, when I read news headlines about automakers considering joint ventures or partnerships with Chinese battery manufacturers, I think we should be asking very careful questions about who controls the software that dictates how the battery operates.

It has been widely discussed, for example, that a compromised battery management system could cause a battery to set on fire, which, of course, would not be

a good thing if it was inside your car.

So although it sounds perhaps extreme to worry about sabotage in automobiles I think it's not difficult to imagine scenarios in which thousands of even millions of cars halting on our streets could be an obvious tool for a foreign adversary, and China is certainly considering these capabilities.

So the espionage and the sabotage risks, I think, are real, and they deserve to be addressed, and there are several capabilities we have to begin to address them. The first is an authority called ICTS at the Commerce Department, which has been used in the past couple of years to restrict sourcing of certain components as well as software from Chinese firms for deployment in American automobiles. The Connected Car Rule, as this is referred to, is, I think, a very targeted measure that only focuses on connectivity equipment that is relevant for automobiles as well as software written by Chinese providers, and it limits their use in automobiles sold in the United States. I think this is an important effort and it should be strengthened and expanded, in particular, by providing

codification for ICTS, which currently has as its legal authority an executive order, but which I think should be codified by Congress.

Second, we need to think more carefully about encouraging our allies to take similar measures, because just as we face risks, so too do our allies, and many of our allies have more Chinese cars on their roads than we do. That's true in Europe. It's true in Australia. It could soon be true in Canada, as well, where these countries are becoming increasingly reliant on Chinese cars.

So in sum, I think we must take the risk of the data collected by automotive components seriously. We must take seriously also the risk that if we are sourcing key components and key software from China that this presents a significant risk of both espionage and sabotage.

Thank you very much for having me.

[The prepared statement of Dr. Miller follows:]

COMMISSIONER SLEVIN: Thank you, Dr. Miller. Ms. Staheli.

STATEMENT OF DIANE STAHELI, SENIOR STAFF MEMBER, CYBER SECURITY AND INFORMATION SERVICES DIVISION, MIT LINCOLN LABORATORY

MS. STAHELI: Thank you to the Commission for having me here today to speak about Chinese data strategy, advanced artificial intelligence, and cybersecurity.

As the Commission's previous report has noted, China's approach to artificial intelligence is built on an open model strategy and dominance in manufacturing, creating a feedback loop that enhances its long-term AI competitiveness. By promoting open models that are inexpensive to deploy and customize, Chinese firms make it easier to integrate AI into industrial settings, like factories, logistics, and robotics. These deployments generate vast amounts of real-world data which can be used to train and improve models.

Access to large-scale, real-world interaction datasets could give China a competitive edge in developing the next generation of large language models. Many researchers predict future advancements

in LLMs will depend on three key areas: richer real-world awareness, stronger multistep reasoning, and physical intelligence, or the ability to act through machines in the physical world. Domains like robotics, autonomous systems, and code generation are already benefitting enormously from this type of data.

China's regulatory environment amplifies its data advantage. Privacy protections and norms are much less restrictive than in the U.S. or the EU, particularly in areas like e-commerce and public security. This allows for large-scale ingestion of biometric data, video feeds, and location histories into AI pipelines.

Chinese AI firms also benefit from access to state-collected datasets and commercial data from apps, payment systems, and logistics platforms. This create a rich corpus for training models in areas like facial recognition, crowd analysis, and vehicle tracking, all of which have commercial and state security applications.

China's state strategy further aligns public and private interests in AI. Data is treated as a

strategic national resources, and organizations are incentivized or compelled to share datasets and models across sectors. This accelerates progress at a system level. In contrast, U.S. entities often treat data as proprietary, with regulatory and business constraints limiting cross-sector sharing. Even if U.S. organizations collectively hold more data, it is harder to combine and reuse at scale for national AI objectives.

Export controls on advanced hardware have slowed China's progress on frontier AI models, but the gap is narrowing. Chinese labs have optimized software and model architectures to maximize efficiency on available hardware, achieving significant gains without large accuracy losses. Additionally, evidence of intellectual property theft through distillation-style attacks on closed-source models have been observed. These adaptations, combined with China's data advantages and coordinated strategy could allow it to close much of the capability gap in real-world applications even if it lags behind on frontier benchmarks.

Data poisoning attacks exploit the vast datasets used to train LLMs by injecting malicious or biased data. For example, attackers could plant fabricated information on public platforms that organizations create for training data. This could suddenly manipulate a model's behavior such as associating neutral terms with negative connotations or embedding trigger phrases to illicit specific responses.

Detecting poisoned data is challenging due to the scale of the training sets and the subtlety of the attacks. Poisoned data may constitute only a small fraction of the corpus, making it difficult to identify.

It's important to note that data poisoning is a general security concern in machine learning and not unique to any specific country. However, U.S. reliance on a small set of web-scraping providers creates a systematic vulnerability.

China's open source AI ecosystem accelerates innovation but also introduces security risks. Companies often build on each other's models, including U.S.-developed ones, creating derivative

models that can cross borders. A single security flaw in model code or tools can propagate across organizations and products, complicating vulnerability attribution and remediation. Again, this isn't unique to China, but it is broadly true of the open source software ecosystem.

Open source platforms are also attractive targets for bad actors. Malicious code can be embedded in malware depositories or scripts and redistributed as legitimate contributions. Organizations should treat AI artefacts as software supply chain components and by applying standard security controls like scanning, provenance checking, and other best practices. The combination of emerging model security tools and existing practices can help mitigate some of these risks.

Organizations often seek the best AI performance at lowest cost. Non-frontier models that deliver competitive performance at reduced costs may be more attractive for startups, small business, and governments with limited resources, especially those in regions or countries that have a mobile-first

innovation strategy. This reflects a natural progression of technology where advancements eventually become accessible to broader audiences at lower price points. Open models cloud APIs, and embedded AI and commodity hardware are accelerating this trend. In addition to benchmarks, costs should be treated as a predictor of China's global AI diffusion.

To better assess model capability in general and to ensure better model security, we need further advancement in measurement and testing infrastructure. Benchmarking AI models is useful, but it currently lacks standardization. Many benchmarks are biased, oversaturated, or tailored to specific tests, which can inflate results without reflecting real-world performance. To address this, the field needs independent evaluators to administer benchmarks under transparent protocols and published unbiased results. Investment in better measurement methods and reproducible testing infrastructure is also essential.

Transparency for model providers is another key area for improvement. Standardized documentation,

such as data and model cards, should describe training data sources and filtering processes. This would help detect data poisoning and systemic bias. Structured red teaming exercises and responsible disclosure of vulnerabilities are also critical for improving AI security.

Finally, the AI community needs robust mechanisms for sharing information about threats and vulnerabilities. This includes publishing security reports, sharing indicators of compromise, and establishing formal channels for collaboration. Strengthening these practices will help build collective defenses against emerging risks in the AI ecosystem. Thank you.

[The prepared statement of Ms. Staheli follows:]

COMMISSIONER SLEVIN: Thanks very much, Ms. Staheli. Finally, Mr. You.

STATEMENT OF EDWARD YOU, FOUNDER, EHY CONSULTING LLC
AND FORMER FBI SUPERVISORY SPECIAL AGENT

MR. YOU: Good morning, Mr. Chairman, Mr. Vice Chairman, Commissioners. I want to thank you for the opportunity to be able to present to you all.

I benefit from going last, and I wanted to start by saying that I think we are very much crucially at an inflection point, that it's not just about data acquisition but it is looking at data operability. And especially when it comes to China, I thought I would start by using biotechnology as a reference point and to provide some context.

There is a reason, because China is intentional about looking at biotech and data specifically, because if you look at what is happening right now, they are facing some real-world challenges. They are facing climate change, which is impacting food security. They are looking at workforce and population sustainability problems. They are looking at environmental remediation impacts because of their manufacturing scale over time. And especially with current events and looking at what's happening with

the oil supply, they are facing major energy dependence issues, as well.

Biotechnology offers quite a bit of solutions with that. For example, looking at health care -- and I appreciate the Commission has provided reports on this -- but the fact of the matter is that China's access to genetic data, not just in the U.S. but around the world, looking at even things like electronic health records, as was mentioned before, pattern of life behavior information, what we're seeing right now is not just about them being able to provide antibiotics because we can't make them anymore. They dominate the generic pharmaceuticals. But we are also looking at next-generation therapeutics like CAR-T cell therapies or mRNA vaccines that are all basically AI enabled.

As it stands right now, China is sponsoring more CAR-T cell clinical trials than any other country in the world. And what is happening now is that we are sponsoring some of those clinical trials, and the resulting data and the trials that we are hosting here in the U.S., coming from U.S. patients, is going back

to China. That is not genetic information. That is not some of the sensitive data that our current policies are focusing on. However, clinical trial data is probably far more valuable and far more consequential, especially when you're looking at going into an AI flywheel to iterate and generate the next version or iteration of these therapeutics.

That is really going to be impacting not only China's ability to take care of themselves, but translate that into how they deploy that and foster even more supply chain dependencies on the U.S. and abroad.

And I will also now pivot to agriculture. We are seeing that now there, too, that a combination of technologies like GPS systems, China has more GPS satellites than the U.S. That translates into more accuracy. It translates into the fact that China dominates globally the drone market in agriculture. And it is not just scanning telemetry, but it's spraying.

You combine that with China's LOGINK for tracking overseas shipping, ZPMC cranes, rail, autonomous

trucking, it is end-to-end full-stack logistics that combined with, again, an AI-enabled GMO crops, for example, seeds that are going to be genetically modified to become heat resistant, drought resistant, they are offering all that, especially in the Global South countries, where you're seeing the highest concentration of biomass and carbon. So think soy for biodiesel, corn for ethanol. They are able to provide that to particularly the BRICS alliance member countries, especially other developing countries.

We saw, for example, Angola leading OPEC a few years ago because China is offering them advanced biotech and agriculture. We are starting to see at least six other African nations following suit. Brazil, China is even offering them their own dedicated satellites to launch into orbit to monitor their forestry, their farmland, their water usage.

In essence, everything is happening so that China is able to not only solidify their own supply chains for their own imports, whether it be looking at crops, which basically is marginalizing our farming sector. I'm not really sure what the forecasts look like for

our ability for farmers to sell our soy and corn to China because they're able to diversify their own sources through South America.

It becomes even more exacerbating because of the fact that due to the oil crisis, they are going to be looking at, well, even if the oil prices go down, one thing that is lost now is the stability of the supply chain. So that means even more renewed interest in renewables. So suddenly those countries in the Global South that are potentially agriculture rich become incredibly viable for new carbon feedstocks.

And again, this all translates into acquisition of data, translating that into being able to make it operable, translating that into products and services that they can offer to other countries, and in many ways bypass us.

And on the flip side, the U.S. is an enormous agricultural powerhouse, but we don't have the ability right now to translate the surplus that we now have because China is not buying, to internalize that into our own economy and convert that into industrial chemicals, maybe not replace oil specifically but at

least make us more resilient.

But what I am trying to highlight to you all is that it's not just about access to data. It's not just about espionage. It's not just about some of the things that have been discussed over this morning. But it really is how does the entity that can access the data and operationalize it and scale it, faster than anybody else, will give them the strategic advantage. And it can be from an intelligence standpoint, sure. It could be from a military standpoint, of course. But absolutely from an economic standpoint, China stands right now to take a significant strategic advantage.

And from a policy standpoint, again, I'm going to be focusing on a biotech angle, is that, one, we are not assessing the risk when it comes to biotechnology, especially when it comes to convergence of artificial intelligence. Primary focus has been, what, the generation or engineering of next-generation bioweapons. Is that of concern? Of course it is. However, if that is the only framing of the scoping of assessing what our risks are, we are opening ourselves

up to where we are right now.

It also means that if we assess risks appropriately we should be identifying new opportunity spaces. It's not about export control or trying to get back what we lost, but it also identifies new greenfield areas that we should be investing in, whether it's looking at talent development or infrastructure development, to ensure that we maintain our first mover advantage, because we are really at risk of losing that.

So with that I really thank the Commission for the time and I welcome your questions.

[The prepared statement of Mr. You follows:]

PANEL II QUESTION AND ANSWER

COMMISSIONER SLEVIN: Thank you all. Really excellent testimonies. I'll lead off the questions of this round, and I want to pick up on the pattern of life concept that was also raised in the first panel, which many points of that I personally find compelling. But some might push back on it as just overly theoretical at this point. So I wanted to kind of pressure test it a bit, Dr. Falco, with you.

Having data is not the same as understanding it, and I think, from the Commission perspective, where we advocate for policy recommendations when we're working with Congress, and there is always a fight for attention, political and policy attention, I kind of want to hear from you a little bit more as to what's out there, what's the evidence that suggests China has the analytical capabilities to turn data into meaningful intel? So I'm wondering if you can comment on that.

DR. FALCO: Yeah, thanks for the question. I would say the first way I would answer that is we can do this. And if we can do this, I know they can do

this. Because I see it in the academic literature. I see things that were published three years ago, five years ago, describing side-channel attacks, power traces, published by top Chinese universities. Now, can I guarantee you that that has worked its way into its tech ecosystem? No. But do I know that those universities are funded by their intelligence-gathering complex? Absolutely.

So I know those capabilities exist. I know that we actively test and do these things for our systems, again, mostly to understand what the threats look like so that we can redesign for better systems. But that's kind of the best I can give you, because I don't have a smoking gun saying I know they're doing this, but if I see it in the literature and I know that we're doing it, it just follows.

COMMISSIONER SLEVIN: Thanks. Anyone else like to comment on the question?

MR. YOU: I sort of mentioned in my opening statement that we are seeing that in agriculture. So the point of the fact is that China, as I mentioned, they are the only country that is providing

agricultural drones globally, on every continent. Whether it's a DJI, AUTEL, or XAG, there really is no other competitor. So if you are a farmer with limited resources, having these types of drones that collect the telemetry, that collects the midrange infrared spectroscopy, that is able to enable precision spraying, which translates into a 30 percent drop in supply costs and a 60 percent savings in labor costs.

So it's a win-win. They are providing a service that many of our farmers are not able to pass up, because there is no alternative, and we are giving them our data. And that translates into, well, you're optimizing farming, you are potentially increasing yield, but at the same time you are now fostering incredible dependencies on that capability. And that is something, again, that goes back to the risk assessment that we are not really paying attention to. And it's not just us. This is happening especially in those agriculture-rich countries that I mentioned before.

COMMISSIONER SLEVIN: Thank you. Thank you for that. Dr. Miller, I'm glad you raised the ICTS

program at Commerce. I think that does not get as much attention as it should. The Connected Vehicles Rule, to me, and I think you would agree, is the clearest proof of concept. And relative to other technologies -- drones, spacecraft -- I am wondering how you see that process around connected vehicles as being applied to other platforms and technologies, and if anything, what needs to change, do you think, at ICTS or from Congress. You mentioned codifying ICTS as being an important step. Tell us a little bit more as to why that's important.

DR. MILLER: Thank you for the question. I think the ICTS authority, as written, does enable a broad range of actions by the Commerce Department to address these types of risks in different sectors. Thus far we've seen only a small number of sectors actually tackled by ICTS, and there has been a significant slowdown the last year or so in terms of ICTS's action in addressing different sectors.

But I think you're right to suggest that when we look across the industrial base and across consumer products, anything that has data gathering and

connectivity capabilities is within the remit of what should be at least looked at, to examine what are the risks. And it seems to me that we should be encouraging ICTS, both by codifying but also by helping identify additional sectors that should be tackled.

I'll give you one example. It is now abundantly clear that data center infrastructure is critically important for the future of technology, for the functioning of our economy. It seems to me very important to understand what are the risks of using certain types of critical Chinese equipment in our data center infrastructure. That would be a natural place for ICTS to do more work.

COMMISSIONER SLEVIN: That's great. And you mentioned Europe and Israel, as well, as taking similar steps. What is the ideal forum, do you think? Who should be at the table if we are to try to have some alignment with countries around the set of rules like ICTS?

DR. MILLER: Well, it's a hard question because every government has a different set of regulatory

authorities. Our friends in Europe, I think, have been very hesitant to call out China specifically when regulating these types of risks and prefer instead to talk vaguely about cybersecurity risks. And that has been a challenge because, of course, our rules do allow us to target countries of concern specifically.

I think we have seen some positive developments in Europe, in particular, in terms of actually taking seriously these concerns, in Norway, in Denmark, in Poland, in the U.K. just the last couple of months. We have seen new public discussions as well as new governmental action to begin to tackle these topics, but I would say a lot more work needs to be done, both within these countries and then to align policies with us and our allies.

COMMISSIONER SLEVIN: Great. Thanks very much. Commissioner Miller.

COMMISSIONER MILLER: Thank you, Commissioner Slevin. I'd like to turn to biotech. Dr. You, you had mentioned in some of your remarks the implications of pharmaceutical data, other data. I want to ask you the question in a little bit more direct way. Right

now Western pharmaceutical companies are flooding into China right now, for clinical trials, for early stage drug licensing. What are the implications here in terms of data accumulation and synthesis on the broader Chinese thrust to dominate biotechnology or biomanufacturing? Are we giving up something by going over there? What the problems? Help talk us through this issue, please. And anyone else who can weigh in on that is welcome to answer, as well.

MR. YOU: Thank you very much for the question. I think in many ways the tables have turned, that historically it used to be U.S. and other pharma hoping to get into the Chinese market to get access to the 1.4 billion potential customers. I think post-COVID the Chinese recognize that there is a significant benefit, not only for their own population but commercially. You see that in their strategic plans. In their most recent 15th Five-Year Plan they just released you see a specific prioritization of biomanufacturing in pharma, in agriculture, in renewables.

So what I think is happening is that, as I

mentioned, you are starting to see more Chinese startups coming up with new, innovative drugs, and the majority of them are being AI enabled through the data that they have.

Where the tables have turned is that other companies are now licensing those new candidate drugs to be able to bring it to the market while the Chinese companies retain domestic control. So the paradigm has flipped. And in the short term it's a great potential windfall for the companies that are able to achieve that license, but I don't think they are paying attention to what the long game is, is that, as you mentioned, that is access to more data, that then gets iterated to generate the next tranche of innovative candidate drugs or even, more importantly, especially when you think about cancer therapeutics, very specific, individualized treatments, long-term wise we may be giving away the farm and not really recognizing that.

And it kind of goes back to my original statement that we're just not doing the risk assessments appropriately. It is the same old thing. It is

looking at it from a quarterly financial report rather than looking at what the long-term implications are.

COMMISSIONER MILLER: I think you're right there. Companies are focused on short-term profits, and I think it is Congress' job to look at the long game and to look at the national security implications, so I appreciate you bringing this to our attention.

Ms. Staheli, talk to us about data poisoning attacks. How should we think about this? Obviously it is a major problem, but is this the sort of problem that should be viewed holistically? Should it be viewed in terms of trying to find a solution or trying to find a way to plug vulnerabilities, something that we should be looking at by sector, because of the importance of the sector? Is it something we should be talking to our top companies about, on a company level? Help us think through this idea of data poisoning and how to defend ourselves against it.

MS. STAHELI: Certainly. Data poisoning attacks are not just a consideration in terms of China, it is something that is broadly worried about in the community. It is not necessarily anything that is

new.

As I mentioned, most of the U.S. models, as well as China, do train their models on -- there's one very specific dataset and derivatives of that dataset that are used in the training. So that is a place where anyone can go onto the internet, post documents, make social media posts, blog posts, videos, and the crawl engine will come and ingest all of those documents.

A sophisticated adversary could, in a coordinated manner, poison those datasets in as few as 250 documents. There was some research released recently that talks about that. But so could anyone else with that intent. So there is much research that needs to be done there to figure out how do we discern a poison attack from someone spreading misinformation, or even AI-generated content could be something that creates these problems.

And in general, these kinds of attacks may not even be intentional. In some cases it might just be poor data quality. So we should be looking at more standardized ways to assess the data pipelines that these companies are using for training, looking at

what are the best practices for cleaning, labeling data, to ensure that either intentionally or unintentionally the models are being trained on the best approaches that we've seen coming out of the research.

COMMISSIONER MILLER: Thank you.

COMMISSIONER SLEVIN: All right. Thank you. Commissioner Stivers.

COMMISSIONER STIVERS: Thank you. I'd like to turn to Chinese autos. Dr. Miller, a few years ago members of Congress pushed the Biden administration to impose 100 percent tariffs on Chinese autos into the United States. Having grown up in Detroit, I know firsthand how devastating that would be to the auto industry and to our economy as a whole.

While I know this is not a hearing about trade, certainly the responses on data and trade are intertwined. And so my questions to you are twofold. First -- well, there is also new legislation which I think would strengthen some of the restrictions on components in Chinese vehicles. I wondered if you've had a chance to look at that legislation, and are

there things in that legislation that could go farther, that the Commission could push, would be my first question. My second question is, how can the U.S. response to Chinese state-subsidized vehicles be effective if there is no running-faster component, which we didn't talk so much about in this hearing, but we're not going to be able to compete with these vehicles, in Europe or throughout the world, or even Canada for that matter, unless we can provide a better alternative.

DR. MILLER: Well, I completely agree that you need to provide a better and price competitive alternative, and that has to, I think, increasingly rely on autonomy and the types of capabilities that sensor-powered cars enable. So any regulatory steps that are taken need to make sure it doesn't slow down that rate of progress.

But I think we do, nevertheless, need to not only be concerned about not slowing down progress and also take seriously the risks that I outlined, and, of course, listening to industry. At times there is only a focus on driving down costs, which is certainly

important and not a focus on addressing our security concerns.

I would say when it comes to trade dynamics, I think it is critical to note that tariffs don't address these risks. Tariffs apply at the car level, not at the level of the sensors and the communications devices within cars. So we need to be very precise and specific about what are the components that are most of concern. And I think the Department of Commerce was right to target connectivity components and software as the highest level of concern.

I also mentioned in my testimony battery management systems. The software that goes around batteries is something that also should be specifically targeted, especially if and when U.S. automakers consider closer collaboration with Chinese battery makers, as has been discussed recently in the media.

So I do think expanding the scope of components that we focus on is the right direction of travel, but we need to be targeted at the restriction level and not count on tariffs or broad-based bans on Chinese

cars, because it is easily conceivable that American or European and Japanese cars could also have problematic components inside of them.

COMMISSIONER STIVERS: Okay. Anything on the running faster part of it?

DR. MILLER: I would just say that, to reemphasize the central importance of enabling our firms to gather and utilize this data. We must not slow that down in any capacity.

COMMISSIONER STIVERS: Thank you. We spent a lot of time on the last panel talking about industrial espionage and IP theft and how to respond to it. But it seems like the larger problem, from what I'm hearing, is the legal acquisition of this low-level data, broader low-level data. My question, for anyone who wants to respond, but Mr. Falco in particular, to what extent have U.S. companies, through these data broker sales, joint ventures, crowd servicing agreements, app distribution, functioned as unwitting or knowingly complicit with Chinese state or so-called Chinese private data collection?

Dr. Falco, you said we should double down on

components restrictions, but do we also need better disclosure requirements? I think a lot of these U.S. companies would respond if they had to disclose that they are entering into this agreement with a Chinese state-owned or so-called private company. Any thoughts on that?

DR. FALCO: I think American companies probably are very happy to be ignorant about what's happening when it comes to letting their data leak or go somewhere, that might be into Chinese hands. Working with industry for my entire career, in and out of academia, I like running fast with scissors, like to your other question. And industry does too. What they don't want to start seeing is people telling you who you're allowed to run fast with scissors around.

And I think the challenge that we're going to have here is to figure out how to not disable the innovation ecosystem and the commercial ecosystem that we rely on and the, frankly, meritocracy that our companies are based on, while still giving the right restrictions to protect our national security.

One thing I would offer is I spent a lot of time

in Europe with different intelligence communities and different academics. And what has been really stark recently is their lack of interest in using American software. So for example, the government of Denmark -- I know this is not China, but the government of Denmark now is using open LibraOffice or something like that, because they don't want to use Microsoft because they're pissed at us.

And this is not a requirement. This is not a law that is in place. This is a pushback of sovereignty. And I don't know how we can properly mechanize that same sentiment, but maybe that's the approach, which is less of a required law saying you can't do blah-blah-blah and instead moving towards, let's lead by example and have certain companies who are part of a coalition of the willing demonstrate how they should approach this thing. So I think that's what's happening in Europe.

COMMISSIONER STIVERS: Thank you. Mr. You.

MR. YOU: If I may, I just want to kind of expand on that. I kind of touched on it in my opening statement. But you really need to pay attention to

what China is doing in international standard-making efforts, they have historically been called fast followers, but especially in light of their, as I said, data aggregation and the ability to operationalize it, I think they are evolving to become fast adopters. And what I mean by that is that they are developing the standards in places like the World Radiocommunication Conference, the International Telecommunications Union, International Civil Aviation Organization. But basically they are laying the groundwork for what the future looks like. And if they are able to define the standards and they adopt it, then everybody else is going to have to play by those rules, as well, too.

And one of the things that you should be paying attention to is something that they have already determined is a priority, is the low-altitude economy. This is everything below 400 feet, and that is not covered by the FAA. So think of drone-delivered Uber Eats or Grubhub, or something along those lines. It's building out that infrastructure and technology to support that, and especially the guidelines and the

regulations to support that. Because if you get that, that's basically the whole ball game for the future of next-generation commerce.

So you think about that, if they are able to influence that then think of automated delivery of special diets, or your prescription medicine. This transcends privacy, but it's also looking at the next level e-commerce, built on this new technology that has even more data access that we are not paying attention to right now.

Because admittedly we do need to look at what's happening now and how we're being hurt, but if we're not paying attention to strategically what their intentions are -- because as I said, they have drivers for why they need it to happen, but it also then potentially translates into other vulnerabilities that we are not assessing at this point, and we absolutely need to.

COMMISSIONER STIVERS: Great. Thank you. Sorry I went over.

COMMISSIONER SLEVIN: Thank you, Commissioner. Chairman Schriver.

CHAIR SCHRIVER: Thank you, Mr. Chairman, and thank you to our witnesses. I really appreciate your statements and the statements so far.

Most of our hearings it doesn't take too long until we get into deeper discussions about alliances, partnerships, cooperation, and there hasn't been as much in this hearing, although, Dr. Falco, you mentioned the NATO piece, given your focus on defense systems, and Dr. Miller, you talked about differing standards when it comes to importing connected vehicles and the like.

But I wanted to give you each an opportunity to talk about that, the importance of alliance cooperation to address the areas in which you each have interests. And this notion of developing patterns of life, aggregation of data, is this something that we can be resilient on our own if we restrict and control and are resilient on American data? Is there an American gap, even if they are getting lots of data from elsewhere? But really the general topic of alliance and partner cooperation.

DR. FALCO: Thanks for the question. I want to

double down on the notion of science diplomacy, and the reason why is because right now, especially in the current geopolitical posturing of the U.S. juxtaposed with the rest of the world, we don't have a lot of common ground with some of our historic allies, for better or worse. We have our own interests, and we have to pursue our interests. But one thing that has historically helped was to be able to find the off-nominal diplomacy conversations through science, which we have done a little bit of pulling back from.

And the reason why I am mentioning this is because, as described earlier in the testimony, we see scientific installations and research stations being used for dual-use purposes, in every manner. And our collaborators, our allies who we have historically done these missions with, these scientific research missions, have been very supportive of us doing things dual use in those places that we've been installing things with them.

But when we aren't investing in that infrastructure anymore, and where there are new areas to explore and discover, and we're not there, they're

going to do it with someone else.

Take, for example, in Antarctica. That is all dual-use infrastructure, right. We think it's all science. It's not. We all know that there are a lot of things going on down there. And this is something where historically the National Science Foundation has pushed towards science installations, but we don't care as much right now about those installations, from a science standpoint. But that means that we're losing visibility from an intelligence gathering and from a military standpoint, and especially posturing with our allies that we are showing we care about these areas. If we don't care, they are going to go somewhere else.

So I think that's an angle that we really need to figure out how to double down on.

DR. MILLER: I certainly agree with the importance of the question. I would say there are two different dynamics that I would focus on. The first is the ability to aggregate data in third countries is both something we don't want to China to have and that we want to have ourselves. So it matters a great

deal, I think, whose cars are driving around Europe streets. It matters commercially because if our companies are getting access to that data they can build better autonomous driving systems, whereas if Chinese are gathering that data they have an advantage in terms of quantity of data. But, of course, it also has intelligence implications, as well.

The second implication that I think is just as important is the economic dynamics. If our companies are only selling critical components to the domestic market, that is a relatively small share of global GDP. And if China wins the rest of the world market, for sensors, for communications equipment, but also for certain types of software, they have the scale to become more efficient over time.

And that's why I think it is critical to align U.S., European, Japanese and other country standards so that we have the bigger market along with our allies and can out-compete the Chinese in industries where scale does matter.

MR. YOU: And I want to provide a slightly different answer, in that if anything, it should be an

indication of where we should be doubling down, as was mentioned, investment in research and development. So it's the ability to run faster and not just play defense all the time. And that's important because, one, working with international partners to help them understand a lot of the vulnerabilities that I highlight, because we're not the only ones suffering from it. In many ways, our partners are probably getting hit worse in data exfiltration.

But then the existential threat, though, too, is that if China is able to, because they have operationalized the data and been able to scale it, and then that means that some of those places like the universities, whether it's in Cambridge, Boston, Massachusetts, the West Coast in Silicon Valley, you know, Austin, Texas, or I should mention, because of agriculture, a lot of our agriculture-heavy states that have land grant universities, what happens if it is suddenly because we didn't invest in that then they no longer are the centers of gravity for research. It turns out that there is a shift to Beijing, to Suzhou, Shanghai, Shenzhen for academic excellence, not only

for the U.S. but for other international countries. And those become the centers and we lose that. That's something I don't think we're going to be able to recover from.

MS. STAHELI: One area that is overlooked in the data realm is data to be used in the context of testing artificial intelligence capabilities. We hear from defense contractors, startup companies. Sometimes it's hard to get government mission data for the capabilities that they are building. But that data is also essential for making sure that the capabilities that they are creating for the government are robust, are reliable, are representative of the missions that they are servicing.

So having better channels for that data sharing to happen, whether it's to build or to evaluate capabilities, would benefit the entire community.

COMMISSIONER SLEVIN: All right. Commissioner Price.

COMMISSIONER PRICE: Thank you all very much. This is an excellent panel, and I appreciate all of your efforts.

So I spend a lot of time thinking about how we are going to implement some of the policy suggestions that you all make, that we make to Congress. And what it keeps coming back to is do Americans really want whatever change it is that we're looking for on any given day or any specific hearing that we have.

So I want to ask a hypothetical. In each of your areas that you were asked to address today, if you were talking to your neighbor, not someone who studies China or studies these issues or tech issues on a day-to-day basis, but why should they care? Why should it matter to them what kind of sensors they have on their car? They just know that it makes it easier to park. Why should they care about what information they're gathering through AI and what they're searching for and that kind of thing, and the same in the other areas, as well.

So you're having this short conversation with your neighbor. Give your top lines of how you're going to explain to them why they should care, and therefore, why policymakers need to take action.

MR. YOU: So again, coming from a biotech

perspective, because we do not pay attention to the value of our personal data and many times we don't have control of who gets access to it, or more importantly, who determines how valuable that is, the tagline I use is that we're going to wake up one day and realize, well, holy crap, we've just become health care crack addicts and China has become our pusher.

What happens if become completely dependent upon a foreign supply chain for our ability to maintain our fitness, our health? But then more importantly, that means that we've lost market share, we've lost job opportunities, and especially for the students, for example, that are studying biology in college right now, by the time they graduate what prospects are we offering them if we are not understanding the value of the data, making the appropriate protections but also, more personally, the investments to ensure that the U.S. stays the innovation lead globally in this space.

MS. STAHELI: Certainly from a privacy and reliability perspective many of the commercial AI tools are being used in every aspect of American life now, and people are revealing the private, innermost

thoughts to these technologies. And certainly most Americans wouldn't want their most private thoughts exposed to their employers, to their insurance companies, to other countries. So that is one of the effects that is important to manage that risk and make sure that individual privacy continues to be protected.

DR. MILLER: I would point my hypothetical neighbor towards a research report that was done by a group of Norwegian cybersecurity experts about two years ago. They bought a car in Norway, a Chinese-made car. They did a teardown of every sensor and tried to ascertain where the data from that sensor went. They found that the microphone inside of the car stored data, transmitted it to a server in China, and there was no visibility as to what was done with that data after the fact. I don't think I'd have a hard time convincing my neighbor that they probably wanted some understanding of where the microphone in their car was transmitting to.

DR. FALCO: From an aerospace and defense side of things, the U.S. is the protector of democracy for the

world, and I think that it's very hard for any neighbor I have, being foreign or American, to agree that we can't have any compromise of our defense capabilities going over to China.

On the other side, from an aerospace standpoint, drones have already been filtered and people are very accustomed to seeing these around, and most of my neighbors want to shoot them out of the sky with their gun.

So, you know, this is also not harder to tell them, you know, you might not want all of this information going over to China that they're collecting on you. And even though the data is not about them specifically, it's about this pattern of life and how things are used, it still creeps them out. So my neighbors are probably an easy sell.

COMMISSIONER PRICE: Thank you.

COMMISSIONER SLEVIN: Great comments. Commissioner Kuiken.

VICE CHAIR KUIKEN: Thank you very much, Commissioner Slevin. To Mr. You, it's always good to see an original, card-carrying member of the biotech

mafia in front of the Commission, so thank you for being here. You talked about adoption -- on the first panel we talked about convergence and adoption. And as we think about biotech data, or DNA data essentially, becoming more and more accessible and stored on the cloud, how should we think about the issue of convergence in AI in the biotech space? Because Commissioner Schriver and I have been going around talking about last year's recommendation. This is an area where I think we're almost at the point where we're going to see this incredible flywheel start in the biotech space, not just in pharmaceuticals. I mean, everyone wants to talk about the cancer drugs or the things that's going to make all of us live longer.

The thing that actually gets me going is biomaterials, bioindustrials, bioagricultural. How do we unlock biology as a general purpose technology? And I feel like as the Chinese continue to do this investment in data and in biotech, we are about to see an incredible acceleration. And we're the country, in the democratic world, to unlock chemistry and physics

as a general purpose technology. Biotech is not unlocked yet, but this convergence, this accumulation of data, seems to put us on that pathway. What do you think?

MR. YOU: All too true, and I think that it's sort of a recurring theme that we are one of the few developed countries that do not have a biotech strategy. And I think that just blows me away.

So to your point, we covered down on health so much, but when you think about agriculture in particular, it is now no longer just farm to fork. It's farm to fiber, farm to fuel, especially on that aspect, too. It's becoming strategic in its nature.

And absolutely, the convergence of AI and pattern of life behavior for plants, for example, or water usage, the entity that is able to optimize all that and translate that into efficient crop yields, right, then you are going to get renewables. You are going to get manufacturing materials.

And as I said before, I can't forecast the future, but in light of what's happening right now with global oil supply chain, for biofuels, for

example, it really wasn't viable unless oil was, what, $120 per barrel. We are kind of there. But even if we go back down, I think the one thing that changes is stability. I think that's in question now. So if that being the case then suddenly renewables, to your point, that's biotech based, is really going to become with renewed interest internationally, globally, and especially for China, that is so much so and energy dependent.

So absolutely, yes, I wholeheartedly agree that you're going to see major convergence and a lot happening in biotech.

VICE CHAIR KUIKEN: I was hoping you were going to tell me no.

A couple of you touched on this issue of exquisite versus good enough, and think, Dr. Staheli, you touched on this especially. The thing that I think we're starting to see is one of the reasons the Chinese are being successful in the artificial intelligence space is they have basically adopted the good-enough strategy.

So as I think back over the Iraq and Afghanistan

war and I think about the various Secretaries of Defense and knowns, unknowns, and all the iterations there, and also the pursuit of the exquisite instead of the good enough, and the good enough is often what allows you to accelerate adoption. think that's what you're telling us.

Is there anything that we should think about in terms of policy recommendations that advance sort of a good-enough approach? It's okay to continue to pursue sort of the frontier lab, exquisite approach, but is there a way we should think about the good enough as we think about deploying AI across the U.S. government, at the state government level, at the local government level?

MS. STAHELI: Yeah. So certainly when you're considering national level strategy you should think of it as two separate but related pieces. On the national security side you want to worry about exquisite, best of breed, frontier models, because you want to be thinking about technological surprise and how to avoid that, also preserve that advantage for the United States.

But on the economic side, cost is one of the driving factors of adoption. Innovation theory tells us that as innovations mature the more than you can make your innovation available at a lower price point, the more your innovation is going to be adopted.

From a perspective of China, certainly we should be looking at the countries that they are engaging with as far as what their abilities are to be able to adopt technology. Certainly in Africa, where low connectivity or mobile-first innovation ecosystems are going to be a predominant part of the economy, smaller models, lightweight models, models that can run on your phone, models that can run on smaller infrastructure or data centers are going to be more prevalent there, just because that's one of the limiting factors.

And the more that we think about innovation in the government, we have to make sure that we are thinking about making a good match between the use case and what the technology need is, where we're making choices about what technology we adopt.

One of the gaps that we have right now is the

ability to truly measure and characterize models for their abilities in different domains. So benchmarking is one way that is done, but it's very broad, general testing. We don't have really yet a testing regime that helps us to identify for my specific application what are the metrics that I need to be hitting. We don't really have standard ways of testing or standard places that we can go to, to test these models.

And we know that there is lots of research happening in many different places, and that may be another opportunity for the collaboration that was talked about earlier, as well. How do we get the expertise together to work on that problem.

VICE CHAIR KUIKEN: Thank you.

COMMISSIONER SLEVIN: Commissioner Hodges.

COMMISSIONER HODGES: Thank you. It seems clear, based off of the testimony today, that China's data acquisition strategy is not primarily aimed at penetrating U.S. systems. It's a big problem but not one we're really focusing on today. But instead it's a structural play at data dominance, across modeling, operability, application, and that's global.

I'm curious, as some of you were speaking we were referencing sort of third-party countries, the idea of nation sovereignty came up, and I'm curious if you've got any specific examples, based off of your discussions, where countries are starting to really prioritize the understanding and need for data sovereignty when it comes to AI or working on these different levels of components. Mr. Falco?

DR. FALCO: Thanks for the question. Sovereignty is a big deal right now across Europe. As I mentioned earlier, we are seeing this especially in the cloud services environment and in the data center infrastructure space. This is something where we are actively hearing about -- and I work a lot with Nordic countries specifically, so Sweden, Norway, Iceland, Denmark, there is a major push to propel its very small innovation ecosystem -- it's small just because of numbers, right. They are smaller countries. But they're pushing their innovation ecosystem towards designing and building companies that are specifically trying to replicate what we're doing, on our frontier models, on our data center infrastructure, on our

energy system plays, from a novel technology standpoint, because they just feel icky about working with the U.S., in some ways, right now, for better or worse.

And this is something where we're seeing a direct investment in their innovation ecosystem for sovereignty. I think that's something that we don't necessarily have the mechanism to achieve necessarily in the U.S., and I don't think we want to replicate that. But it is happening very clearly in Europe, especially now we see Europe's defense strategy, where they are doubling down on looking at Germany as a big protector of Europe. France and Italy are also part of that ecosystem, but they want German products. They want Dutch products.

I was at The Hague last week talking about novel UAVs for chemical weapon nonproliferation, and there was a whole bunch of products out there that they were talking about, and they had to be purchased from somewhere in Europe. And there were a whole bunch of capabilities that were Chinese and American, but those weren't on the top of the list. There was some

prioritization mechanism there that said Europe first.

So for better or worse, that's kind of where we're at right now with some of those allies.

COMMISSIONER HODGES: Okay. Thank you for that. And Mr. You, going back to you on the idea of bio, I'm curious. Related to this question, there have been some interesting countries that have been coming to Congress recently to talk about engagement on bio opportunities. I'm curious of your perspective on this. Is there an opportunity for the U.S. to really lean into this and start working on the bio front when it comes to emerging technology?

MR. YOU: Absolutely there is, and I think my fellow witness here mentioned it before, that we have a history of being innovators and leaders in the research and development space, and we should lean into that. And other aspects of it, too, is that -- and this goes to sort of like the safeguarding science perspective -- as the U.S. we do want to highlight individual rights, individual privacy. And there is a reason why the U.S. has been leaders, because we do also believe in collaboration and openness and equity.

That is why science has been able to accelerate as much and innovate so powerfully here in the U.S.

We sort of lost sight of that, I think, a little bit, but that's something that we should be leaning on because that, historically, has been how we were able to have terrific scientific diplomacy, collaborations, partnerships.

And sort of on the flip side, too, is basically if we understand, again, the value of our data, the sensitivity, then it's basically, do your due diligence. Know who you're doing business with. Read the fine print. Understand what the risks are. And combining those two, I think, we can still be very effective in partnerships internationally.

COMMISSIONER HODGES: Thank you.

COMMISSIONER SLEVIN: Anyone with follow-on questions? We have a little time. Go ahead.

VICE CHAIR KUIKEN: Thank you, Commissioner Slevin. I was listening to you, Dr. Miller and -- is it Mr. Falco or Dr. Falco?

DR. FALCO: Doctor.

VICE CHAIR KUIKEN: Doctor. Sorry. Commissioner

Schriver said no more first names. So as I was listening to Chris talk about software and teardowns, I love good teardown of a car or a chip, I was thinking about tire pressure monitoring systems in cars, because those have been around for a long time, and all of the things you said sound really scary, but these TPMS systems have been around for a long time, and there are sensors all around every city that pick these up, and you can basically geolocate anything.

I had a friend recently tell me he went to visit one of the intelligence agencies, and he didn't bring his phone. And I said, "Did you drive your car?" And he looked at me and said, "Well, of course I did." And I was like, "Okay. Then somebody can track down where you are." So it was one of these things that sort of amused me.

It also got me thinking, Chris, or Dr. Miller, and Dr. Falco, on your comments, where we have this download now, decrypt later sort of philosophy going on. I guess I would be interested in your view on that whole space and how we should think about that in the context of data, whether it's car data or biotech

data, like Mr. You talked about.

And then the second thing that I had at this moment, as I was reacting in my head to you guys, why not just give up? Why does this even matter? Commissioner Price talked about her neighbor. I have this moment all the time where it's like, I mean, Google already has all of my data. Amazon has all of my data. I don't have a Facebook account but I'm sure they've hoovered up something somewhere.

So why not just give up? Does this matter? Boil it down for me in sort of a very crisp and clean way. And, Mr. You, if you have something on the biotech comment, go ahead. So that's my question. Why not give up, download now, decrypt later. You can talk about tire pressure monitoring systems too, if you'd like.

DR. MILLER: Thank you for the question. I think it is an important one. You're right to say that there are lots of different devices that have our location, that listen to what we're saying in certain ways.

I think the keys to me are twofold. First, do we

understand what standards are in place? Google has all of my data, but I've learned over the last 20 years that I have some ability to trust what they do with my data. They don't leak it very often. They have a track record of pretty good cybersecurity. Not perfect. But I think roughly what they are going to do with my data, in a way that I don't understand many other devices that I have. So that, to me, is a key question.

And I think we should assume a different level of vulnerability for a device or a software system built in the United States versus in an allied country, versus in China. And I know the Commission has done work on the legal requirements that Chinese firms have to hand over data. Even if the firm itself doesn't want to, the party can demand it.

So I would differentiate between levels of risk for different types of data that's being gathered, based on who is actually gathering the data.

The second thing I would say is that there are different volumes of data, gathered by different types of systems. It's true that tire pressure monitors

can, in many cases, identify where you are. But I guess I would posit to you that my GPS location is a lot less valuable than my GPS location plus a microphone plus a camera inside the car plus 10 cameras outside the car, et cetera, that are fusing that data together and providing a much richer picture of what I'm doing, where I'm driving, and everyone else who is driving around me, everyone else who is walking the streets around me, coupled with facial recognition in terms of what the cameras are seeing on the sidewalks around me.

So I think we should impose higher standards for devices that are gathering more types and broader categories of data than, for example, just a single tire pressure monitor system. So that would be the rubric, (a) do we understand who is setting the requirements around the data? Is it a U.S. company? Is it a foreign company? And then (b), what are the quantities and types of data that are actually being gathered. And that would be the rubric I would use to determine what's my willingness to pay to substitute in U.S. components or design out Chinese software in

any given type of system.

DR. FALCO: I really like that recommendation about one type of data, not so interesting. Multiple types of data, maybe you have to worry about that a little bit more. But to the why do we care, I have a long thought that privacy is dead, and I still believe that, even though I've been working on trying to make it not the case for a while.

But you need to care because of the ability to anticipate with this data. We don't want everyone to know what we're going to do next. Mindreading is not an actual thing right now, but it will be an actual thing if you have enough data to be able to anticipate movements and be able to cross-correlate across all these things.

So our privacy, on an individual level, might be gone, but right now we still have the ability to protect anticipation and operational surprise. And I think that's starting to go away if we allow too much data collection.

VICE CHAIR KUIKEN: I just want to respond. You have just given us the title for this chapter,

"Privacy is Dead." So thank you very much for that.

The one thing I would say, though, is that the amount of data that's available, that I can just buy -- Dr. Miller, you pushed back on me a little bit on the tire pressure monitoring system. I mean, agree with you. At the same time I can go acquire all these things. I mean, Salt Typhoon and Volt Typhoon are operational preparation of the environment, and that is data collection, and that gets to your microphone issue and all those things.

So anyway, thank you for the title to the chapter, and Mr. You.

MR. YOU: So just a couple of things. First off, at the end of the day we still have our data. It's our data. So it's what are the investments we're making to capitalize and operationalize the data for ourselves, to be able to continue to be the first mover advantage leaders in innovation. So there is that.

The second part kind of goes back to Commissioner Price's question, why should we care, how should we articulate this. On the bio threat angle, I have had

a lot of debates, because especially when I get rubbed the wrong way when they say, "Well, when it comes to bio threats you have to factor in global catastrophic risk." And I'm like, are we talking about 100 million plus fatalities? And I'm like, come on now. Is that important? Sure.

But in my mind I want to commend the Commission for tackling this. This is absolutely a challenging issue. If we don't address this now then my nightmare scenario is that what happens if we suddenly find out that because of the access to the data we find that an authoritarian regime has control or influence in all aspects of our ability to live? You know, the ability to maintain our health, control of our food supply, looking at the future of renewables, all because we failed to recognize where our data is going, how it's going to be utilized.

And I agree. I don't think privacy, as we knew it, exists, but data privacy might just be a simple question of who gets to see my data? At least we should be able to determine that.

Second question is about data sovereignty meaning

more about who determines what my data means and ascribes the value to it, because I don't have any control over that.

And then, finally, data security is basically going to be who gets to access the data and what are they going to do with that?

I think those are going to be three critical questions that we should be able to answer as we move forward, because AI is not going to stop.

So my colleagues are right. I don't think privacy exists anymore, at least in the framework that we used to recognize it, but there some of these other fundamental questions that we should be tackling, because the nightmare scenario is not acceptable, as an individual and especially as a democracy.

VICE CHAIR KUIKEN: Thank you, Mr. You. Thank you for the questions. Great hearing, guys.

COMMISSIONER SLEVIN: I'll exercise privilege on a comment, and then I will go to Commissioner Hodges. But just on this question of why should we care, maybe it's being in the presence of Dr. Miller who wrote the book on chips, and colleagues like Mike Kuiken, who

worked so much on the legislation.

But there is a small community of national security professionals, maybe a small percentage of readers of *The Wall Street Journal*, who kind of understood the dependency we had on Taiwan and elsewhere for semiconductors. I think, to me, what made it applicable to your neighbor was when, in 2020, auto companies were furloughing workers, and it became more visceral. I don't know what the right analog to that, to the discussion we're having, but being with Dr. Miller and appreciating his book I wanted to make that comment. Commissioner Hodges.

COMMISSIONER HODGES: Thank you. I'll keep it short. Dr. Falco, your exchange with Commissioner Kuiken on privacy led me to want to ask this question. You said mindreading is not possible yet and all that, and I completely agree. From your perspective, though, is there a real threat -- and I would open this up to the rest of the panel, as well -- is there a real threat related to sort of data's implications on potential nefarious actors' abilities to have some sort of cognitive engagement of cognitive

manipulation?

DR. FALCO: That's a great question. If they are able to anticipate our future actions as a result of the dragnet of information that's being collected, from a tactical standpoint, let's say we're talking about drones or building a space vehicle that may engage on orbit in dogfighting ways, I believe that there probably are ways that they can incept scenarios in public dialogue that would make us go different directions with our technology development.

And I think that is actually a real threat. They are going to be using the media in order to facilitate this. We already see this. I do work with NATO, and when we come up with a new idea, it's published in the news, and then two weeks later we hear something out from the *South China Morning Post* of how China has combatted that already and this is the new direction they're going in.

So that cat-and-mouse game already exists from the mind games standpoint. The question is where do we get dragged down with them?

COMMISSIONER HODGES: Thanks.

DR. MILLER: Could I just note, on that front, it seems to me we've got, in the social media sphere, plenty of evidence of companies already being able to predict what people would like to click on. This was the key driver behind Congress' completely justified concern about TikTok, and the ability of ByteDance to understand what video one wants to see next is an example, in a narrow space, but an example of this capability already being widely demonstrated.

COMMISSIONER HODGES: I appreciate that.

CLOSING REMARKS

COMMISSIONER SLEVIN: I think that concludes our hearing. Really excellent discussion. I want to thank our witnesses for their testimony.

As a reminder, all of the written testimonies and a transcript of this hearing will be posted on our website, uscc.gov.

With that we are adjourned.

[Whereupon, the above entitled matter went off the record at 12:30 p.m.]