IP AND STRATEGIC COMPETITION WITH CHINA: PART III—IP THEFT, CYBERSECURITY, AND AI

HEARING

BEFORE THE

SUBCOMMITTEE ON COURTS, INTELLECTUAL PROPERTY, AND THE INTERNET

OF THE

COMMITTEE ON THE JUDICIARY

U.S. HOUSE OF REPRESENTATIVES

ONE HUNDRED EIGHTEENTH CONGRESS

FIRST SESSION

THURSDAY, OCTOBER 19, 2023

Serial No. 118–49

Printed for the use of the Committee on the Judiciary

Available via: *http://judiciary.house.gov*

U.S. GOVERNMENT PUBLISHING OFFICE
53–827 WASHINGTON : 2023

COMMITTEE ON THE JUDICIARY

JIM JORDAN, Ohio, *Chair*

DARRELL ISSA, California
KEN BUCK, Colorado
MATT GAETZ, Florida
MIKE JOHNSON, Louisiana
ANDY BIGGS, Arizona
TOM McCLINTOCK, California
TOM TIFFANY, Wisconsin
THOMAS MASSIE, Kentucky
CHIP ROY, Texas
DAN BISHOP, North Carolina
VICTORIA SPARTZ, Indiana
SCOTT FITZGERALD, Wisconsin
CLIFF BENTZ, Oregon
BEN CLINE, Virginia
LANCE GOODEN, Texas
JEFF VAN DREW, New Jersey
TROY NEHLS, Texas
BARRY MOORE, Alabama
KEVIN KILEY, California
HARRIET HAGEMAN, Wyoming
NATHANIEL MORAN, Texas
LAUREL LEE, Florida
WESLEY HUNT, Texas
RUSSELL FRY, South Carolina

JERROLD NADLER, New York, *Ranking Member*
ZOE LOFGREN, California
SHEILA JACKSON LEE, Texas
STEVE COHEN, Tennessee
HENRY C. "HANK" JOHNSON, JR., Georgia
ADAM SCHIFF, California
ERIC SWALWELL, California
TED LIEU, California
PRAMILA JAYAPAL, Washington
J. LUIS CORREA, California
MARY GAY SCANLON, Pennsylvania
JOE NEGUSE, Colorado
LUCY McBATH, Georgia
MADELEINE DEAN, Pennsylvania
VERONICA ESCOBAR, Texas
DEBORAH ROSS, North Carolina
CORI BUSH, Missouri
GLENN IVEY, Maryland
BECCA BALINT, Vermont

SUBCOMMITTEE ON COURTS, INTELLECTUAL PROPERTY, AND THE INTERNET

DARRELL ISSA, California, *Chair*

THOMAS MASSIE, Kentucky
SCOTT FITZGERALD, Wisconsin
CLIFF BENTZ, Oregon
BEN CLINE, Virginia
LANCE GOODEN, Texas
KEVIN KILEY, California
NATHANIEL MORAN, Texas
LAUREL LEE, Florida
RUSSELL FRY, South Carolina

HENRY C. "HANK" JOHNSON, JR., Georgia, *Ranking Member*
TED LIEU, California
JOE NEGUSE, Colorado
DEBORAH ROSS, North Carolina
ADAM SCHIFF, California
ZOE LOFGREN, California
MADELEINE DEAN, Pennsylvania
GLENN IVEY, Maryland

CHRISTOPHER HIXON, *Majority Staff Director*
AMY RUTKIN, *Minority Staff Director & Chief of Staff*

CONTENTS

THURSDAY, OCTOBER 19, 2023

Page

OPENING STATEMENTS

WITNESSES

LETTERS, STATEMENTS, ETC. SUBMITTED FOR THE HEARING

QUESTIONS AND RESPONSES FOR THE RECORD

IP AND STRATEGIC COMPETITION WITH CHINA: PART III—IP THEFT, CYBERSECURITY, AND AI

Thursday, October 19, 2023

HOUSE OF REPRESENTATIVES

SUBCOMMITTEE ON COURTS, INTELLECTUAL PROPERTY, AND THE INTERNET

COMMITTEE ON THE JUDICIARY

Washington, DC

The Subcommittee met, pursuant to notice, at 10 a.m., in Room 2141, Rayburn House Office Building, the Hon. Darrell Issa [Chair of the Subcommittee] presiding.

Present: Representatives Issa, Cline, Gooden, Kiley, Lee, Johnson, Lieu, Ross, Dean, and Ivey.

Also present: Representative Nadler.

Mr. ISSA. The Subcommittee will come to order.

Without objection, the Chair is authorized to declare a recess at any time.

We want to welcome everyone here to the hearing on China: IP Theft, Cybersecurity, and AI. Please have a seat.

I will now recognize myself for a short opening statement.

First, for everyone in attendance, especially our witnesses, I want to thank you for your indulgence as we have had a series of missteps and delays in what I believe is one of the most important hearings that this Subcommittee will have this year.

Our panel of experts understand all too well the critical threat faced by the communist Chinese Government. I always say the "Communist Chinese Government," so as to differentiate it from the government in Taiwan, which, at one time, was known for disregarding patents, trademarks, and the like but has done an about-face over the last several decades, and now is very much part of a community that is responsible in its actions toward intellectual property.

With the advent and growth of artificial and regenerative artificial intelligence, one of the key activities that we see the Chinese Government doing is, in fact, predictive use of AI to both steal real intellectual property and also to box off and, in fact, deny real inventors their intellectual property.

The cyber warfare conducted by the Chinese Government is not new. In fact, the Chinese military itself has divisions that exist both to steal military secrets and commercial activities.

In the coming years, AI will pose a transformative relationship to all industries, but it also will particularly affect cybersecurity. A supercomputer that can break any code, a supercomputer that can anticipate changes and the like, can, in fact, completely neuter existing cybersecurity systems. As a result, AI will be fighting against AI in cybersecurity.

We will hear shortly if China wins the cyber-AI arms race. Their ability to steal technology and harm, not just our country but the free world, will, in fact, be permanent.

To be sure, American AI development must be done carefully, ethically, and with respect for the values that make us different than the Chinese adversaries.

Today's hearing should make clear to everyone how important the 21st century arms race is, not only to Republicans and Democrats, but to all Americans, and particularly to those who want to be the inventors and the innovators of the future.

I hope all my colleagues on both sides of the aisle will join with me in seeing the importance of urging the administration—my opening statement says, to shift their priorities, and I will modify that by saying, to enhance and expand their priorities, to meet the challenge.

All of us must come together as AI users, creators, technology companies, and, yes, the government, to meet this challenge. No less than the American way and the free world advancements we've had since World War II are at stake.

I want to thank all our witnesses for being here today.

With that, I recognize the Ranking Member, Mr. Johnson, for his opening statement.

Mr. JOHNSON of Georgia. Thank you, Mr. Chair, for holding this important hearing. Thank you to our bipartisan slate of witnesses for being willing to share your perspectives with the Committee today, and thank you for your forbearance in our having to postpone this hearing in the past.

Americans cannot pick up a newspaper without a near daily reminder that artificial intelligence, or AI, is transforming the world as we know it. With a few keystrokes, a layperson can generate an image indistinguishable from a photograph and can make a business plan based on AI-driven, supply chain predictive analysis, or write code for a new application.

Langston Hughes may have died over 50 years ago, but sitting here today, I can ask ChatGPT to write an original poem in his style.

AI innovations have sparked necessary debate about intellectual property protections for both the owners of the massive quantities of data used to train AI models and the authors of final products of AI-assisted works. The disruptions to society don't end there. Looming behind labor disputes lie questions about the future of work when AI is used by the powers that be to replace writers, technicians, and auto workers.

I'm committed to working with my colleagues across the aisle to protect creators, inventors, and intellectual property rights overall, while encouraging innovation and invention. We are here today to talk about just one of the many ripple effects of AI innovation: How AI is being used and can be used in the future to augment China's strategy toward the United States.

As a global leader in AI innovation, the People's Republic of China, or PRC, is in a unique place to deploy AI before many other Nations. If the PRC chooses to use AI to increase its authoritarian hold over its own people, to advance its cyber espionage strategy, or to interfere in its neighbor's elections, such actions will undermine competition and innovation, not just in China, but around the world.

Since the PRC entered the World Trade Organization 20 years ago, it has endeavored to gain American data, intellectual property, and our Nation's secrets. Cyber intrusions from the Chinese Government or affiliated groups have successfully infiltrated the United States Department of Justice, our military bases, and businesses across the country.

The adoption of AI only increases China's ability to continue these tactics. So far, China has tested swarms of AI-powered drones, used AI-generated propaganda to target U.S. politics, and stolen AI technology from U.S. companies.

Experts disagree as to how far China has advanced in AI development. Indeed, many argue that AI innovations are happening so quickly that it is difficult to know what the technology can and cannot do at any given time. There is a consensus that the United States, with its broad array of businesses, strong intellectual property protections, and widespread investment in scientific research, is ahead of most other Nations.

Many Americans believe that it is incumbent on the United States to lead. I am one of them. Leading in development alone is not sufficient.

The European Union this summer took steps to regulate artificial intelligence by passing draft legislation that the EU is calling, quote, "the world's first comprehensive AI law." Even China has issued interim guidelines to regulate the use of generative AI in theory, if not in practice.

Of the leading Nations on AI, the United States stands out for its absence of basic rules of the road. American technology companies and industry leaders have called on the U.S. Government to regulate AI and curtail the privacy and security risks posed by the technology.

I'm eager to hear from our witnesses whether Congress can properly regulate AI, while allowing the innovation to flourish. We should not stop there. To succeed, we need international collaboration and cooperation in the form of a multinational agreement on privacy and security.

It is only when the leading Nations on AI, including China, agree to AI, intellectual property, privacy, and security principles, that we can take full advantage of the benefits AI promises.

I look forward to hearing from our witnesses, and I yield back the balance of my time.

Mr. ISSA. I thank the gentleman.

We now recognize the Ranking Member of the Full Committee, Mr. Nadler, for his opening statement.

Mr. NADLER. Thank you, Mr. Chair, for holding this important hearing today.

Like any new technology, AI can be used for good purposes or for bad purposes, and it has startling political potential. For example, using AI, one could generate political ads, convincing political ads, showing Jim Jordan endorsing Joe Biden or me endorsing Donald Trump.

During our first hearing of this series, I noted that the Government of the People's Republic of China, or PRC, has both manipulated the free-market system and used outright, illegal means to acquire other nations' intellectual property. In a field that largely relies on players to act in good faith, acquisition of new technologies through theft, cyber espionage, and other forms of subterfuge is part of China's broader national security and economic strategy. In no other field of innovation is this truer than in that of artificial intelligence.

The raw material of AI is data. This is why entities backed by the PRC are taking steps to acquire massive quantities of data from the United States and its allies, and they are using all means at their disposal to do so.

Within the past decade, we have seen well-publicized data thefts originating in China, such as the 2015 data breach at the U.S. Office of Personnel Management, the SolarWinds hack back in 2020, and the Microsoft Exchange hack in 2021. The thefts that make headlines are just a small fraction of the total. According to a 2022 report by *CrowdStrike*, which is represented here today, China was behind 67 percent of cyber-attacks between mid-2020 and mid-2021.

Because the Chinese Government exercises authoritarian control over the country's economy, many companies in the PRC are state-affiliated, maintain close ties to military and State security services, and are susceptible to State coercion, or all three.

This blurs the lines between public and private collection of Americans' data. Chinese-affiliated actors are buying data from commercial data brokers. They are also collecting data on U.S. persons through Chinese-owned software applications such as TikTok and medical diagnostic platforms like the DNA-sequencing company BGI.

Even as the Chinese Government attempts to gain access to as much data as possible from the United States and its allies, Chinese officials have taken legal and regulatory steps to limit access to data that originates in China. They have implemented controls that prevent the export and use of such data outside the PRC. Their goal is to gain an unfair advantage over other nations, first by obtaining greater quantities of information, and then by using that information to create new AI capabilities.

The widespread acquisition and deployment of AI by China has implications for the world at large. Using the power of AI, a hacker can scour a network for so-called zero-day vulnerabilities in seconds. An espionage agent tasked with spreading disinformation can create a video that appears to show a domestic political dissident or a foreign political leader confessing to a crime or endorsing the wrong candidate, as I said before.

A police state can track persecuted groups and quell dissent, as the Chinese Government has already done with members of its Uyghur minority.

Until now, the PRC's influence campaigns have mostly targeted its own people, focusing on sources of internal friction such as the status of Taiwan and COVID–19. For example, the DNI found that China did not attempt to influence the 2020 Presidential elections. Many experts agree that posture is swiftly changing, which means that the threat posed by China's development of AI is growing.

Recently, *The New York Times* reported that in an attempt to sow discord within the United States, China used AI-generated images to spread conspiracy theories about the Maui wildfires that caused the deaths of nearly a hundred Americans.

Whether these particular deepfakes were successful remains to be seen, but the danger is unmistakable. Addressing that danger begins with understanding the full nature of China's artificial intelligence strategy and the steps Congress can take to help address the threats posed by it.

For that reason, this series of hearings is absolutely crucial. At the same time, I would also like to add that I appreciate the tactful manner with which these hearings have been conducted.

Even as we protect our national security and intellectual property, we continue to see common ground with China on issues that affect both our countries, such as fighting climate change. Even when we express deep concern over actions taken by the authoritarian Chinese Government, we recognize that those actions do not represent the will of the Chinese people.

The United States, meanwhile, is home to an estimated 17.8 million Asian Americans, including many residents of the Upper West and Upper East sides of Manhattan.

Like so many lawmakers, I have heard from Asian-American constituents who are terrified by the rise in anti-Asian hate and anti-Asian violence that we have seen as friction grows between the PRC and the United States.

I am glad that our hearings have called attention to the very real national security and economic challenges America faces from the policies of the Chinese Government, without demonizing the more than one billion people who live in China or the millions of Asian Americans who make our communities and country stronger every day.

I am hopeful and confident that our important work will continue, not just in this hearing, but in the weeks and months to come.

Thank you, Mr. Chair, and I yield back the balance of my time.

Mr. ISSA. I thank the gentleman.

Without objection, all other opening statements will be included in the record.

It's now my honor to introduce our distinguished panel of witnesses.

Dr. William Hannas is the lead analyst at Georgetown Center for Security and Emerging Technology. Prior to joining CSET, or C-S-E-T, he was a member of the Senior Intelligence Service at the Central Intelligence Agency, where he served as an expert on advanced technical projects and was the three-time recipient of the McCone Award for technological innovation.

Dr. Hannas has also served as Assistant Professor of Chinese at Georgetown while concurrently serving with the CIA's open source enterprise.

We are also joined by Dr. John Brennan. Dr. Brennan is the general manager, public sector, at Scale AI. He has 25 years of experience across the public and private sectors, and has developed and led programs in cloud computing, data science, in support of intelligence collection and analysis, cybersecurity, new product innovation, and supply chain.

He has also served our country in the United States Army with the Central Intelligence Agency and the Office of the Director of National Intelligence.

We're also joined by Dr. Benjamin Jensen. Dr. Jensen is a Senior Fellow for future war-gaming and strategy in the International Security Program at the Center for Strategic and International Studies. He is also a Professor of strategic studies at the Marine Corps University School of Advanced Warfighting.

Dr. Jensen has worked with the Defense Advanced Research Projects Agency of the Marine Corps Warfighting Lab, NATO, and the U.S. Army, and a range of other government agencies and foundations to develop war games and scenario-driven exercises.

Mr. Robert Sheldon. Mr. Sheldon is the Senior Director of Public Policy and Strategy at *CrowdStrike*, where he leads corporate engagement on a variety of U.S. Federal, State, and local government policies, programs, and initiatives. He runs *CrowdStrike*'s election security initiatives, serves as its company's representative to the Joint Cyber Defense Collaborative and IT Sector Coordinating Council, and heads the Congressional Affairs practice.

Mr. Sheldon also serves as an Adjunct Professor/Lecturer on international cybersecurity policy at the American University School of International Service.

We seldom have this much—no, let me rephrase this. On this side of the dais, we never have this much intellect, and even among our distinguished witnesses, all of you stand out.

Pursuant to Committee Rules, I would ask that you please all rise now to take the oath.

Raise your right hand.

Do you swear or affirm under the penalty of perjury that the testimony you are about to give will be the truth and correct to the best of your knowledge, information, and belief, so help you God?

Please be seated.

Let the record reflect that all witnesses answered in the affirmative.

Please know that as witnesses, all your written statements and collateral material you wish to give us will be included in the record. So, with that, I would ask that you limit your actual oral statements initially to five minutes to allow plenty of time for everyone to speak.

I will mention—and I apologize that there has been scheduled a conference for the majority at 11 o'clock. That does not mean we'll necessarily adjourn at that moment, but it does mean that Members will be a little rushed, and we'll try to get as many in as we can before that.

So, with that, we go to Dr. Hannas first for your five minutes. You're recognized.

STATEMENT OF DR. WILLIAM HANNAS

Dr. HANNAS. Chair Issa, Ranking Member Johnson, distinguished the Members of the Subcommittee and staff, I'm grateful for the opportunity to join today's hearing on two topics that have fascinated and, frankly, terrified me over the past decades; namely, China's use of foreign technology to fuel its science and technology enterprise and China's drive to become the world's leader in artificial intelligence.

I'm a founding member of Georgetown University's Center for Security and Emerging Technology where I work with a small team to identify threats posed by Chinese AI. Prior to that, as stated, I was with the CIA where I managed open-source exploitation of Chinese S&T materials and built a program to track China's transfer of U.S. technologies.

These efforts culminated in two books on "Chinese Industrial Espionage," and "China's Quest for Foreign Technology," which became de facto handbooks, and the recent volume—co-authored volume, "Chinese Power and Artificial Intelligence," a comprehensive look at Chinese AI.

China's technology transfer programs date from 1956 and cover every imaginable practice and venue. The link with AI, besides China's use of its collection apparatus to tap global AI know-how, is the likelihood that China will soon, if it has not already, used AI for cyber exploits to further its transfer agenda, an unholy marriage in which advances in the one promotes progress in the other, multiplying existing threats to U.S. and allied security.

I'll talk about these three in turn. First, to Chinese technology transfer practices. It's impossible to condense some 700 pages of book narrative, terabytes of unclassified data, a mile-long list of known cases, and two decades of horror stories, into this brief space.

My testimony accordingly is limited to an overview of how the Chinese transfer system operates, with emphasis on so-called extralegal or gray area transfers, maneuvers, at which China excels and which are devilishly hard to track.

Chinese artificial intelligence. My team does not share the perception that China's alleged lag in generative AI—that is, large language models—absolves us from concern because (A) they're not that far behind; (B) China need not be at the cusp to adapt these models wherever it wishes; and (C) it can literally beg, borrow, and steal what it needs to be competitive; and (D) finally, and I think most importantly, China is aggressively pursuing alternative paths to advanced AI aimed at artificial general intelligence and a first mover advantage.

China's use of tech transfer to further its AI program. This is two-sided. While respecting China's home-grown efforts to build advanced AI which we have come to greatly admire—they do a lot of the good indigenous work—China has not shied from acquiring AI technology from abroad. My team has documented China's use of each of its acquisition venues to advance its AI program. Legal venues of support provided by U.S. multinationals are on a scale that shocks even this jaundiced observer.

A case against China's efforts to relieve the world of proprietary technology is easier to make now than years before, as evidenced by today's hearing. Myths die hard, such as the notion that China can't create in AI or other high-tech disciplines—they can—that it will always be behind—that's not necessarily true—or that exposure to democracy will lead to responsible behavior. We all know how that experiment turned out.

The United States Intelligence Community (USIC), of which I was a part, and to that extent responsible, should also be held accountable for its failure to seriously pursue so-called science and technology, S&T, intelligence; that is, identifying and monitoring foreign S&T threats, and for relegating open source intelligence to an enabler of classified collection rather than regarding open source as an entity worth pursuing in its own right.

In sum, I'm arguing that you can't make good policy if you don't have good data. Our efforts to monitor foreign science and technology, inherently an open-source exercise, are, frankly, pathetic. They're worse than useless because these cosmetic efforts are seen as evidence of measures in places where there are few or none. China, by contrast, runs a world-class open-source S&T intelligence network with a staff, by their admission, of more than 100,000 professionals that is light years ahead of us.

Accordingly, I recommend establishing an entity within the U.S. Government—for lack of a better name—a national science and technology analysis center—outside the USIC, or if that isn't possible, as a stand-alone unit directly within—under the Director of National Intelligence, to collect, analyze, forecast, give timely policy support and, as needed, help mitigate or interdict foreign S&T threats. Since China's ability to appropriate technology is part of its S&T posture, the center would also track these transfers using unclassified data and tradecraft honed by open-source experts.

As for the threat to U.S. IP generally, we've appended to our written testimony some 18 proposed legislative and institutional remedies that address the problem in a nuanced fashion.

That's all I have to say.

[The prepared statement of Dr. Hannas follows:]

CSET CENTER *for* SECURITY *and* EMERGING TECHNOLOGY

Testimony before the House Committee on the Judiciary, Subcommittee on Courts, Intellectual Property, and the Internet
on
"managing the dual challenges of Chinese technology appropriation and China's progress toward general artificial intelligence (AGI)"

William C. Hannas
Research Professor and Lead Analyst
Center for Security and Emerging Technology, Georgetown University
September 20, 2023

Introduction and Summary

Chairman Issa, Ranking Member Johnson, distinguished members of the subcommittee and staff, I am grateful for the opportunity to join today's hearing on two topics that have fascinated—and terrified—me over the past decades, namely, China's use of foreign technology to fuel its science and technology enterprise, and China's drive to be the world's leader in artificial intelligence.[1]

I am a founding member of Georgetown University's Center for Security for Emerging Technology (CSET), where I work with a small team to identify threats posed by Chinese AI. Prior to that, I was an SIS officer in the Central Intelligence Agency, where I managed open source exploitation of Chinese S&T materials and built a program to track China's transfer of U.S. technologies. These efforts culminated in two books on *Chinese Industrial Espionage*[2] and *China's Quest for Foreign Technology*,[3] which became *de facto* handbooks, and the recent volume *Chinese Power and Artificial Intelligence*,[4] a comprehensive look at China AI.

China's technology transfer programs date from 1956[5] and cover every imaginable practice and venue. The link with AI, besides China's use of its collection apparatus to tap global AI know-how, is the likelihood that China will soon—if it has not already—use AI for cyber exploits to further its transfer agenda, an unholy marriage in which advances in the one promote progress in the other, multiplying existing threats to U.S. and allied security.

My testimony covers this topic in three parts:

[1] PRC State Council, "New Generation AI Development Plan" (国务院关于印发《新一代人工智能发展规划》的通知), PRC State Council, 2017.

[2] William C. Hannas, James Mulvenon, and Anna Puglisi, *Chinese Industrial Espionage*. (New York and London: Routledge, 2013).

[3] William C. Hannas and Didi Kirsten Tatlow, eds. *Beyond Espionage: China's Quest for Foreign Technology* (New York and London: Routledge, 2021).

[4] William C. Hannas and Huey-Meei Chang, eds., *Chinese Power and Artificial Intelligence* (New York and London: Routledge, 2023).

[5] "1956-1967 年科学技术发展远景规划纲要 (Outline of the Long-term Plan for the Development of Science and Technology from 1956 to 1967), State Council," August 1956. Ratified in December 1956.

1. China’s technology transfer practices. It’s impossible to condense 700 pages of book narrative, terabytes of (unclassified) data, a mile-long list of known cases, and two decades of horror stories into this brief space. My testimony accordingly is limited to an overview of how the Chinese transfer system operates, with emphasis on “extralegal” or gray area maneuvers, at which China excels and which are devilishly hard to track.

2. Chinese artificial intelligence. My team does not share the perception that China’s alleged lag in “generative” AI large language models (LLMs) absolves us from concern, because (a) China need not be at the cusp to *adapt* these models wherever it wishes; (b) it can literally “beg, borrow and steal” what it needs; and (c) China is aggressively pursuing alternate paths to advanced AI aimed at AGI and a “first mover advantage.”.

3. China’s use of tech transfer to further its AI program. While respecting China’s home-grown efforts to build advanced AI—which we have come to greatly admire—China has not shied from acquiring AI technology from abroad. My team has documented China’s use of each of its acquisition venues to advance its AI program. *Legal* venues of support, provided by U.S. multinationals, are on a scale that shocks even this jaundiced observer.

A case against China’s efforts to relieve the world of proprietary technology is easier to make now than years before, as evidenced by today’s hearing. But myths die hard, such as the notion that China can’t create—in AI or other high-tech disciplines, that it will always be behind, or that exposure to democracy will lead to responsible behavior. The USIC, of which I was a part—and to that extent responsible—should also be held accountable for its failure to seriously pursue so-called S&T intelligence, i.e., identifying and *monitoring* foreign S&T threats, and for relegating open source intelligence to an “enabler” of classified collection.

In sum, I’m arguing *you can’t make good policy if you don’t have good data*. Our efforts to monitor foreign science and technology, inherently an open source exercise, are pathetic. They are worse than useless because these cosmetic efforts are seen as evidence of measures in place, where there are few or none. China by contrast runs a world-class open source S&T intelligence network with a staff of more that 100,000 professionals, that is light-years ahead of us.

Accordingly, I recommend establishing an entity within the USG—a “National Science and Technology Analysis Center”— outside the USIC or, if that is impossible, as a standalone unit directly under the DNI, to collect, analyze, forecast, give timely policy support and, as needed, help mitigate or interdict foreign S&T threats. Since China’s ability to appropriate technology is part of its S&T posture, the Center would also track these transfers using unclassified data and tradecraft honed by open source experts.

As for the threat to U.S. IP generally, we have appended some 18 “Proposed Legislative and Institutional Rememdies” to this testimony that address the problem in a nuanced fashion.

China's foreign technology transfer—in a nutshell

China's quest for the world's technology began in the mid-19th century as an effort to preserve its moribund polity, while relying on foreign nations for the means to defend it. Known as the "*ti-yong*" (体用) policy or "Chinese learning as substance, western learning for application," its spirit has persisted to the present. An excerpt from Xi Jinping's speech in 2013 to an overseas Chinese organization[6] charged with facilitating tech transfer typifies the mentality:

> "As Comrade Deng Xiaoping profoundly pointed out, 'We are carrying out socialist modernization to catch up with the developed capitalist countries economically and, politically, *create a higher and more effective democracy than the capitalist countries*. Moreover, we will train more and better skilled persons than in those countries." [7]

The message was clear: the goal of foreign "exchanges" is, as before, a stronger China; western democracy is not part of the agenda.

Between then and now China has steadily grown its state-supported apparatus for transferring foreign technology:

- 1950s: from its early "lean to one side" (一边倒) reliance on Soviet Russia;
- 1956: through the establishment of a world class open source document procurement system;
- 1978: joint R&D ventures and more overseas study after China's "opening;"
- From the late 1980s on: mobilization of diaspora networks and proliferation of foreign-based S&T support associations;
- 1994: multiple foreign "talent" (人才) outreach programs and the creation of Overseas Chinese Scholar (OCS) returnee parks, where ideas (and IPR) accessed abroad are commercialized in subsidized enclaves;
- 2001: National Technology Transfer Centers, which link Chinese developers to the latest foreign technologies; and,
- more recently, leveraged buyouts of technology-rich companies, state-funded "angel" investments, and sponsorship of international startup competitions—not to mention direct purchases, trade-for-technology clauses, overseas subsidiaries (tech spotting and talent acquisition), state-hosted technology exchange forums (physical and virtual), patent mining, "dual-base" labs, short-term consultative visits, appointments of foreigners to advisory staffs, and a host of illicit activities.[8]

[6] The Western Returned Scholars Association (欧美同学会). The WRSA's charter focuses wholly on benefits the party and state expect to gain by sending students abroad, and on students' obligation to provide those benefits. (http://www.wrsa.net/content_39103492.htm).

[7] Xi Jinping, "使留学人员回国有用武之地，留在国外有报国之门 (This will enable overseas students to be useful when they return to China, and help them serve China if they stay abroad.)." *Xinhua*, October 21, 2013. My italics. http://www.xinhuanet.com//politics/2013-10/21/c_117808372.htm.

[8] Hannas and Chang, "Chinese technology transfer—an introduction" in Hannas and Tatlow, eds., *Beyond Espionage*, (Routledge, 2021), 5.

What follows is an abriged list of venues and practices China uses today to acquire foreign high-tech, categorized by type. Concrete examples of each are provided in our published studies.

Illegal transfers

Breach of contract
Computer network exploitation
Copyright infringement
Insider operations
Reverse engineering
Traditional espionage
Willful patent infringement
Violation of NDAs

Legal transfers

China-based U.S. subsidiaries
Competitions (companies, universities)
Conferences and colloquia
Direct technology purchases
Enrollments at U.S. universities
Investments / acquisition of companies
Joint Sino-U.S. research organizations
Loopholes in trade agreements
Patent mining and exploitation
PRC-backed venture capital funds
Startup accelerators and incubators
State-backed investments in U.S. research
Tech exchanges, trade-for-tech agreements
U.S.-based labs, representative offices

While China's illicit transfers—theft and cyber operations especially—capture most of the public's attention, many such transfers happen right under our noses, forming a gray area of "extralegal" operations, whose legality cannot be determined because no one is looking. The following are their organizational components.

Extralegal transfers (organizations)

Document acquisition facilities
Front organizations for PRC offices
Overseas scholar returnee facilities
PRC ministry offices (national, local)
Recruiting and brokerage websites
Sino-U.S. professional associations
Technology transfer centers
Technology transfer forums
Transfer incentive programs
U.S.-based facilitation companies
U.S.-based student/alumni associations
University-linked "innovation" parks

I omit for lack of space a breakdown of a dozen *classes* of personnel engaged professionally in these extralegal activities;[9] a discussion of the triangular relationship between China's enabling bureaucracy, foreign-based professional support guilds, and 900+ technology transfer centers in

[9] William C. Hannas and Huey-Meei Chang, "China Access to Foreign AI Technology," CSET, September, 2019, 6, https://cset.georgetown.edu/publication/chinas-access-to-foreign-ai-technology/.

China that commercialize or weaponize the take;[10] and a litany of statutory provisions enacted at the state level to facilitate formal *and informal* acquisition of foreign tech, including:[11]

- 1994: "*Ministry of Personnel Notice on 'Implementing Temporary Measures to Subsidize Overseas Chinese Scholars who Return to China for Short Periods to Work in Areas Outside the Educational System'*." Share with the motherland while remaining abroad.

- 2001: "*Circular on the Release of Opinions on Encouraging Overseas Chinese Scholars to Serve the Country by Multiple Means*." Endorsed by five ministries—basically a carte blanche to provide whatever is useful, wherever it is found.

- 2017: "*13th Five-year Plan for S&T Military and Civil Fusion*." Cross-pollination of military and civilian technology, e.g., quantum computing, neuroscience, brain-inspired research, will be supported by a range of foreign outreach initiatives.

We end this section by referring the Committee to a chapter in our 2023 book on China AI, where we offer a tongue-in-cheek apologia for China's behavior based on PRC rhetoric and a more plausible explanation, which ends as follows:

- "China's predatory [transfer] practices will not end when it achieves parity, because the causes of the behavior predate the problem… The upshot is a unique system that avoids blind alleys and allows China to 'leap ahead' on technologies important to China—while skirting liberalization."[12]

China's multiple paths to artificial general intelligence (AGI)

We segue now to this testimony's next focus—China's efforts to leverage advances in AI to promote state and Party goals, in particular, its declared intent to create AGI (通用人工智能) and gain what it calls a "first mover advantage" (先发优势) over competing nations.

"AGI," defined as broadly capable software that can replicate or exceed human functionality in all or most fields of endeavor, has been the holy grail of AI since its inception. Until recently most AI scientists considered the goal decades out, if attainable at all, although Chinese scientists were more optimistic, predicting AGI's arrival in 28 years (median figure) compared to 76 years for their U.S. counterparts.[13] Current thinking has narrowed the window to as few as 1-3 years from now, depending on one's definition of the target.[14]

[10] Colleagues who continue to follow the issue have identified more than a thousand units functioning under various names and occupying simple storefronts to multi-storied, multi-acre mega-complexes.

[11] See Hannas and Chang, "Chinese technology transfer—an introduction" in Hannas and Tatlow, eds., *Beyond Espionage*, (Routledge, 2021), 9-11, for a sample of 18 such measures.

[12] Hannas and Chang, "Foreign support, alliances, and technology transfer," in Hannas and Chang, eds., *Chinese Power and Artificial Intelligence*, (Routledge, 2023), 36-38.

[13] Katja Grace, John Salvatier, Allan Dafoe, Baobao Zhang, Owain Evans, "Viewpoint: When Will AI Exceed Human Performance? Evidence from AI Experts," *Journal of Artificial Intelligence Research* 26, July 2018, 734.

[14] The Millennium Project, "International Governance Issues of the Transition from Artificial Narrow Intelligence to Artificial General Intelligence," Report of Phase 1, 2023, www.Millennium-Project.org. At the heart of the issue is the "goal post" problem, where increasingly capable AI begets increasingly stringent definitions.

Many Chinese researchers do not believe "AGI," as referenced in the dialog on generative large language models, is the only or even the best way of viewing AI's future.[15] Advanced AI can take—and has taken—many forms that exhibit amazing ability in certain fields while performing abysmally in areas that young children easily master. The concern should not be with software that mimics humans but with "super" forms of intelligence that run autonomously, ubiquitously, opaquely, and can bootstrap themselves to higher levels by rewriting their own source code.

These caveats aside, Chinese scientists recognize (a minimum of) three approaches to AGI:

- Machine learning (ML) approaches that rely on big data and massive computing power, as represented by today's highly successful large language models.

- Brain-inspired (类脑) artificial intelligence (BI-AI) based on accurate mathematical descriptions of physical brain processes run as algorithms on computers.

- Brain-computer interfaces (BCI) aimed at cognitive enhancement through direct links between human brains and AI resources, in a continuously improving synthesis.

My team went to some length to identify and describe China's "mainstream" approaches to advanced AI as practiced by ten leading organizations[16] in part because it is important, in part as a counter to the misguided notion that China's relative lag behind leading US and UK companies in ML techniques is a perpetual given. Significant work is being done, which we ignore at our peril, at the same time China leverages close links with the world's AI giants.

Meanwhile, what is overlooked in the fuss over LLMs are China's prodigious efforts to achieve AGI through a brain-inspired approach. BI-AI, while harder to do than "next token prediction" on which today's computational approaches are based, promises to overcome many bottleneck problems that have eluded traditional ML research, such as intuition, creativity, sense making, imagination and planning—all easily done by the three-pound biomass inside our skulls using 25 watts of power. China recognizes this and has invested in some 30 BI-AI labs and centers.[17]

This counter-trend to realize "big tasks with small data" (小数据，大任务) is exemplified in the rise of two major AGI research empires in Shanghai and Beijing, along with significant albeit less well-known efforts in the "provinces." The former is managed by returned Chinese scholar Pu Muming (蒲慕明), whose enterprises include factory-scale primate farms (macaque monkeys) for in vivo experimentation.

The Beijing complex, more recent of the two, is an amalgam of resources from China's top universities (Tsinghua and Beijing), CAS's Institute of Automation, the AI department of CAS University, and a wholly new entity stood up in 2020 whose name—Beijing Institute of General

[15] See "Survey of Chinese scientists and project managers" in Hannas, Chang, Wang, Aiken and Chou, "China AI-Brain Research," CSET, September 2020, 41-45, https://cset.georgetown.edu/publication/china-ai-brain-research/.
[16] Hannas, Chang, Chou and Fleeger, "China's Advanced AI Research," CSET, July 2022, 7-11, https://cset.georgetown.edu/publication/chinas-advanced-ai-research/.
[17] Hannas, Chang, Wang, Aiken and Chou, "China AI-Brain Research," CSET, September 2020, 29-34.

Artificial Intelligence (北京通用人工智能研究院)—belies its mission. BIGAI is run by returned UCLA professor and DARPA funds recipient Zhu Songchun (朱松纯), who regards the program to achieve AGI as on a par with China's historic development of "nuclear weapons, ballistic missiles, and earth satellites."[18]

BIGAI has a targeted staff of 1,000, drawn "from China and abroad."[19] A sense of its scale is given by the following photo:

Source: Beijing Institute of General Artificial Intelligence[20]

The third approach, BCI research, is the topic of a current CSET study focused on China's non-therapeutic use of these interfaces to achieve multiple objectives associated with AGI, including "twin brains" and, at one extreme, digital immortality. The project is summarized by Wu Zhaohui (吴朝晖), former dean of Zhejiang University, Chinese Academy of Science and IEEE member, and vice-director of China's Science ministry:[21]

> "We believe the fusion of brain and machine intelligence represents a new form of future AI, compatible with biological intelligence's perception of environment, cognitive mechanism, and ability to learn how to reason, and with machine intelligence's capability for information integration, storage, and compute.
>
> The basic intent is to start from the brain, use human information processing methods to build a virtual brain, and use brain-computer interaction to realize the fusion and integration of a biological brain, virtual brain, and human-computer intelligence.

[18] Irene Zhang, "AI Proposals at 'Two Sessions'." China Talk, March 8 2023, https://www.chinatalk.media/p/ai-proposals-at-two-sessions-agi.

[19] Chang and Hannas, "Spotlight on Beijing Institute of General Artificial Intelligence," CSET, May 2003, https://cset.georgetown.edu/publication/spotlight-on-beijing-institute-for-general-artificial-intelligence/.

[20] https://www.bigai.ai/about/.

[21] Wu Zhaohui, "From AI to CI—the development of brain-machine intelligence." Global Artificial Intelligence Technology Conference, Hangzhou, China June 5-6, 2021, https://dl.caai.cn/home/Literature/details.html?id=266.

> China's academics and practitioners agree overall with this demarcation of tasks. The 'hybrid enhanced intelligence' in the [2017] New Generation Artificial Intelligence Plan originated from this understanding."

Technology transfer as a tool for AI progress

However one views China's AGI programs—and we consider them highly credible—a decisive factor invariably left out of these East-West comparisons is China's ability to "leap ahead" (超越) in AI development by doing what it has always done when pressed with the need to compete—access foreign know-how.

We considered this phenomenon important enough to have dedicated our Center's inaugural report in 2019 to "China's Access to Foreign AI Technology."[22] We addressed it again in a standalone chapter on "Foreign support, alliances, and technology transfer" in our edited book on China AI,[23] to which we refer the Committee for an in-depth treatment. The main takeaways are (1) China is using, to good effect, the same tried-and-true venues and techniques elaborated over the course of decades for S&T in general to transfer foreign AI, and (2) the efforts are facilitated by the eagerness of U.S. academics and technology companies to bolster China's AI prowess.

Here is an abbreviated list of transfer venues China has used to support its AI agenda:

Venues of foreign support to China AI

Chinese academic institutions
Chinese AI companies
Chinese research and investment abroad
Co-authorship of academic articles
Foreign research and investment in China
Government outreach facilities
Government-sponsored labs
Innovation and returnee parks
Official PRC policy support
Online and physical exchange forums
Overseas study and research
Sino-foreign AI conferences
Sino-foreign cooperation associations
Talent recruitment programs
Technology transfer centers
Think tanks and professional groups.

Evidence from open sources attests to the use of each of these enablers for China's AI development. Research I conducted in 2020 elicited information on more than one hundred "Thousand Talents Plan" (千人计划) co-optees supporting China's AI programs, chiefly from the United States and Europe, despite efforts by the sponsor to obscure their identities.[24] In 2021, we widened the search to include other talent plans listed in CSET's "Chinese Talent Program Tracker."[25] Each program without exception included dozens to thousands of unique references to "artificial intelligence."

[22] Hannas and Chang, CSET, September 2019.
[23] Hannas and Chang, eds., *Chinese Power and Artificial Intelligence*, 2023, 36-53.
[24] Hannas and Chang, "China's artificial intelligence," in Hannas and Tatlow, eds, 2021, 193.
[25] Emily Weinstein, "Chinese Talent Program Tracker," CSET, 2021, https://chinatalenttracker.cset.tech/.

Looking only at the academic dimension, we found examples of Sino-foreign AI transactions spread over ten categories, including training by "international" scientists, multinational alliances, bilateral associations, school-to-school partnerships, foreign-based alumni groups, academic forums, academic sponsorship of commercial ventures, co-authorship of academic papers, "using foreigners to draw in foreigners" and Chinese AI students abroad.[26]

In terms of corporate involvement, we found multiple examples of ongoing support to China AI and information technologies through in-country research facilities established by Amazon, Dell, IBM, Intel, Microsoft, and dozens of others, some of which began in the mid-1980s.

As is true of technology transfer in general, it is disingenuous to attribute these academic and corporate link-ups to a quest for knowledge and profit alone, as the Chinese government's hand can be seen in most of it. For example, China's 2017 "New Generation AI Development Plan"—the gold standard for national AI development—has a Section 4 that reads like a recitation of the transfer techniques described in this testimony's first section.[27] Subsequently, three ministries each issued programs for AI development calling for:

- Full use of international cooperation mechanisms and attracting high-level talent through the "Thousand" and "Ten Thousand Talents" Plans (MIIT); [28]

- "Foreign intellect recruitment innovation bases" (创新引智基地, "Program 111"), joint AI laboratories, importing top scholars, and organizing international AI forums (MOE);[29]

- Use of foreign scientists employed concurrently by foreign and Chinese employers as AI project leaders (MOST).[30]

I conclude this section with an excerpt from a Chinese Ministry of Education notice released in 2020, that deserves to be quoted at length:

> "Aiming at the international cutting edge of AI and at weaknesses in domestic development, increase support for joint training of doctoral students in AI-related fields at home and abroad. Actively encourage high-level talent to carry out international exchanges and expand the depth and breadth of cooperation. Hold internationally influential AI academic conferences and forums and create high-level academic journals. Build a number of AI international cooperative scientific research platforms and bases and strengthen the development and training of international high-end talent. Encourage universities to initiate and organize AI international big science projects (大科学计划) and create international academic organizations and university cooperation alliances. Promote

[26] Hannas and Chang, "Foreign support," in Hannas and Chang, eds., 2023, 45-47.

[27] Hannas and Chang, "China's artificial intelligence," in Hannas and Tatlow, eds., 2021, 189.

[28] 促进新一代人工智能产业发展三年行动计划 (Three-year Action Plan to Promote the Development of New-Generation AI Industry), MIIT 315, 2017. Section 4, "Accelerate the cultivation of talent."

[29] 高等学校人工智能创新行动计划 (AI Innovation Action Plan for Institutes of Higher Education), MOE 3, 2018.

[30] 科技部关于发布科技创新 2030—"新一代人工智能"重大项目 2018 年度项目申报指南的通知 (Project Application Guidelines for S&T Innovation 2030-'New Generation Artificial Intelligence' 2018 Major Projects), MOST 208, 2018.

> the formation of relevant international standards and ethical norms in the field of AI. Vigorously cultivate internationalized talent to participate in its global governance."[31]

What's to be done?

My colleagues and I deeply respect the United States Intelligence Community (USIC), in which we were privileged to serve. Indeed, some of us were responsible for managing issues this testimony addresses. Hence it is with some authority that I testify, in good faith, that the USIC is ill-suited to perform many of the collection and analysis tasks needed to interdict these threats.

The problem is two-fold. Title-50 organizations are chartered—budgeted—to do classified collection through specific venues: HUMINT, SIGINT, IMINT, MASINT, etc. Although each acknowledges the value of open source (OSINT) in principle, in practice it is seen—even referred to—as an "enabler" of the house specialty, not as an -INT worth exploiting in its own right. Secondly, the USIC, in the post-Cold War era especially, has relegated S&T intelligence (STI) to last place behind terrorism, economics, political leadership, and military intentions. These biases have been known since at least 2013, when pointed out by a congressionally established commission charged with reviewing USIC R&D programs,[32] and have led my team to conclude, in exasperation, that:

> "In the United States, STI has the same standing within the USIC's open source community that OSINT has in the broader intelligence community, namely, last at the budgetary trough."[33]

This posture, where open source is the -INT of last resort, is the exact opposite of China's long-standing commitment to exploit OSINT. I detailed China's STI organization and practices in a separate paper but lack space to repeat those findings here, other than to affirm that China beats the U.S. by two or more orders of magnitude in size, quality, automation, professionalism, level of commitment and, importantly—access to state policymakers.[34]

Accordingly, I join my CSET colleagues in recommending in the strongest terms that the USG stand up a dedicated STI organization, outside the USIC or, if necessary, as an office under DNI auspices, provisionally called the "National Science and Technology Analysis Center" to identify, monitor, and alert policymakers of important foreign S&T developments early enough to matter.

While its details are beyond the scope of this testimony, we have considered the matter in depth and would be happy to share our thoughts. Underlying this recommendation is a maxim almost too banal to repeat, namely, good policy depends on good information, which the USG currently lacks. While I have nothing useful to say about what the USG should do to counter the emerging

[31] 关于"双一流"建设高校促进学科融合, 加快人工智能领域研究生培养的若干意见 (Notice on the Publication of "Certain Opinions on Promoting Curricula Merging at 'Double World-Class' Institutes of Higher Education and on Accelerating the Cultivation of Graduate Students in the AI Field"), MOE 4, NDRC, MOF, 2020.

[32] "Report of the National Commission for the Review of the Research and Development Programs of the United States Intelligence Community (unclassified version)," 2013.

[33] Hannas and Chang, "China's STI Operations," CSET, January 2021, 7.

[34] Ibid.

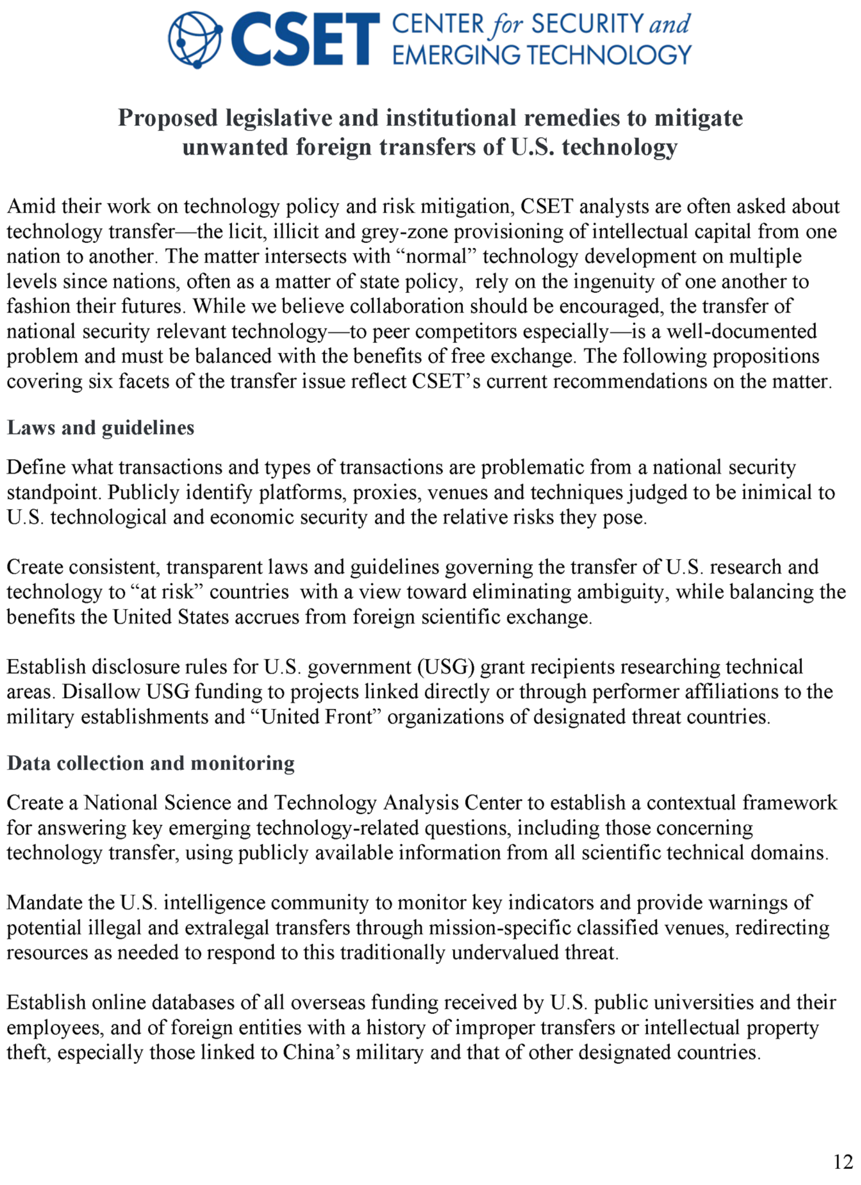
China AI threat, I can say with confidence that we are not at present equipped to understand it, let alone discuss ways to deal with it.

My second recommendation pertains to Chinese technology transfer, outlined in an appendix to this testimony (below). Effective measures depend on timely data, which we lack. The problem mirrors the former conundrum: one cannot interdict unwanted transfers without knowing China's needs, just as one cannot grasp the S&T challenge without knowing what China can steal.

Thank you for this opportunity to testify.

Wm. C. Hannas

Appendix



CSET CENTER *for* SECURITY *and* EMERGING TECHNOLOGY

Proposed legislative and institutional remedies to mitigate unwanted foreign transfers of U.S. technology

Amid their work on technology policy and risk mitigation, CSET analysts are often asked about technology transfer—the licit, illicit and grey-zone provisioning of intellectual capital from one nation to another. The matter intersects with "normal" technology development on multiple levels since nations, often as a matter of state policy, rely on the ingenuity of one another to fashion their futures. While we believe collaboration should be encouraged, the transfer of national security relevant technology—to peer competitors especially—is a well-documented problem and must be balanced with the benefits of free exchange. The following propositions covering six facets of the transfer issue reflect CSET's current recommendations on the matter.

Laws and guidelines

Define what transactions and types of transactions are problematic from a national security standpoint. Publicly identify platforms, proxies, venues and techniques judged to be inimical to U.S. technological and economic security and the relative risks they pose.

Create consistent, transparent laws and guidelines governing the transfer of U.S. research and technology to "at risk" countries with a view toward eliminating ambiguity, while balancing the benefits the United States accrues from foreign scientific exchange.

Establish disclosure rules for U.S. government (USG) grant recipients researching technical areas. Disallow USG funding to projects linked directly or through performer affiliations to the military establishments and "United Front" organizations of designated threat countries.

Data collection and monitoring

Create a National Science and Technology Analysis Center to establish a contextual framework for answering key emerging technology-related questions, including those concerning technology transfer, using publicly available information from all scientific technical domains.

Mandate the U.S. intelligence community to monitor key indicators and provide warnings of potential illegal and extralegal transfers through mission-specific classified venues, redirecting resources as needed to respond to this traditionally undervalued threat.

Establish online databases of all overseas funding received by U.S. public universities and their employees, and of foreign entities with a history of improper transfers or intellectual property theft, especially those linked to China's military and that of other designated countries.

Institutional remedies and reform

Establish within the White House a high, preferably Cabinet-level position to recommend and oversee national technology policy aimed at securing American leadership in critical "new and emerging" fields using expanded information and monitoring resources as identified above.

Create as an adjunct to the above office dedicated policymaking infrastructure to protect the United States from disadvantageous transfers of technologies created on U.S. soil, and by multinational companies (MNCs) headquartered on U.S. soil, to agents of "at risk" countries.

Ensure law enforcement agencies are resourced and able to investigate and prosecute cases of IP theft, fraud, economic espionage, and other forms of legally-defined illicit tech transfer, and that funding agencies have mechanisms to monitor compliance with grant agreements.

Repairing our national S&T base

Build up America's S&T base to avoid a zero-sum struggle. Develop national strategies to promote commercialization of research and to build talent. Appreciate that mitigation is no substitute for positive efforts to create and operationalize wholly new indigenous technologies.

Encourage foreign students and researchers to remain in the United States, become citizens, and help their new country prosper, especially in areas where we face critical shortages. Facilitate the transition by offering a clear path from temporary status to permanent residence and citizenship.

Encourage MNC's to consider the interests of their home country in their technology sharing and stewardship. Corporate advantage should also be interpreted in a national security context, while hedging against the negative impact of overly restrictive measures on free exchange.

Outreach and cooperation

Institute a USG-sponsored outreach program to alert businesses, universities, research labs, foreign governments, foreign students entering the United States, and foreign advocacy groups in the United States to the risks and penalties of illicit transfers.

Acquaint universities and other research institutions with the talent recruitment programs of designated threat countries and pertinent USG policies. Develop recommendations for these institutions to mitigate talent recruitment activity. Fund measures for compliance.

Establish with allied country cooperation a consortium of common cause democratic states chartered to combat hostile appropriation of sensitive and proprietary research, and empowered to share and act on information of general concern.

Foreign talent programs and support guilds

Prohibit all persons, regardless of position or nationality, who are receiving USG research grants from being members of foreign talent recruitment programs and technology support groups identified with designated threat countries.

Broaden the Foreign Agents Registration Act to cover talent program co-optees and technology transfer intermediaries serving foreign states, including technology support groups identified by charter with designated threat countries.

Encourage research organizations to familiarize staff with policies pertaining to designated threat countries' recruitment programs and to update their policies on IP, research integrity, conflicts of interest, and external appointments as necessary.

William C. Hannas
Huey-Meei Chang

Mr. ISSA. Thank you.

Dr. Brennan.

STATEMENT OF DR. JOHN BRENNAN

Dr. BRENNAN. Chair Issa, Ranking Member Johnson, and the Members of the Subcommittee on the Courts, Intellectual Property, and the Internet, thank you for the opportunity to be here today.

My name is John Brennan, and I joined Scale AI in April to lead our public sector business. This work puts me at the crossroads of AI development, government adoption, and its proper governance structure.

Supporting the Federal Government is deeply personal to me. I come from a family with five generations of service to our Nation. I have always felt a strong commitment to ensuring the U.S. leads the world in adopting next-generation technologies that support our democratic values.

Scale was founded in 2016 with the mission of accelerating the development of AI. Scale creates training data, fine-tunes, red teams, tests and evaluates the leading frontier large language models and computer vision system. This puts us in a unique vantage point to best understand the development of safe, secure, and trustworthy AI for the public and private sectors.

While AI is more accessible today, this does not mean the technology is new. Despite years of global investment in the development of these technologies in the U.S., China has a clear lead in certain areas of AI technology, such as computer vision for facial recognition. This is concerning because China's using the technology to suppress the Uyghurs and surveil its population.

The U.S. is ahead when it comes to large language models and generative AI, though this leadership is at risk. Since 2020, China has launched 79 large language models, launched tens of national AI labs, and has been heavily investing in both the compute necessary to power AI and the engineering talent to develop it.

Additionally, this year alone the Chinese Government's investment into AI is at $14.75 billion, which stands in stark contrast to the administration's Fiscal Year 2024 proposal for $5.5 billion in Federal AI spending.

It is critical that the AI is developed and trained in alignment with democratic values. Currently, the best LLMs are developed by some of the leading U.S.-based engineers, and the data they are trained on reflects our democratic ideals.

If the U.S. does not continue to invest in developing generative AI, we risk letting the ideals of the Chinese Government drive AI development around the world. It is imperative that the United States maintains this momentum if we want the most transformative technology of this era to reflect our leadership.

The U.S. has always led the world in adoption of new technologies, and AI will be no different. When it comes to governance, it is better to be right than to be first. To do this, we must work and lead the development of AI through governance frameworks that enable innovation, while putting in place the proper guardrails.

Globally there's no shortage of proposals being generated and passed, and all boil down to a key question: How do we know the AI is safe to deploy?

Scale firmly believes that the best way to ensure AI safety is through active and constant data fine-tuning, through reinforcement learning with human feedback, red-teaming to expose vulnerabilities, and then applying a risk-based approach to test and evaluate to ensure that the AI is safe to deploy. These evaluation methods can incorporate ideals that are critical to protect, like property rights over copyrighted materials and other intellectual property.

For these reasons, the administration has recognized the value of red-teaming and test and evaluation, both in the voluntary commitments that more than a dozen leading companies, including Scale, have agreed to, and through their support for the DEF CON 31 AI Village red team event.

Beyond putting in place the right mechanisms to ensure the development of safe and responsible AI, Congress must play a role to help enact the right governance structure.

In the United States, we have also seen actions that are helping to establish the right foundation. The 2019 AI Executive Order was a key step to help get our Federal agencies ready to adopt AI. More recently, the release of the NIST AI Risk Management Framework, a blueprint for an AI bill of rights, and the Biden-Harris voluntary commitments are essential precursors to any comprehensive legislative package.

Like other emerging technologies, it's also important to first understand any deficiencies within the current or existing laws. Once these gaps are identified, we can address them through rulemaking and new legislation.

While it might feel urgent to act swiftly to keep up with global developments and maintain the United States' strategic advantage, one of the most important things we can do now is to establish an effective regulatory framework that will ultimately be the approach the rest of the world wants to adopt.

Thank you again for the opportunity to be here today, and I look forward to your questions.

[The prepared statement of Dr. Brennan follows:]

scale

STATEMENT BY
JOHN BRENNAN, Ph.D.
GENERAL MANAGER, PUBLIC SECTOR
SCALE AI

BEFORE THE
SUBCOMMITTEE ON THE COURTS, INTELLECTUAL PROPERTY, AND THE INTERNET
OF THE
HOUSE JUDICIARY COMMITTEE

ENTITLED
“IP AND STRATEGIC COMPETITION WITH CHINA: IP THEFT, CYBERSECURITY, AND AI”

SEPTEMBER 20, 2023

Chairman Issa, Ranking Member Johnson, and Members of the Subcommittee on the Courts, Intellectual Property and the Internet, thank you for the opportunity to be here today to testify on the importance of U.S. leadership in the development and adoption of responsible, ethical artificial intelligence (AI).

I am honored to be here today to discuss these topics with you.

INTRODUCTION

My name is John Brennan, and I joined Scale AI (Scale) in April to lead our public sector business. This work enables me to be on the front lines of the intersection between AI development, government adoption, and its proper governance structure.

Supporting the federal government is deeply personal to me as I come from a family with four generations of service to our nation. From my childhood growing up in Mobile, Alabama, to my time at West Point, and throughout my professional career in the military and intelligence community, where I was humbled to serve my family's 100th year of service, I have always felt a strong commitment to ensuring the United States leads the world in the adoption of next generation technologies in support of our democratic values.

Scale was founded in 2016 with the mission of accelerating the development of AI. From our earliest days labeling data for autonomous vehicle programs at companies like General Motors and Toyota, to our commercial work today with the leading frontier model developers like OpenAI, Microsoft and Meta, and our work with federal government stakeholders, like the Department of Defense's (DoD) Chief Digital and AI Office (CDAO) and U.S. Army, Scale has always been on the forefront of AI development.

Today, Scale fine-tunes, red teams, or tests and evaluates nearly all of the leading frontier large language models (LLMs), which provides us a unique vantage point to best understand the development of safe, secure, and trustworthy AI.

AI SUPERIORITY IS CRITICAL TO U.S. GLOBAL LEADERSHIP

While AI may be more accessible today through LLMs, this does not mean that the technology is new. The truth is that AI has been around for decades and is already heavily in use in the U.S. and countries around the world. From the development of the Turing test,[1] to machine learning computer vision algorithms helping automobiles improve their safety and even streaming services suggesting new programs for consumers to watch,[2] machine learning and AI have been in use for decades.

These years of experience have enabled countries around the world to understand how to embrace AI in line with their values and begin crafting a governance framework around them. At a fundamental level, generative AI models learn patterns and structure from large datasets to create new content, and the algorithms and their outputs reflect the values and biases of the information that they are trained on. This is why it is critical that AI is developed and trained in alignment with democratic values. If the U.S. does not continue to heavily invest in maintaining our leadership in the development and adoption of generative AI, we risk letting the ideals of the Chinese government drive AI development around the world.

China is investing disproportionately in AI and has also started to craft its own governance framework that requires AI to adhere to communist party principles.[3] It is clear that China is leveraging the combined influence of government and industry (military-civil fusion), along with distinct IP and cybersecurity rules that favor state control of technology, to drive its AI development efforts.[4]

Despite years of global investment in the development of these technologies from the U.S., China has the clear lead in certain areas of AI, such as computer vision. This was evident in a 2022 global aerial imagery detection contest when teams from China placed first, second, third and fifth .[5] The development of this technology has also extended to facial recognition technologies that are much more prevalent in China today than the U.S. While this may not present an obvious problem, it is concerning

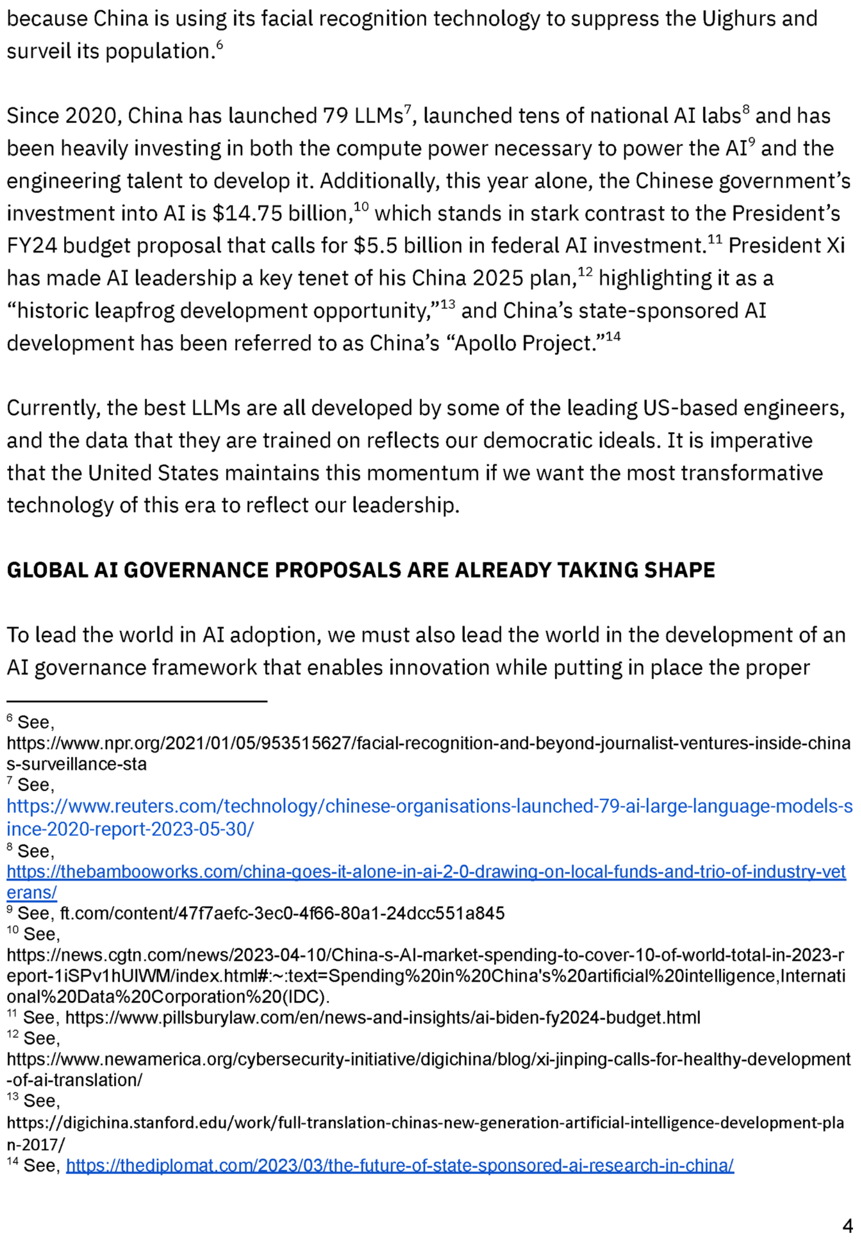
[1] See, https://plato.stanford.edu/entries/turing-test/

[2] See, https://www.simplilearn.com/how-netflix-uses-ai-data-science-and-ml-article#:~:text=How%20does%20the%20Netflix%20algorithm,that%20the%20member%20has%20consumed.

[3] See, https://carnegieendowment.org/2023/07/10/china-s-ai-regulations-and-how-they-get-made-pub-90117

[4] See, https://2017-2021.state.gov/military-civil-fusion/

[5] See, https://paperswithcode.com/sota/object-detection-on-coco



because China is using its facial recognition technology to suppress the Uighurs and surveil its population.[6]

Since 2020, China has launched 79 LLMs[7], launched tens of national AI labs[8] and has been heavily investing in both the compute power necessary to power the AI[9] and the engineering talent to develop it. Additionally, this year alone, the Chinese government's investment into AI is $14.75 billion,[10] which stands in stark contrast to the President's FY24 budget proposal that calls for $5.5 billion in federal AI investment.[11] President Xi has made AI leadership a key tenet of his China 2025 plan,[12] highlighting it as a "historic leapfrog development opportunity,"[13] and China's state-sponsored AI development has been referred to as China's "Apollo Project."[14]

Currently, the best LLMs are all developed by some of the leading US-based engineers, and the data that they are trained on reflects our democratic ideals. It is imperative that the United States maintains this momentum if we want the most transformative technology of this era to reflect our leadership.

GLOBAL AI GOVERNANCE PROPOSALS ARE ALREADY TAKING SHAPE

To lead the world in AI adoption, we must also lead the world in the development of an AI governance framework that enables innovation while putting in place the proper

[6] See, https://www.npr.org/2021/01/05/953515627/facial-recognition-and-beyond-journalist-ventures-inside-chinas-surveillance-sta

[7] See, https://www.reuters.com/technology/chinese-organisations-launched-79-ai-large-language-models-since-2020-report-2023-05-30/

[8] See, https://thebambooworks.com/china-goes-it-alone-in-ai-2-0-drawing-on-local-funds-and-trio-of-industry-veterans/

[9] See, ft.com/content/47f7aefc-3ec0-4f66-80a1-24dcc551a845

[10] See, https://news.cgtn.com/news/2023-04-10/China-s-AI-market-spending-to-cover-10-of-world-total-in-2023-report-1iSPv1hUlWM/index.html#:~:text=Spending%20in%20China's%20artificial%20intelligence,International%20Data%20Corporation%20(IDC).

[11] See, https://www.pillsburylaw.com/en/news-and-insights/ai-biden-fy2024-budget.html

[12] See, https://www.newamerica.org/cybersecurity-initiative/digichina/blog/xi-jinping-calls-for-healthy-development-of-ai-translation/

[13] See, https://digichina.stanford.edu/work/full-translation-chinas-new-generation-artificial-intelligence-development-plan-2017/

[14] See, https://thediplomat.com/2023/03/the-future-of-state-sponsored-ai-research-in-china/

guardrails. The U.S. has always led the world in the adoption of new technologies and crafting the right governance approach for them, although we have not necessarily been the first to implement regulations. AI will be no different.

Globally, there are no shortage of proposals being generated and passed. The European Union recently passed the EU AI Act.[15] Additionally, the United Kingdom[16] detailed a vision for AI regulation and China issued its own guidelines. There have been announcements out of the UN,[17] G20,[18] and more.

These frameworks all boil down to a few key questions, and the most important question is, “How do we know that AI is safe to deploy?”

To best answer this question, we must think about it throughout the entire AI development cycle. AI fundamentally comes down to compute power, a foundational model, and data. In the case of safe deployment of AI, I will focus on the foundational model and data because a model’s performance is only as good as the data it is trained on. Scale has worked on nearly every generative AI advancement and LLM released. We have also pioneered many of industry’s best practices today around data fine-tuning, red teaming, and test and evaluation.

MODEL REFINEMENT & TESTING ARE CRITICAL FOR SAFE AI

Our unique vantage point, working with all major companies in the space, has enabled us to understand how to make AI safe. Scale firmly believes that the best way to do this is through active and constant data fine-tuning, red teaming to expose unintended vulnerabilities, and then applying a risk-based approach to test and evaluation to ensure that the AI is safe to deploy.

AI safety begins with foundational training data that is then fine-tuned for specific use cases through a process known as Reinforcement Learning with Human Feedback (RLHF). In practice, the more RLHF completed on a model, the better performing that model will be as there is a direct tie between model performance and RLHF.

[15] See, https://artificialintelligenceact.eu/the-act/
[16] See, https://www.gov.uk/government/publications/ai-regulation-a-pro-innovation-approach/white-paper
[17] See, https://press.un.org/en/2023/sgsm21880.doc.htm
[18] See, https://cointelegraph.com/news/g20-ai-use-and-development-india

After fine-tuning the data, it needs to undergo testing to uncover vulnerabilities through red teaming, followed by testing and evaluation procedures. These methods rely on industry best practices and consensus-based standards, offering the most reliable means to guarantee the safe deployment of AI for its intended purpose. It is crucial to adopt a risk-based approach that aligns the level of risk with an appropriately rigorous test and evaluation process.

This approach would ensure that higher risk activities, such as using an LLM for cancer research, undergo a more stringent evaluation process than a lower risk activity, like using LLMs for writing routine summaries. While all AI should go through this process, it is clear that certain use cases will require a higher bar.

Evaluation methods, including red teaming and benchmark tests, can incorporate the items that are critical to protect like copyrighted material, intellectual property (IP), and other sensitive topics. While industry still has work to do, this work is well underway.

Recently, Scale published our vision for test and evaluation[19] and will soon publish our technical methodology for our approach that builds on our work with OpenAI and the DoD's CDAO. This framework calls for a combination of machine and human testing, relying on red teaming, evaluation against leading frontier models and benchmark datasets, and human expert review. Once this methodology is released, we intend to work across industry to drive towards a consensus approach that will eventually turn into an industry standard for test and evaluation.

Industry standards are key for the safe deployment of AI and these standards currently are in the early stages of development. Once in place, this will give governments certainty that test and evaluation will be the right approach to ensure AI is safe to deploy. While standards already exist for items like cybersecurity, it is vital that we perform the proper policy gap analysis to best understand where new standards may be necessary for AI and ultimately work to fill the gaps.

For these reasons, the Biden-Harris Administration has recognized the value of red teaming and test and evaluation, both in the voluntary commitments that 15 leading

[19] See, https://scale.com/guides/test-and-evaluation-vision

companies, including Scale,[20] have agreed to and through their support for the DEF CON31 AI Village Red Team event in August 2023.[21] The voluntary commitments specifically call for, amongst other topics, internal and external red teaming and testing to ensure that AI adheres to the AI Bill of Rights blueprint and other responsible AI principles such as the DoD ethical AI principles.[22] Additionally, the recent DEF CON event saw over 2,200 participants red team eight leading LLMs on a test and evaluation platform built by Scale.[23] This event demonstrated the critical role that test and evaluation plays in both model development and ensuring AI is safe to deploy.

ENSURING U.S. LEADERSHIP THROUGH THE RIGHT REGULATORY FRAMEWORK

Beyond putting in place the right mechanisms to ensure the development of safe and responsible AI, it is clear that Congress must play a role to help enact the right governance structure. AI stands out for its ubiquity in people's everyday lives, ranging from machine learning algorithms to LLMs. The use cases for it and its centrality to our day-to-day lives will only continue to grow. Due to the importance of this, Scale fully supports Congress' approach to understanding the complexities of AI before working to legislate.

As mentioned above, we have already seen governments start to develop frameworks that will enable safe, secure, and trustworthy AI. These proposals all have their pros and cons, and are important to understand. However, putting in place an effective governance structure does not mean being first, but it does mean being right.

In the United States, we have also seen actions that are helping to establish the foundation for the right governance structure for AI. The 2019 AI executive order was

[20] See, https://www.whitehouse.gov/briefing-room/statements-releases/2023/09/12/fact-sheet-biden-harris-administration-secures-voluntary-commitments-from-eight-additional-artificial-intelligence-companies-to-manage-the-risks-posed-by-ai/

[21] See,https://www.whitehouse.gov/briefing-room/statements-releases/2023/05/04/fact-sheet-biden-harris-administration-announces-new-actions-to-promote-responsible-ai-innovation-that-protects-americans-rights-and-safety/

[22] See, https://www.defense.gov/News/News-Stories/Article/Article/3429864/dod-committed-to-ethical-use-of-artificial-intelligence/

[23] https://www.airedteam.org/news/more-than-2-200-participants-exchange-more-than-165-000-messages-with-leading-artificial-intelligence-large-language-models-during-the-generative-red-team-challenge

the first key step to help get our federal agencies ready to adopt AI.[24] More recently, the release of the NIST AI Risk Management Framework, blueprint for AI Bill of Rights, and the Biden-Harris voluntary commitments are essential precursors to any comprehensive legislative package. Additionally, the forthcoming executive order and updates to the procurement guidance will continue to move AI forward for the federal government.[25]

Much like other forms of emerging technologies, it is also important to first understand any deficiencies within the existing laws. Once these gaps are identified, we can take appropriate measures to address them through rulemaking or new legislation. For this reason, Scale supports regulating AI through the existing regulatory agencies, with a centralized coordinating body to focus on cross-cutting topics like research and development priorities.

A notable example of this process occurred with the emergence of the Internet and then video streaming, which initially posed challenges to the protection of copyrights and license agreements for text, music, and video content. After identifying the gaps in existing protections, industry and the government collaborated to develop solutions that are now considered the standard operating practices.

While it might feel urgent to act swiftly to keep up with global developments and maintain the United States' strategic advantage against China, one of the most important things we can do now is to establish the most effective regulatory framework that will ultimately be the approach adopted by the rest of the world.

CONCLUSION

Thank you again for the opportunity to be here today to discuss this critically important topic. All of my life, I have believed that the United States can and must demonstrate global leadership. I firmly believe that the U.S. must continue that leadership with the adoption of AI so America and the free world can reap the national security and economic benefits that will accompany it. I look forward to your questions.

[24] See, https://www.federalregister.gov/documents/2019/02/14/2019-02544/maintaining-american-leadership-in-artificial-intelligence

[25] See, https://www.whitehouse.gov/briefing-room/statements-releases/2023/09/12/fact-sheet-biden-harris-administration-secures-voluntary-commitments-from-eight-additional-artificial-intelligence-companies-to-manage-the-risks-posed-by-ai/

Mr. ISSA. Thank you.
Dr. Jensen.

STATEMENT OF DR. BENJAMIN JENSEN

Dr. JENSEN. Chair Issa, Ranking Member Johnson, and distinguished Members of the Subcommittee, I'm going to build off some of their points, and I'll be on time because you have two Army officers in a row, so you're welcome for that.

Mr. ISSA. Go Army, beat Navy.

Dr. JENSEN. I had to do it to you, sir.

No, honestly, I'm kind of envious when I look at you as legislators. You're sitting at a critical moment in history, and just separate all the noise for a second and think about the task at hand. If you get this right, if we get this right, you set the foundation for economic growth, prosperity, and protecting free markets and open societies for the next generation.

So, I'm honestly humbled as a citizen to even be part of helping you have that dialog, and I thank you for continuing to draw attention to it.

Although, now I'm going to be a bit of a downer and talk about the Chinese Communist Party and economic warfare, because it actually—we can't separate your responsibility to us as a Nation from someone actively trying to undermine it.

So, I don't think this competition needs to turn to conflict, but it will almost certainly continue to see networks of operatives wage systematic cyber espionage campaigns.

Put simply, China is trying to cheat its way into the top of industries in the 21st century. The intellectual property they don't subsidize or buy through shell companies, their cyber spies will steal. It would be foolish to think their quest for dominance in AI would be any different.

Let's start with the facts on this. According to the Dyadic Cyber Incident and Campaign Dataset, an academic dataset that studies cyber statecraft, the Chinese Communist Party and leading the PRC is the world's most egregious actor in terms of cyber espionage targeting private firms and linked to stealing intellectual property. Since 2000, China's been associated with 90 documented cyber espionage campaigns against rival states. That's 30 percent more than Russia, to put that into context, and I know we all know Moscow is not the good guy there. The actual number is likely higher, and each instance sees multiple businesses targeted in overlapping priority industries that's specified in the Made in China 2025 Plan. They're targeted, they're deliberate.

The scale of the theft is just staggering. A survey of chief financial officers estimates that one in five U.S. corporations has had their IP stolen. Just think about that for a second—one in five—and I'm sure there's another one that's just not saying.

Some of the leading generative AI systems, in fact, come out of nonprofit research labs that grew out of tech accelerators and not Fortune 500 companies. Why that's important is, if you're a small veteran entrepreneur—I know Representative Cline's done work on that—if you're a small business and you're scraping by to make payroll, are you really buying high-end cybersecurity to protect yourself?

They have to make hard choices and, frankly, our most innovative companies are the 44 percent of our economy that's in small businesses that are most at risk from the world's largest thief.

I want you to imagine for a second a young startup, using generative AI to develop entirely new chemical compounds and materials that could support the green economy. Communist Party-linked advance persistent threat groups could scan the internet for key technologies of interest—you can openly look up, as you know, patents, and where VC money and patents kind of come together is a good indicator—and then they could just go ahead and steal it.

The case is not far-fetched. In 2014, a U.S. grand jury indicted five agents of the People's Liberation Army for hacking SolarWorlds, a firm that was about to release a revolutionary new solar cell.

Every entrepreneur with a new idea for applying generative AI to solve a problem is a target for the largest authoritarian regime the world has ever seen.

Even more disconcerting, APT's link to the Communist Party could seek to undermine cloud computing and chip infrastructure the new AI economy relies on. Imagine an entirely new form of economic warfare in which hackers poison datasets and digitally sabotage data centers in rival States.

Again, this is not as farfetched as it sounds. In 2023, a network of still unidentified hackers—I think we have a good idea who they might be—gained login credentials from major data center operators.

The strategic logic of corrupting rival States' data will only grow as the Communist Party trying to keep data inside China. Therefore, the question before you is; what can Congress do to protect American businesses in this new era of competition? I'll conclude with a few thoughts.

First, there is no cybersecurity without cloud security. Generative AI models require access to large datasets and computer power to learn. Helping companies find ways to protect their data, without stifling innovation, is a critical national security challenge.

If we thought of national security in terms of cybersecurity along these lines, the loss of hundreds of billions of dollars in IP theft would be unacceptable. It would be the equivalent of every ship in the Navy sinking each year.

Second, we have to probably get to what you heard my colleague talk about, to think about how you would go about regulating the gray space used to actually support tech transfers.

This isn't just an AI issue. We have American ships and Shahed drones that are hitting Ukraine and hopefully don't hit one of our other major partners and allies.

Third, this is going to get hard—how do you, without overstepping, actually give grants to small businesses, what CISA does to the dot-gov that actually help them secure their own networks so they can focus on being innovative?

In closing, competition is inevitable. Conflict is not. I think that we can make sure we keep this as competition and not conflict if we maintain the strength of our economy through protecting small businesses and the innovation that drives America. I thank this Committee in particular for really taking the lead on that.

[The prepared statement of Dr. Jensen follows:]

CSIS | CENTER FOR STRATEGIC & INTERNATIONAL STUDIES

Statement before the
House Judiciary Subcommittee on Courts, Intellectual Property, and the Internet

"How the Chinese Communist Party Uses Cyber Espionage to Undermine the American Economy"

A Testimony by:

Dr. Benjamin Jensen

Senior Fellow, International Security Program, CSIS

September 20, 2023
2141 Rayburn House Office Building

CSIS does not take policy positions, so the views represented in this testimony are solely my own and not those of my employers.

Chairman Issa, Ranking Member Johnson, distinguished Members of the Subcommittee, I am honored to sit before the people's house and humbly share my thoughts on how we can protect our future.

The United States is locked in a long-term competition with the Chinese Communist Party (CCP). Even though that competition need not turn to conflict, it will almost certainly continue to see a network of operatives linked to the CCP wage a systematic cyber espionage campaign designed to gain an intelligence advantage and steal intellectual property. Put simply, China is trying to cheat its way to the top of key industries in the 21st century. Their quest to achieve dominance in artificial intelligence and machine learning (AI/ML) is unlikely to be any different.

Let's start with the facts. According to the Dyadic Cyber Incident and Campaign Dataset (DCID), the People's Republic of China is the world's most egregious actor in terms of cyber espionage targeting private firms and linked to stealing intellectual property. Since 2000, China has been associated with 90 cyber espionage campaigns, 30% more than Russia. The actual number is likely higher and each instance sees multiple businesses targeted that overlap priority industries specified in the CCP's "Made in China 2025" plan.[1] In other words, hackers work for communist technocrats in modern China. And, as seen in numerous cases these cyber operations work alongside clandestine human intelligence networks to steal trade secrets from U.S. firms.[2] These multifaceted campaigns have the potential to offset any advantages artificial intelligence brings to cyber defenses, a reality on display in the recent discovery of malware in U.S. critical infrastructure.[3]

Take Operation CuckooBees, a multiyear cyber espionage campaigning targeting multinational companies revealed by Cybereason in 2022.[4] The operation involved APT 41, the same group connected to DOJ indictments in 2020 against five Chinese nationals in connection with hacking over 100 companies.[5] Initial estimates suggest Operation CuckooBees exfiltrated hundreds of gigabytes of intellectual property from companies, much of it linked again to Made in China 2025 national science and technology goals.

[1] Office of the United States Trade Representative. *Findings of the Investigation into China's Acts, Policies, and Practices Related to Technology Transfer, Intellectual Property, and Innovation Under Section 301 of the Trade Act of 1974* (Washington: Executive Office of the President, March 22, 2018) <https://ustr.gov/sites/default/files/enforcement/301Investigations/301%20Draft%20Exec%20Summary%203.22.ustrfinal.pdf>

[2] Frank Cullen "Congress Should Investigate Chinese IP Theft" *The Hill* February 23, 2023 <https://thehill.com/opinion/congress-blog/3871875-congress-should-investigate-chinese-ip-theft/>

[3] Ryan Naraine "Microsfot Catches Chinese.Gov Hackers Targeting U.S. Critical Infrastructure" *Security Week* May 24, 2023 <https://www.securityweek.com/microsoft-catches-chinese-gov-hackers-in-guam-critical-infrastructure-orgs/>

[4] Cybereason Nocturnus. *Operation CuckooBees: Deep-Dive into Stealthy Winnti Techniques* <https://www.cybereason.com/blog/operation-cuckoobees-deep-dive-into-stealthy-winnti-techniques>; Nicole Sganga "Chinese Hackers Took Trillions in Intellectual Property from 30 Multinational Countries" *CBS News* May 4, 2022 < https://www.cbsnews.com/news/chinese-hackers-took-trillions-in-intellectual-property-from-about-30-multinational-companies/>.

[5] Department of Justice Press Release "Seven International Cyber Defendants Including "APT41" Actors, Charged in Connection with Computer Intrusion Campaigns Against More Than 100 Victims Globally" *Department of Justice September* 16, 2020 <https://www.justice.gov/opa/pr/seven-international-cyber-defendants-including-apt41-actors-charged-connection-computer>

The scale of the theft is staggering. A survey of Chief Financial Officers estimates that 1 in 5 U.S. corporations has had their IP stolen.[6] The challenge is especially acute in startups and small businesses, the areas likely to see the greatest innovation linked to AI/ML. The leading generative AI systems we are all experimenting with came from Open AI - a non-profit research lab that grew out of a tech accelerator not a Fortune 100 company.[7] Small businesses account for over 44% of U.S. economic activity.[8] These are the exact firms least likely to invest in state-of-the-art cyber security.

Now, consider how this pattern of activity could accelerate given advances in generative AI. First, it will create new targets for China's espionage campaigns. Imagine a young startup using generative AI to develop entirely new chemical compounds and materials that could support the green economy. Communist party linked advanced persistent threat (APT) groups could scan the internet for key technologies of interest for national development goals and once they found the startup tailor malware to infiltrate its network. For example, the APT group could use generative AI to tailor phishing attempts to gain access and steal intellectual property (IP).[9] The case is not farfetched. In 2014, a U.S. grand jury indicted five agents from the People's Liberation Army for hacking SolarWorlds, a firm that was about to release a revolutionary new solar cell.[10]

Even more disconcerting, APTs linked to the Chinese Communist Party could seek to undermine the cloud computing and chip infrastructure the new AI economy will rely on. Imagine an entirely new form of economic warfare in which hackers poison data sets and digitally sabotage data centers in rival states. Again, this is not farfetched. In 2023, a network of still unidentified hackers gained login credentials for major data center operators. The strategic logic of corrupting rival state's data will only grow as the Chinese Communist Party mandates firms keep Chinese data inside China.[11]

Next, imagine an entirely new form of cyber-enabled political warfare.[12] Tailored messages and deep fakes could undermine trust in public institutions, a phenomenon that has been on the rise globally for the last decade.[13] In fact, we addressed this scenario in the U.S. Cyberspace Solarium

[6] Eric Rosenbaum "1 in 5 Corporations Say China has Stolen their IP Within the Last Year: CNBC CFO Survey" *CNBC* March 1, 2019
< https://www.cnbc.com/2019/02/28/1-in-5-companies-say-china-stole-their-ip-within-the-last-year-cnbc.html>

[7] Sarah O'Neill "History of Open AI" *LXA Hub* May 2, 2023
< https://www.lxahub.com/stories/the-history-of-openai>

[8] *U.S. Small Business Administration Release No. 19-1 ADV*, January 30, 2019
<https://advocacy.sba.gov/2019/01/30/small-businesses-generate-44-percent-of-u-s-economic-activity/>

[9] Susan Caminiti "The Generative AI Battle Between Companies and Hackers is Starting" CNBC August 2, 2023 < https://www.cnbc.com/2023/08/02/the-generative-ai-war-between-companies-and-hackers-is-starting.html>

[10] Christian Roselund "SolarWorld Testifies on Chinese IP Theft" *PV Magazine October* 10, 2017 < https://pv-magazine-usa.com/2017/10/10/solarworld-testifies-on-chinese-ip-theft/>

[11] Raffaele Huang "American Firms Race to Meet China's Data Rule Deadline" *Wall Street Journal* March 1, 2023
< https://www.wsj.com/articles/china-data-transfer-law-adds-to-strains-on-multinationals-91b9764f>

[12] Jensen, Benjamin. 2017. "The Cyber Character of Political Warfare" *Brown Journal of World Affairs* 24: 159-171; Valeriano, Brandon, Benjamin Jensen and Ryan Maness. *Cyber Strategy: The Evolving Character of Power and Coercion* (New York: Oxford University Press, 2018);

[13] Philip N. Howard and Samuel Woolley. *Computational Propaganda: Political Parties, Politicians, and Political Manipulation on Social Media* (New York: Oxford University Press, 2018).

Commission.[14] While, the tactic is more in line with Russian cyber strategy, there is nothing stopping the Chinese Communist Party from adopting a proven playbook using algorithms already available.

It stands to reason that cyber espionage campaigns by the Chinese Communist Party are about to increase in scope and severity with the proliferation of generative AI. APT groups will gain new targets of opportunity as the technology unleashes a business revolution. Every entrepreneur with a new idea for applying generative AI to solve a problem will become a target of the largest authoritarian regime the world has ever seen. The hackers and spies supporting the Chinese Communist Party will use this same technology to develop new forms of malware, holding the American economy at risk from sustained IP theft.

Therefore, the question before you is what can the Congress do to protect American businesses in this new era of competition. I will conclude with a few thoughts.

First, there is no cybersecurity without cloud security. Generative AI models require access to large data sets and compute power to learn. This learning makes them more responsive to users and adaptable to different business cases. Therefore, without data there is no AI. As a result, helping companies find ways to protect their data without stifling innovation is a critical national security challenge. If we thought about national security in terms of cybersecurity along these lines, the loss of hundreds of billions of dollars to IP theft would be unacceptable. It would be the equivalent of every ship in the navy sinking each year.

Second, maybe it is time to take the gloves off. Consider a Cold War sabotage case. In the early 1980s, KGB Directorate 7 routinely used a network of spies and intermediaries to steal IP, including software. In an effort to undermine these activities and the Soviet economy in 1982 President Reagan authorized inserting malware into software code high on the KGB shopping list.[15] The net result was a massive gas pipeline explosion in Siberia that made the Soviet's think twice about the utility of stealing Western IP. I am not advocating we destroy critical infrastructure in the People's Republic of China. I am suggesting that it is time to think about how to undermine the incentives for stealing American IP. Sanctions and indictments don't appear to be enough.

Competition is inevitable. Conflict is not. The United States must find ways to compete outside of military confrontation that deny the ability of the Chinese Communist Party to undermine the American economy. Hearings like this are a positive first step and help to shed light on the magnitude of the challenge ahead. Thank you again for the opportunity to testify.

[14] Montgomery, M., B. Jensen, E. D. Borghard, J. Costello, V. Cornfeld, C. Simpson, and B. Valeriano. 2020. *Cyberspace Solarium Commission Report*. Washington, DC. https://www.solarium.gov/report.

[15] David Hoffman. "Reagan Approved Plan to Sabotage Soviets" *Washington Post* February 27, 2004 < https://www.washingtonpost.com/archive/politics/2004/02/27/reagan-approved-plan-to-sabotage-soviets/a9184eff-47fd-402e-beb2-63970851e130/>

Statistical Appendix
Compiled by Jose Macias, Center for Strategic and International Studies Future Lab

Objective	Russia	China
Espionage	69	90
Disruption	28	22
Degrade	16	2
Total	113	114

Table 1: Cyber Campaign Objectives by Country (2000-2020)

Table 1 summarizes data from the recently published Dyadic Cyber Incident and Campaign Dataset (DCID 2.0).[16] China has engaged in 114 documented cyber campaigns from 2000-2020. Of these 114 documented cases, 90 are attributed to espionage campaigns. Of these 90 espionage cases, 32 operations targeted private entities across 10 different commercial sectors (See Table 2 In appendix). The sectors targeted most frequently were Information Technology (7), Healthcare and Public Health (5) and Energy (4). Regarding the suspected theft of intellectual property, not including personal identifiable information, email or non-trade secrets, DCID recorded China's cyber theft of research on cancer, vaccines, submarines, oil production, blueprints for unmanned vehicles, technical specifications for fifth-generation stealth fighters, nuclear power plant designs, metallurgy secrets, and solar cells.[17]

Select Cases of Espionage on Private Entities

Aviation

Senior defense officials reported that the F-35 Joint Strike Fighter's self-diagnostic system was compromised in 2009.[18] The majority of the files stolen focused on the design and performance statistics of the fighter, as well as its electronic systems.[19] With access to these files, officials suspected that adversaries may reduce the efficiency of the fighter jet by understanding its limitation and performance weaknesses.

A complaint and investigation began into suspected spy Su Bin in 2014 where the U.S. Department of Justice argued his role in the criminal conspiracy to steal military technical data, including data relating to the C-17 strategic transport aircraft and certain fighter jets produced for the U.S. military.[20] Su pleaded guilty and admitted to conspiring with two persons in China from October

[16] Ryan C Maness et al., "Expanding the Dyadic Cyber Incident and Campaign Dataset (DCID): Cyber Conflict from 2000 to 2020," *The Cyber Defense Review*, 2, 8, no. Summer (August 22, 2023): 65–89.
[17] For further review, see DCID 2.0 Incidents # 125, 136, 127, 106, 95, 103
[18] The Guardian, "Chinese Man Charged with Hacking into US Fighter Jet Plans," *The Guardian*, July 12, 2014, https://www.theguardian.com/technology/2014/jul/12/chinese-man-charged-with-hacking-into-us-fighter-jet-plans
[19] U.S. Department of Justice, "Chinese National Pleads Guilty to Conspiring to Hack into U.S. Defense Contractors' Systems to Steal Sensitive Military Information," *Office of Public Affairs* , August 11, 2016, https://www.justice.gov/opa/pr/chinese-national-pleads-guilty-conspiring-hack-us-defense-contractors-systems-steal-sensitive
[20] ibid

2008 to March 2014 to gain unauthorized access to protected computer networks in the United States, including computers belonging to the Boeing Company in Orange County, California, to obtain sensitive military information and to export that information illegally from the United States to China.[21]

In 2011 Chinese intelligence officers focused on the theft of technology underlying a turbofan engine used in U.S. and European commercial airliners.[22] In 2018, The U.S. DOJ indicted Zha Rong and Chai Meng, and other co-conspirators who worked for the Jiangsu Province Ministry of State Security ("JSSD") on charges for breaching aerospace companies based in Arizona, Massachusetts and Oregon.[23] The intelligence officers targeted companies that manufactured parts for the turbofan jet engine. Separate to this indictment, it is also reported that Chinese spies have stolen data on unmanned aerial vehicles (UAV).[24]

Energy Sector

In 2011 it was reported that Chinese intrusions in commercial facilities led initially to the defacement of public facing websites.[25] However, when formal charges were brought in 2018, two individuals were indicted on the theft of data from over 45 companies based in at least 12 states.[26] The U.S. DOJ indicted Zhu Hua and Zhang Shilong who worked for a "technology company" in Tianjin, China, and supported the Chinese Ministry of State Security's Tianjin State Security Bureau in its mission to steal trade secrets. The investigation found that Zhu and Zhang stole data on oil and gas exploration and production. The full extent of the investigation uncovered a deeper web of theft through an array of commercial activity, industries and technologies. These included aviation, satellite and maritime technology, industrial factory automation, automotive supplies, laboratory instruments, banking and finance, telecommunications and consumer electronics, computer processor technology, information technology services, packaging, consulting, medical equipment, healthcare, biotechnology, pharmaceutical manufacturing, and mining. They also gained access to U.S. Department of Energy's Lawrence Berkeley National Laboratory.

Between 2006-2014, Members of the Chinese People's Liberation Army (PLA) broke into Westinghouse Electric Co. (Westinghouse), U.S. subsidiaries of SolarWorld AG (SolarWorld), United States Steel Corp. (U.S. Steel), Allegheny Technologies Inc. (ATI), the United Steel, Paper and Forestry, Rubber, Manufacturing, Energy, Allied Industrial and Service Workers International

[21] ibid

[22] U.S. Department of Justice, "Chinese Intelligence Officers and Their Recruited Hackers and Insiders Conspired to Steal Sensitive Commercial Aviation and Technological Data for Years," *Office of Public Affairs* | United States Department of Justice, July 13, 2022, https://www.justice.gov/opa/pr/chinese-intelligence-officers-and-their-recruited-hackers-and-insiders-conspired-steal

[23] IBID

[24] Edward Wong, "Hacking U.S. Secrets, China Pushes for Drones," *New York Times*, September 21, 2013, https://www.nytimes.com/2013/09/21/world/asia/hacking-us-secrets-china-pushes-for-drones.html

[25] Jeremy Kirk, "'night Dragon' Attacks from China Strike Energy Companies," *PCWorld*, February 10, 2011, https://www.pcworld.com/article/494731/article-1776.html

[26] U.S. Department of Justice, "Two Chinese Hackers Associated with the Ministry of State Security Charged with Global Computer Intrusion Campaigns Targeting Intellectual Property and Confidential Business Information," *Office of Public Affairs | United States Department of Justice*, July 13, 2022, https://www.justice.gov/opa/pr/two-chinese-hackers-associated-ministry-state-security-charged-global-computer-intrusion

Union (USW) and Alcoa Inc. to steal trade secrets and benefit their state-owned enterprises.[27] The operation was not attributed until 2014 when the U.S. concluded their investigation into the breach and indicted five PLA members, Wang Dong, Sun Kailiang, Wen Xinyu, Huang Zhenyu, and Gu Chunhui, who were officers in Unit 61398 of the Third Department of the Chinese People's Liberation Army (PLA).[28]

Maritime

In 2017, Chinese operatives breached the computers of a Navy contractor at a university and stole research on undersea fighting capabilities apart of a Department of Defense (DoD) project named Sea Dragon.[29] The research stolen was on supersonic anti-ship missile that would be fitted on submarines by 2020. Specifically, the intruders stole signals and sensor data, submarine radio room information relating to cryptographic systems, and the Navy submarine development unit's electronic warfare library.[30] Further reporting found that this is not the only instance of research by universities on maritime military capabilities, rather that it is a part of a systematic campaign that targeted at least 27 universities.

[27] U.S. Department of Justice, "U.S. Charges Five Chinese Military Hackers for Cyber Espionage against U.S. Corporations and a Labor Organization for Commercial Advantage," *Office of Public Affairs | United States Department of Justice,* July 22, 2015, https://www.justice.gov/opa/pr/us-charges-five-chinese-military-hackers-cyber-espionage-against-us-corporations-and-labor
Also see: Jose Pagliery, "What Were China's Hacker Spies After?," *CNNMoney*, March 19, 2014, https://money.cnn.com/2014/05/19/technology/security/china-hackers

[28] U.S. Department of Justice, "U.S. Charges Five Chinese Military Hackers for Cyber Espionage against U.S. Corporations and a Labor Organization for Commercial Advantage*," Office of Public Affairs | United States Department of Justice*, July 22, 2015, https://www.justice.gov/opa/pr/us-charges-five-chinese-military-hackers-cyber-espionage-against-us-corporations-and-labor

[29] Accenture, "MUDCARP'S FOCUS ON SUBMARINE TECHNOLOGIES," Accenture, n.d., https://www.accenture.com/_acnmedia/PDF-96/Accenture-Security-MUDCARP.pdf - zoom=50

[30] Ellen Nakashima and Paul Sonne, "China Hacked a Navy Contractor and Secured a Trove of Highly Sensitive Data on Submarine Warfare," *The Washington Post*, June 9, 2018, https://www.washingtonpost.com/world/national-security/china-hacked-a-navy-contractor-and-secured-a-trove-of-highly-sensitive-data-on-submarine-warfare/2018/06/08/6cc396fa-68e6-11e8-bea7-c8eb28bc52b1_story.html

Table 2: Private Entities Affected by Country

Sector	Documented Cyber Espionage Campaigns
Information Technology	7
Healthcare & Public Health	5
Energy	4
Financial Services	3
Government Facilities	3
Academia & Election infrastructure	3
Communications	2
Defense Industrial Base	2
Transportation Sytems	2
Critical Manufacturing	1
Chemical	0
Commercial Facilities	0
Total	32

Source: DCID 2.0

Mr. ISSA. Thank you.
Mr. Sheldon.

STATEMENT OF MR. ROBERT SHELDON

Mr. SHELDON. Chair Issa, Ranking Member Johnson, and the Members of the Subcommittee, thank you for the opportunity to testify.

The People's Republic of China presents significant threats to U.S. national interests today. This Subcommittee, in the previous hearings in the series, has done an admirable job of highlighting the scope and scale of these threats. From the military and diplomatic arenas to all areas of economic and trade relations, the U.S. faces a formidable set of challenges.

CrowdStrike, as a leading U.S. cybersecurity company with global visibility, has a useful vantage on Chinese actions in this space. As a technology, threat intelligence, and services provider for the Federal Government, as well as a commercial provider serving major tech companies, 15 of the top 20 largest U.S. banks, and thousands of small-and medium-sized businesses, we confront all manner of cyber threats.

As a brief primer, *CrowdStrike* tracks threat actors according to three primary motivations: Nation-State, criminal, or hacktivist interests. When we develop sufficient visibility on these groups to identify or attribute them, we assign them a code name. Under this system, Chinese Government-related threat actors are referred to broadly as Pandas. Individual groups receive specific names like Judgment Panda or Vanguard Panda, which often derive from community-based identifiers.

These groups are numerous and prolific. Out of over 220 named actors *CrowdStrike* tracks at the time of this writing, over 50 are Panda groups. For scale, that exceeds the number of groups we track from Russia and North Korea combined.

It's clear that some Panda actors are quite capable. For example, in July, Chinese threat actors once again exploited authentication flaws in a major software company's office productivity and email platform, this time resulting in threat actors' unauthorized access to the email of two Cabinet Secretaries. Under slightly different geopolitical conditions or adversarial objectives, these incidents could've enabled scaled, destructive attacks.

The nexus between cybersecurity and artificial intelligence isn't new, but the intersections are increasing and diversifying. For most of the history of the cybersecurity industry, defenses were primarily reactive. An organization would be breached. At some later point, and sometimes much later indeed, malicious artifacts from that breach would be recovered and disseminated among the security community. Vendors would periodically update signatures in their products based on those artifacts, which would limit their impact going forward. When the artifacts changed even slightly, the process would start again.

Starting approximately a decade ago, *CrowdStrike* pioneered an approach leveraging machine learning and AI to enable a more proactive defense. The innovation focused on detecting anomalous behavior in a chain of system events. A tiny software agent deployed to end points would stream hashes of system events back to a secure cloud environment. AI and machine learning applied against the data in the cloud, as well as AI deployed on the agent itself, would work in concert to detect and prevent threats in real time. Crucially, this approach would work at a scale even for completely novel threats.

Today, defenders also leverage AI for vulnerability management, robust identity threat detection and response, and a host of other use cases. For our part, most recently, we've created a capability leveraging large language models, or LLMs, to provide a natural language interface to key cybersecurity tools. This will radically simplify and speed up work analysts do daily and make certain cybersecurity roles more accessible to people with different skills or less formal training.

Of course, adversaries will also leverage AI. Threat actors have expressed interest in a number of areas. These include crafting more persuasive lures for phishing attacks, vulnerability discovery, exploit and malware development, bulk data processing, and deepfakes. I've included more detail on these threats and others in my written statement.

As the Committee continues its work on AI, I'd like to offer a few recommendations.

First, support continued AI innovation for fields like cybersecurity. Although threat actors will leverage AI, it's important to recognize the significant, current benefits AI is driving in cybersecurity now. Today's solutions overperform, by a wide margin, legacy tools that do not leverage AI. Importantly, attackers will continue to leverage AI to innovate regardless of the rules of the road for defenders.

Second, invest in threat intelligence. The security community must continue to monitor threat actors engaged in intellectual property theft and the use of AI for malicious purposes. The more we understand about these groups, their targeting practices, their resources, and their constraints, the more accurate a threat model we can develop to help us defend against them.

Third, promote U.S. Federal cybersecurity. U.S. Government faces among the most severe threat environments of any organization globally. To the extent that threat actors are able to leverage AI to enhance their capabilities, the U.S. Government will be an early target. Moreover, findings from successfully defending Federal agencies can support the development of best practices of value to other sectors like academia, commercial enterprises, and nonprofits.

Thank you again for the opportunity to testify today, and I look forward to your questions.

[The prepared statement of Mr. Sheldon follows:]

U.S. HOUSE JUDICIARY COMMITTEE
Subcommittee on Courts, Intellectual Property, and the Internet

Robert Sheldon
Sr. Director, Public Policy & Strategy
CrowdStrike

Testimony on "IP and Strategic Competition with China: Part III – IP Theft, Cybersecurity, and AI"

September 20, 2023

Chairman Issa, Ranking Member Johnson, members of the Subcommittee, thank you for the opportunity to testify. The People's Republic of China presents significant threats to U.S. national interests today. This Subcommittee, in the previous hearings in this series, has done an admirable job of highlighting the scope and scale of these threats. From military and diplomatic arenas, to all areas of economic and trade relations, the U.S. faces a formidable set of challenges.

Arguably, the cyber domain is the central front of the U.S.-China competition. For two decades, cyber threat actors associated with the Chinese government have been among the most aggressive and persistent adversaries we face. In addition to pursuing national security and defense information, these actors relentlessly target economic data, trade secrets, and intellectual property. They further spy on minorities, religious groups, political dissidents, journalists, activists, and all manner of other participants in civil society.

CrowdStrike, as a leading U.S. cybersecurity company, has a useful vantage point on China's activities in this space. As a cybersecurity technology, threat intelligence, and services provider for the Federal government, as well as a commercial provider serving major technology companies, 15 of the top 20 largest U.S. banks, and thousands of small and medium sized businesses, we confront all manner of cyber threats.

Today, the cyber challenge from China is heightened because it coincides with an ongoing technological revolution related to Artificial Intelligence (AI). Cybersecurity firms increasingly leverage AI to defeat cyber threats rapidly and at scale. But adversaries too are exploring the use of AI to make their own attacks more effective. Both of these trends are likely to accelerate over the coming years.

U.S.-China competition over the foundational technologies that underpin AI complicates matters further. Beijing recognizes AI as a key technology that merits attention and investment in its own right, and has for some time. But export controls and other trade restrictions implemented over the past several years raise the stakes, limiting China's access to supporting technologies like advanced semiconductors. This elevates already significant cyber risks to semiconductor R&D and manufacturing, and the sector more broadly.

Cyber Threats from China

As a brief primer, CrowdStrike tracks threat actors according to three primary motivations: nation state, criminal, or 'hacktivist' interests. When we develop sufficient visibility on these groups to identify or attribute them, we assign them a codename.[1] Under this system, Chinese government-related threat actors are referred to broadly as *PANDAs*. Individual groups receive specific names like *JUDGMENT PANDA* or *VANGUARD PANDA*, which often derive from community-based identifiers.

These groups are numerous and prolific. Out of over 220 named actors CrowdStrike tracks at the time of this writing, over 50 are PANDA groups. For scale, that exceeds the number of groups we track from Russia and North Korea combined. These groups span China's military, intelligence, and security services as well as associated contractor groups. Each one's entire *raison d'etre* is to advance Chinese Communist Party (CCP) interests through hacking campaigns, whether by targeting U.S. or other foreign institutions and entities.

It's clear that certain PANDA actors are quite capable. For example, in July, Chinese threat actors once again exploited authentication flaws in a major software company's office productivity and email platform – this time resulting in threat actors' unauthorized access to the email of two Cabinet Secretaries.[2] Under slightly different geopolitical conditions or adversarial objectives, these incidents could have enabled scaled destructive attacks.

Cybersecurity and AI

The popularization of generative AI tools over the past year, such as DALL-E and ChatGPT, has catalyzed significant experimentation from practitioners across numerous technical disciplines. Like other disciplines, there are many potential applications of generative AI within cybersecurity–for defenders and attackers alike. But the story of AI and cybersecurity long predates the current groundswell of interest precipitated by broad access to these new tools.

For most of the history of cybersecurity, defenses were primarily reactive. Researchers or incident responders would investigate a breach, identify a related indicator (e.g., Web domain) or file, and add details about it (e.g., a file hash) to a register of suspicious or malicious content. Periodically (e.g, once a day), a security vendor would push updates from this register out to security tools like

[1] For further detail on the rationale for this system, see *George Kurtz, Testimony on Cybersecurity and Supply Chain Threats*, Senate Select Committee on Intelligence (February 23, 2021) https://www.crowdstrike.com/wp-content/uploads/2021/03/george-kurtz-senate-testimony-on-cybersecurity-and-supply-chain-threats-022321.pdf, footnote 2.

[2] See Nakashima, Ellen. Menn, Joseph. Harris, Shane. *Chinese hackers breach email of Commerce Secretary Raimondo and State Department officials.* The Washington Post, July 14, 2023. https://www.washingtonpost.com/national-security/2023/07/12/microsoft-hack-china/; and *Results of Major Technical Investigations for Storm-0558 Key Acquisition*, Microsoft, September 6, 2023. https://msrc.microsoft.com/blog/2023/09/results-of-major-technical-investigations-for-storm-0558-key-acquisition/.

legacy antivirus solutions. Among the many problems with this approach, five were particularly untenable:

1. The model essentially assumed one or more sacrificial victims in order to identify the malicious activity in the first instance.
2. The need for a human "in the loop," deciding that something is malicious, meant that the process would scale very poorly.
3. The latency caused by once daily updates meant attackers could breach multiple victims in a single campaign without initially risking detection from security tools.
4. A single change to a malicious file's binary, or signature, such as by modifying the header of the file, would allow previously-known malware to run undetected.
5. Logs were preserved on-premise and could be tampered with, meaning no immutable record of their activity would be preserved.

This broken model was disrupted a decade ago when CrowdStrike (and later other vendors) introduced technology focused on detecting and preventing indicators of attack. Rather than using a file scan on a computer as a proxy for whether an organization was compromised, the innovation focused on detecting anomalous behavior in the chain of system events. The new approach would deploy a tiny software agent to every endpoint on a network. The agent would stream hashes of system events back to a secure cloud environment. AI and Machine Learning applied against this data in the cloud, as well as AI deployed in the software agent itself, would work in concert to detect and prevent threats in real-time.

Crucially, this approach would work at scale even for completely novel threats. Exhibiting a few shared attributes or characteristics of known malicious activity would be sufficient to trigger a detection and prevention. Helpfully, as the corpus of training data (both legitimate and malicious) grew over time, the AI underpinning this capability became more precise. This drove down the risk of false positives and false negatives.[3]

While the example above describes next-generation antivirus capabilities, there are numerous other cybersecurity applications and tools that similarly benefit from AI. Identity Threat Detection and Response tools can apply AI against data gathered from previous authentication history and elsewhere to dynamically issue multi-factor authentication (MFA) challenges during suspicious login attempts.[4] Vulnerability management tools can leverage AI to dynamically score vulnerabilities in order to help defenders prioritize patching and mitigation.[5]

Large Language Models (LLMs) also have applications for cyber defense. There's a notable deficit of skilled cybersecurity professionals, with one industry study estimating the unmet demand for cybersecurity workers in 2022 to be 411,000; and another study estimating that employer demand

[3] *See Charlotte AI: AI Powered Protection*, CrowdStrike, https://www.crowdstrike.com/falcon-platform/artificial-intelligence-and-machine-learning/.

[4] *See CrowdStrike White Paper on Defending the Enterprise with Conditional Access Anywhere*, CrowdStrike, https://www.crowdstrike.com/resources/white-papers/defending-the-enterprise-with-conditional-access/.

[5] *See How Falcon Spotlight's ExPRT.AI Works*, CrowdStrike, https://www.crowdstrike.com/wp-content/uploads/2021/10/crowdstrike-ml-rating-infographic.pdf.

for cyber workers exceeded supply by 32% .[6] But the use of LLMs can make core cybersecurity workflows more accessible, because users can now interface with tools via natural language.[7] This will enable practitioners to more easily make more meaningful contributions more quickly.

Threat actors will also leverage AI, and we've observed "chatter" from threat actors discussing the possibilities.[8] While this description is not exhaustive, a few near-term threats that merit monitoring include:

- *Lure crafting*. Adversaries could leverage LLMs to write more persuasive lures for phishing attacks that, for example, trick victims into clicking a malicious link. This is particularly salient for threat actors working in a non-native language.
- *Vulnerability discovery*. Adversaries could employ AI techniques to assist in *fuzzing* or assessing crash dumps or related data to identify vulnerabilities.
- *Exploit and malware development*. LLMs have already proven a fairly effective aid in software development, and adversaries could use them to assist in the production of malicious code. Although still subject to hallucinations (e.g., calling non-existent functions or code libraries), outputs are likely to improve as LLMs themselves continue to improve over time.
- *Bulk data processing*. Adversaries could use AI to facilitate the processing of large collections of open source data, or data exfiltrated from breaches, for a variety of malicious purposes. These include identification of sensitive information that could later be used for targeting or extortion.
- "*Deepfakes*." Generative AI can produce deceptive audio or video, which might later be amplified on traditional or social media, to facilitate extortion or influence operations.[9]

In addition to leveraging AI for the purposes described above, a few other issues at the nexus of cybersecurity and AI merit continued attention:

- Adversaries will seek to compromise accounts for paywalled generative AI tools. They could seek access for any number of purposes.
- Adversaries will attempt to defeat AI leveraged in legitimate cybersecurity tools through adversarial examples. To the extent this is successful, the tools' capabilities will degrade or fail.
- Adversaries may target legitimate AI tools themselves with data poisoning and prompt injection attacks. This would affect outputs for other users.
- There's longstanding interest from adversaries in intellectual property related to the systems (e.g., semiconductors, semiconductor fabrication, and cloud providers) that serve as

[6] *See The National Cyber Workforce and Education Strategy*, Office of the National Cyber Director, The White House, July 31, 2023. https://www.whitehouse.gov/wp-content/uploads/2023/07/NCWES-2023.07.31.pdf.

[7] See, for example, *Charlotte AI: Accelerate Cybersecurity with Generative AI Workflows* CrowdStrike, https://www.crowdstrike.com/products/charlotte-ai/.

[8] This section draws heavily from analysis on a forthcoming episode ("AI through the lens of Adversaries and Defenders") of CrowdStrike's Adversary Universe Podcast, which will be released later this month. https://www.crowdstrike.com/resources/adversary-universe-podcast/. This section also references techniques associated with Machine Learning.

[9] *See Contextualizing Deepfake Threats to Organizations*, Cybersecurity Information Sheet by NSA, FBI, CISA, September 2023. https://media.defense.gov/2023/Sep/12/2003298925/-1/-1/0/CSI-DEEPFAKE-THREATS.PDF

the substrate for AI development. This will likely increase as AI develops and export controls impact commercial markets for these technologies.

Recommendations

Continued AI innovation. Although threat actors will leverage AI, it's important to recognize the significant, current benefits AI is driving in cybersecurity tools today. These tools overperform by a wide margin legacy tools that do not leverage AI. Continued innovation in this space is essential. Adversaries will continue to leverage AI to innovate, regardless of the rules of the road for defenders.

Threat intelligence. The security community should continue to monitor threat actors interested in intellectual property theft and the use of AI for malicious purposes. The more we understand about these groups, their targeting practices, their resources, and their constraints, the more accurate a threat model we can develop to help defend targeted industries, organizations, and individuals.

U.S. Federal cybersecurity. The U.S. government faces among the most severe threat environments of any organization globally. To the extent that threat actors are able to leverage AI to enhance their capabilities, the U.S. government will be an early target. Moreover, findings from successfully defending Federal agencies can support the development of best practices of value to other sectors, like academia, commercial enterprises, and nonprofits.[10]

Thank you again for the opportunity to testify today, and I look forward to your questions.

###

[10] For specific recommendations on improving federal cybersecurity, *see Rob Sheldon, Testimony on "Evaluating CISA's Federal Civilian Executive Branch Cybersecurity Programs"* U.S. House Committee on Homeland Security, Subcommittee on Cybersecurity and Infrastructure Protection (September 19, 2023). https://homeland.house.gov/hearing/subcommittee-on-cybersecurity-and-infrastructure-protection-hearing-entitled-evaluating-cisas-federal-civilian-executive-branch-cybersecurity-programs/

Mr. ISSA. Thank you.

I want to announce to everyone that shortly after 11 o'clock, we've agreed, on a bipartisan basis, we'll take a recess of approximately an hour. So, if our witnesses can indulge us by having an early lunch and plan to be back here around noon, our intent is to begin coming back and I'll reconvene.

There may be an intervening vote that we'll have to leave for, but, if at all possible, I want to get everyone an opportunity to ask their questions. This is too important to not find a way to get it done today.

With that, we go to the gentleman from Virginia, Mr. Cline.

Mr. CLINE. Thank you, Mr. Chair. I thank the witnesses for being here.

This is a timely topic and some harrowing scenarios that have been painted here, Mr. Sheldon and Dr. Jensen.

I want to ask Dr. Brennan, you stated that China has also started to craft its own AI governance framework that requires adherence to Communist Party principles. Can you describe those principles?

Dr. BRENNAN. Yes. It's very specific, Congressman. Thank you for the question. They have language in the draft regulation like you cannot use artificial intelligence to subvert the government, and you cannot use it to promote any principle other than those that the Communist Party agrees to. So, it's very oppressive and very counter to the ideals that I think we all hold, and it's very transparent.

Mr. CLINE. How does a U.S. company collect and prepare data for AI training, and how does this compare to how Chinese-backed companies collect and prepare AI data?

Dr. BRENNAN. Thank you for the question, Congressman. First, we start with the rule of law and respect for intellectual property. We use contracts to define the relationships between our customers, the large language model builders, and the services that we're providing, which is helping them create exquisite training datasets, whether it's for a large language model or for the self-driving car industry. The customers are responsible for ensuring that they have a legal right to the data that they're sharing with us for labeling and annotation that we perform that's part of either the training process or the test and evaluation process.

Mr. CLINE. The Chinese-backed companies, how do they compare?

Dr. BRENNAN. In general, I think from the open-source information and from our recent warning by the Five Eyes intelligence leaders yesterday, China's engaged in a broad, organized espionage effort against intellectual property around the world. They take that data and information and give it either to their ministries, defense organizations, or to the State-owned companies that are acting on their behalf.

Mr. CLINE. Are U.S. companies taking appropriate steps to protect their IP and data collection, and if so, can you describe how they're doing so?

Dr. BRENNAN. I think this is improving. As a victim of the OPM hack that took all our security clearance data base several years ago, we're all keenly aware of the risk that cyber actors play.

It's important that agencies like CISA and the Department of Homeland Security continue to have the education and awareness programs that they have, to teach small businesses, universities, and schools, how to have proper cyber hygiene.

A good colleague of mine, even recently, was the victim of ransomware in a family business. So, it's happening all the time, it's a persistent threat, and we need to think about it like changing the batteries in our smoke detector; it always has to happen.

Mr. CLINE. You've spoken today about how China acquires foreign high tech, including investments or acquisitions of companies and PRC-backed venture capital funds. The Congressional Research Service recently addressed this topic in an article related to Light Detection and Ranging Technology, also known as LiDAR. The LiDAR market is developing and advancing quickly, and PRC firms are advancing in this area through access to the U.S. market and technology.

Would it be fair to say that LiDAR integration is a risk for both computer vision systems as well as generative AI?

Dr. BRENNAN. As you know, the United States regulated the remote sensing industry for a number of years and has loosened that, and we've all benefited from global positioning satellite capabilities to drive around. Self-driving cars and other industries use full-motion video, LiDAR, and other technologies to create the computer vision models that they need to perform well.

I could imagine, if I put on my former hat, that information like that would be an attractive target to the Chinese Communist Party and the People's Liberation Army. So, like all the other data that's used in the self-driving car industry, it's a high bar for safety, and those companies are keenly aware of the security that they need to apply and leverage some of the leading security capabilities as you'll hear about today, I would imagine.

Mr. CLINE. So, LiDAR data could be used to train AI or make real-time decisions with generative AI, based on the training data it's been given?

Dr. BRENNAN. So, the generative transformers that Google invented in 2017, we've mainly seen applied to language so far, but it could be applied to other data. It's a large matrix, and I think we'll see more experimentation and other modalities in the coming years.

Mr. CLINE. What concerns do you have that China could use data compiled by LiDAR systems to acquire sensitive information and use this information to conduct military or industrial espionage to gain operational advantages?

Dr. BRENNAN. In warfare, things like understanding the terrain and weather can be classified as secrets. So, any sensor, LiDAR or other otherwise, that helps you understand the general condition or terrain is an important asset, and we would need to protect it in the United States.

Mr. CLINE. Thank you. I yield back.

Mr. ISSA. Thank you.

We now go to Ms. Ross.

Ms. ROSS. Thank you, Mr. Chair and Ranking Member, for holding this very important hearing. I also serve on the Science, Space, and Technology Committee, as do a couple of other Members of this Subcommittee, and we're exploring this very issue.

I understand the potential of AI to launch our country into a new era of innovation. For example, I've heard from healthcare organizations in my district—I represent the Research Triangle area of North Carolina—about ways that AI has revolutionized their processes, from analyzing large swaths of medical data to informing research to help doctors more quickly log patient data. I also recently read an article about how AI has helped with breast cancer detection and been more accurate even than human detection.

Our country has been on the cutting edge of science and technology for decades, and I know that to maintain that position, especially when facing competition with China and other superpowers, we need to harness the power of AI.

That said, we should not sacrifice individual privacy and intellectual property protections purely for the sake of outcompeting China. Just because China is willing to forego the rights of individuals and creators in the name of competition does not mean that we should lower our standards and risk-driving innovators away from our country.

Dr. Brennan, access to vast amounts of unique data is critical to achieving high-performance AI models. Can you describe how disparate policies around data collection and access play a role in our competition with China?

Dr. BRENNAN. Thank you for the question, Congresswoman. I think what's important for us to preserve, as you outline, is the checks and balances we have in the public sector on government activities. Whether it's the Institutional Review Board process for experimentation with human subjects or the sort of classification methods that we use for our intelligence data, each of those rules was set up in a time and place to protect, not only the civil liberties that are related to them and the rights, but also the public service or the public good that's trying to be articulated.

Just as our government dealt with the digitization of information from paper and memos to the internet and email, we have cybersecurity professionals and policies that can help us properly protect the information.

Now, there is still a need for the government to feel more open to experiment. Too frequently we meet with customers, and they have this fear that somehow if they bring data together, it will have a different level of classification or something like that, and it just slows down the ability to even experiment. We've seen this time and time again in my own career. So, the government should also continue to encourage proper experimentation with good risk management approaches, such as what NIST has outlined, so we can keep innovating and get the benefits that you identified such as for medical and healthcare.

Ms. ROSS. Thank you, Dr. Brennan and Dr. Jensen, building on your testimony, as Congress considers proposals for AI regulation, including new agencies dedicated to AI licenses, transparency requirements, and compensation for IP holders, and much more, what do you believe is the best way to balance responsible regulation with maintaining our competitive edge?

Dr. JENSEN. Well, thank you for your question and your dedication to this on both Committees. I would just highlight for you before I answer that, actually healthcare and public health were the second most targeted thing for Chinese IP theft.

So, I tend to take maybe a bit more of a free market approach to this, meaning that we have good checks and balances and classifications, and we can actually submit licenses. What you're hearing my colleagues say about doing the right thing and creating overly cumbersome processes really has to be at the forefront of your mind.

The mantra we use in my own work on this are standards are strategy. If you set the right standards and the right framework, and you let market mechanisms respond to those standards, it becomes a public good that allows for the greater exchange of ideas.

Ultimately, as we're seeing, we can't keep having a technological revolution if we overregulate or curb it before it gets started.

So, I think the really hard task for all of you is what is that balance, what does it look like, what is that licensing framework. If I as an entrepreneur have to spend more money on lawyers to basically submit it and protect myself than I do to hire research scientists, I probably have the wrong balance.

I think one very simple first step is, is there some mechanism to help small entrepreneurs get tax credits or incentives to actually protect their own IP. It's their baby. They want to protect it. So, help them protect it, so we can keep moving forward.

Ms. ROSS. Thank you, Mr. Chair. I yield back.

Mr. ISSA. I thank the gentlelady.

We now go to the gentlelady from Pennsylvania, Ms. Dean.

Ms. DEAN. I thank you, Chair and Ranking Member, thanks to all our testifiers today.

It gives all of us great pause over where we are going, where the globe is going on AI, its regulation.

I guess I'll start with you, Dr. Brennan. You talked about that China has a lead on facial recognition and a little bit of a lag on language. Talk about how they are using the facial recognition—you talked about the Uyghurs—and what can be done in terms of governance, what can be done to interrupt the mal use of facial recognition?

Dr. BRENNAN. Thank you for the question, Congresswoman. It's fairly pervasive, down to the primary school level, where facial recognition is used in classrooms to monitor and track every moment of a student's day. It extends into public spaces. When people are walking around the streets, there's constant monitoring and then facial recognition. Obviously, that's not the kind of world that we would want to live in, although computer vision can help with accident avoidance and in disaster response.

So, I think the key is to continue to go back to the principles that we rely on in the Bill of Rights and the protections that the House and Senate have afforded us all as citizens as we find ways to experiment with computer vision and other uses in our lives. I think that's the situation we are in compared to China.

Ms. ROSS. You talked about, in your testimony and in your written testimony, about governance, coming up with a framework of governance, not being first necessarily but being right. Can you, for a layman, explain what that governance best looks like?

Dr. BRENNAN. Absolutely. Some good examples are, if you turn to the Department of Defense, 10 years ago, the leaders in the Department of Defense wrote their first regulation and rule on how to think about autonomy in weapon systems. They continue to update it. Part of that regulation mandates that there must be senior-level reviewers in the process.

So, that's a good example of rulemaking that those leaders can rely on across the Department to ensure that they're going through tests, safety, and other evaluation techniques as they consider an application of AI and autonomy.

If you work your way down through the executive branch, we've had a series of Executive Orders, we've had a draft AI bill of rights from the administration recently, we've had voluntary commitments from large companies. Most of it centers around ensuring that humans are in the loop and that there's a rigorous test and evaluation process.

So, if you have at least those three legs of the stool here in the beginning, I think we're going to be off to a good start in any of the experimentation an agency or a department's engaged in.

Ms. ROSS. Thank you. That's very helpful.

Dr. Hannas, the final thing that you mentioned in your testimony was to develop a separate science—I missed your working name—for the science center. Could you elaborate on that a little bit.

Dr. HANNAS. The National Science and Technology Analysis Center, I agree, that's not going to make it.

Ms. DEAN. Around here, big long names like that work. They don't work for me, but—

Dr. HANNAS. This has been proposed more than once, and no one ever objects to it, that is, outside of the intelligence community. People think it's a good idea. The arguments are pretty straightforward and compelling.

If you want to understand what's happening globally in science and technology, your best source is open source, by far. What 95–98 percent is available, you can get through unclassified information.

I have seen reports written by the intelligence community that are based almost a hundred percent on open source, and they add a classified snippet here and there to justify their budgets and whatnot. The truth is, for S&T, it's all in open source by and large, and we're not prosecuting it, we're not looking at it.

I mentioned the number—I'm not exaggerating, this is right out of the horse's mouth—100,000 people or more that are dedicated professionally in China to pursuing this one discipline. Frankly, I could count on, there were times, just one hand, the fingers of one hand, how many people in our community were looking seriously at Chinese S&T. So, there's a big disparity.

The problem with the intelligence community is that they will understand the issue. They acknowledge it, pay lip service to the fact that it needs to be done, but at the end of the day, they're focused more on current intel. They always have been. S&T is, by and large, long-term. So, that's one problem.

The other problem is, even those within the community that recognize the value of open source itself tend to regard it more as an enabler of the intelligence—the ends that they are budgeted to support, using the open source, for example, to support human targeting, or SIGINT, queueing and tipping, that kind of thing, and they rarely go beyond that.

Ms. DEAN. I thank you for your answers.

Thank you, Professor Sheldon, also for your recommendations and, Dr. Jensen, especially for your optimism. You're right, we are here at an important time. I think this Committee knows that.

Thank you. I yield back.

Mr. ISSA. I thank the gentlelady.

We now go to the gentleman from Maryland, Mr. Ivey.

Mr. IVEY. Thank you, Mr. Chair. I want to commend you again on these hearings. I appreciate the way you've structured them and the fact that you've focused on this repeatedly, because it's such an important topic, and at least from my perspective, taken a bipartisan approach in doing so. Thank you so much for that.

I did have a question. I think this is for Dr. Jensen. You mentioned the—I think it was 44 percent of small businesses are most at risk in the United States for these sorts of cyber-attacks. I think there was a suggestion about perhaps we could provide some sort of subsidy or some incentives to help these companies protect themselves.

Having come out of a small business, it was a law firm, that was victimized in this way and we had to pay ransomware, I'm sure there's probably millions of companies who need this kind of assistance, but can't afford it or just on the day-to-day calculation you do in your risk analysis, you just try and keep your head low and do your work, but it's going to be a problem. So, what sorts of things could we as Congress do to help provide, whether it's incentives or subsidies or something, to help these small businesses protect themselves?

Dr. JENSEN. Well, thank you, Congressman, for that question, and sorry about the Orioles.

Mr. IVEY. Oh, I'm a Nats fan. So, I'm beyond sorrow, I think. Total grief is where we are, but—

Dr. JENSEN. Yes.

Mr. ISSA. Apparently, that's not a bipartisan shared belief here.

Dr. JENSEN. Generative AI—

Mr. ISSA. The sympathy is limited.

Dr. JENSEN. Generative AI is not going to make better baseball players, so we're going to be hurting for a while.

This is a critical question for someone who grew up raised by, also, a family that thinks about—my parents owned a small business, and so exactly what you're talking about I watched daily. I know it sounds like kitchen table issues, but it was like are we hiring someone, are we firing someone? So, the idea of imagining my mom and dad having to think about spending money on cybersecurity just blows my mind when I think about it.

I think the path ahead for you in Congress is you actually have a great case study in the evolution of CISA. So, I think if you actually go back and look at all the fits and false starts really from 2000 forward, as we formed DHS, you began to pull in different agencies, and kind of really lay that out, that'll give an interesting roadmap, because even though CISA has taken the lead in defending the dot-gov, that's over 100 different agencies, each that are very different with all sorts of diverse concerns.

So, I think that is a great case study to start with and see what worked, what didn't want. The good news is, not to be a shameless self-plug, we're actually launching a big report on that history Monday at CSIS. So, we actually detail that history and talk about how you actually balance that, right. At a minimum, I would think there has to be some type of funding provision.

So, for example, CISA will fund, for those Federal agencies, they get the first two years of continuous diagnostic and monitoring software paid for. After that initial two years, the funding becomes a bit more complicated, but at least you can give that jump start in. So, it would be a question of how you fund it, what's the right tool, and then we can't pay for everything indefinitely, so is there like a sunset period? Is there a cost-sharing provision? I think you actually have a good news story in how CISA has evolved and how you then could apply that to protect the small businesses, sir.

Mr. IVEY. All right. And would that be—just to followup on that a little bit, I mean, sort of a funding source, and I would assume we would knock out—for example, law firms that are doing litigation, I don't know that we'd have to protect those. Those that have certain—qualify perhaps for national security providers of some kind or what sort of parameters could we set, so we could target whatever the funding is and get the most bang for the buck?

Dr. JENSEN. So, I think there's a number of different ways you could go about doing this. One would be look at—I'm not saying we go full Communist Party, but what is our national list of critical technologies, and make the fact if you're in some way, shape, or form involved directly or indirectly with that list, you qualify.

The other is to just closely look at universities. So, I think the same logist actually applies to universities. The top 58 universities between 2002–2010 accounted for 37 percent of patents granted, right. So, you're going to have to help both small businesses who are going fast follower they didn't build, barred, or Llama or Llama 2, but they're going to be really creative in how they're going to implement it.

You're also going to have to go upstream and look at those university ecosystems because their budgets are getting hit every year. We're pulling money back at the State level. Private institutions are even seeing lower enrollment. So, I think there's going to have to be—the funding source will vary by the type of innovation and then even by the type of institution. So, it would be both small businesses and universities. I do think larger businesses, even though they're important, they can make those harder choices, but those are the two I'd be most concerned about, sir.

Mr. IVEY. I'm overtime, but if I could ask just one last question. With respect to the larger companies who maybe aren't putting the money toward this that we would hope that they would, would you propose a certain set of standards that would guide them on that front, or should we just be requiring it at some level? What and how should we approach them?

Dr. JENSEN. Great question again, Congressman. Honestly, that's already been set in motion with some of the requirements to report cyber incidents, and the question is less about how do you do it as harmonizing who they report to. So, if you're a major company and you're publicly traded, are you reporting to the SEC first about this or are you reporting absolutely up how it should be through CISA to actually make sure there's visibility on that compromise.

So, you've actually done a good job across parties on getting that right. It's just going to be harmonizing, because the last thing you want, even if you're a large business, is you get three phone calls, one from the FBI, one from the SEC, and then one from NSA, and then you're wondering which one do I return to first. So, I think those are in place for the larger companies. It's just a question of harmonizing that they know routinely which call they'd take first.

Mr. IVEY. Thank you, Doctor.

Thank you to all the witnesses.

Thank you for your indulgence, Mr. Chair.

Mr. ISSA. You're most welcome. The indulgence came from the Ranking Member, who we'll now recognize, Mr. Johnson of Georgia.

Mr. JOHNSON of Georgia. Thank you, Mr. Chair.

Mr. Jensen, China has used AI-generated images to sow discord related to the Maui wildfires a couple of months ago that took 100 American lives. What is America's exposure to deepfakes and AI-generated images from China? How can that hurt us from a security standpoint?

Dr. JENSEN. I think deepfakes are going to be the defining security issue of the next 10 years. As awful as the wars that we find our partners in across—globally, unfortunately, this is the one that scares me the most, because what happens if you destroy trust in a society? You can't have an open polis and a republic if there isn't the ability to trust the information.

Unfortunately, the technology is moving at a pace right now where it's very difficult to keep up with how you can help both, whether through just convention and practice, people identify the fakes, or do clever things like watermarking images. You still probably won't be able to do it with text, unfortunately.

So, I think that you're grappling with the core issue. I would say that we've seen this too in some of the tabletop exercises we've been running. So, as part of that study on CISA, we got together 60 Federal and private sector CISOs, so from large Federal agencies and large companies, and we then had 1,000 Americans, a representative sample of 1,000 different Americans play the same game. Both populations were more concerned about deepfakes than I originally anticipated.

So, I think both the general public is afraid and anticipated some of what we saw. We did these before the Chinese actually amplified the issues in Maui, and business leaders are. The question is, what do you do about it? I think it's going to have to involve a mix of both technological watermarking, so some requirement to mark images, and it probably is going to have to come up with something like the Motion Picture Association of America.

Like how do we start to have some independent body that certifies well-documented fake things that are circulating? I don't know what that looks like, but I don't think it should be government necessarily, because that will quickly become polarized. If you have some entity that can just allow people to know, hey—I think most people are actually good at heart. I take a Locke view, not a Hobbs view. So, if you let them know they're inadvertently circulating fake stuff, I think a good number of them might back down. They don't want to be kind of told by a stranger they're circulating fake things. So, I think that's where you're going to have to get after it. I don't think we're ever going to stop China from doing it though, so it's just a question of rapidly identifying, triaging, and making sure people understand it's fake.

Mr. JOHNSON of Georgia. Thank you.

Dr. Hannas, what role do you think government should play in making sure that deepfakes and AI-generated images do not do us harm either national security or economically?

Dr. HANNAS. Probably not the best person to answer that question, Congressman. My concern is not so much with deepfakes per se, but with the technology that supports deepfakes, and that is AI moving onto artificial general intelligence, which opens up a whole lot of other scenarios, which we need to pay attention to, deepfakes being just one.

Mr. JOHNSON of Georgia. Would—

Dr. HANNAS. I'm more concerned with control at—discrete control at the neuro level which could actually happen.

Mr. JOHNSON of Georgia. OK. Well, let me ask that same question of Dr. Brennan. Thank you.

Dr. BRENNAN. Thank you, Congressman. I think we've already started to see companies highlight this potential risk, and indeed Alphabet has got a new rule that says, if you're going to do a political advertisement and you're going to use generative AI, you need to disclose that to the viewers.

So, there will be a combination of things that happen in the marketplace because people want customers and they don't want to harm their customers, but it will be important for the intelligence services and law enforcement to carefully monitor foreign groups that are perpetrating these activities and pursue them through all means necessary. We should expect that there will be more of this. China saw what Russia and Iran attempted in previous elections, and we should just expect it all the time now.

Mr. JOHNSON of Georgia. Thank you.

Mr. Sheldon?

Mr. SHELDON. Thank you. Yes, I agree with the other panelists that this is a problem that likely could get worse before it gets better. I'm encouraged to see some experimentation both with people who are producing generative images, like the utilities that have created to do that, and with how some social media networks are promoting the ability for users to tag materials that are shared that may be generated.

I think we need to have some more experimentation like that, as well as potentially some tools that operate as registers where people can identify that they've made and associated with a date, time creation, and intentions so that people can look at that sort of thing after the fact. They see something that looks suspicious and verify whether it exists on such a register. So, those are some of the ideas the community is playing with now.

Mr. JOHNSON of Georgia. If I might, Mr. Chair, just one final question.

Mr. ISSA. Go ahead.

Mr. JOHNSON of Georgia. Dr. Hannas, earlier this summer, the cybersecurity—excuse me, the Cyberspace Administration of China released guidelines for the adoption of generative AI technology, which included new requirements for how algorithms are built and deployed, as well as for what information AI developers must disclose to the government and the public. What is the significance of those regulations?

Dr. HANNAS. I think they're trying to do two things. Part of it is for show. They want to get out in front and demonstrate that they are—that the Chinese Government is aware of the problems with AI and controlling it, on the one hand. On the other hand, I do believe that they are sincerely—Chinese Government is aware of its citizens' concerns with privacy and are trying to address it, because they recognize this as a popular issue, and it's to their advantage to address these issues to keep the public happy, is what it comes down to.

So, part of—it's two sided, like I said. On the one hand they're demonstrating to the world that they care; on the other hand, they're demonstrating to their own population that, yes, we hear your grievance and we're doing something about it.

Mr. JOHNSON of Georgia. Thank you. I yield back.

Mr. ISSA. Thank you.

I'll now recognize myself for a round of questioning.

Dr. Hannas, this Committee enjoys a number of pieces of jurisdiction, and not every question being asked today is within our jurisdiction. One that is clearly within our jurisdiction is whether we grant any intellectual property protection for copyrights, patents, or even trademarks if they're produced using generative AI or not produced by human being in a substantial portion.

Do you recommend that we adopt a policy of not granting intellectual property protection of that sort, specifically patents, trademarks, and copyrights; and if so, how would we enforce that?

Dr. HANNAS. I haven't thought about that problem, no. If I were asked to think about it, as you're doing now, yes, I think we need to accept the inevitable that generative AI—and I don't like to just look at that, because we're really dealing with artificial general intelligence at this point. That's just one manifestation of it. It's happening.

Many of the scenarios, which were science fiction 20 years ago, are being taken seriously. They're talking about instead of 30–40 or 100 years from now in a couple of years from now, we'll be dealing with sentient artificial intelligence. So, we have to accept that this is going to happen and deal with it.

Should we grant it rights? If it's sentient, we have to. I recognize that's not going to satisfy a lot of people, but I'm inclined to think that China is right on this score that we're heading toward a merger of human intellect and artificial intelligence that supersedes both.

Mr. ISSA. Dr. Jensen, I'll ask a similar question of you and sort of put your military and CIA hat on. Let's presume for a moment that one or more countries intend to collapse our intellectual property advantage, much of which is built on the back of intellectual property protection, particularly patents.

Let's presume that this country, we'll just call it China for lack of a better name, ran its AI system for hours, weeks, and months, producing patent claims of things which are not reduced to practice. but reduced to what appears to be reduced to practice, puts a name on it coming out of a lab, we'll call it Huawei just for a name, and, in fact, boxes in with tens of thousands or even millions of claims, obviously costing a lot of money, but boxes in anyone who chooses to actually invent something, and then let's particularly assume that they license some and restrict many, is that a scenario that if any of you were running war games would effectively cripple other countries if you're first to strike?

Dr. JENSEN. Well, thank you for that question, Chair. I volunteer openly before all of you to come run that exact war game on high-end economic competition with your Committees, because I'm a big believer in the importance of that, and I've already done it with conference at offsite. This is part of—

Mr. ISSA. We'll take you up on it.

Dr. JENSEN. Deal. Done. I testified, so I have to. So, this is—I would actually take your scenario and take it one step further. I think a lot of—

Mr. ISSA. That was already bad enough.

Dr. JENSEN. Yes, well, we're going to make it worse, sir. Sometimes, we like to think about the history of military confrontation in terms of great men on horseback and decisive battle, but the more insidious side has always been political and economic warfare, and how States and loose networks of organizations can strict strategic choice and undermine economic productivity or even fundamental rights.

So, you've laid out a really compelling move where you use a combination of technology and our own respect for the rule of law to crowd out the space of any one entrepreneur, that even if—with 10 years later in court we realize that was just a phony patent generated by a bot, heck, even the lawyer claim process turned out to be a fake AI person filing it online, it's already too late, right.

I would compound that further with what really keeps me up is financial market manipulation as well, because there can be no innovation ecosystem if you don't have access to reliable capital. So, I would put those two together and start to ask really hard questions about how do we actually create an environment that makes that difficult, and then probably in other title 50 communities, what is that war in the shadows that denies the adversary the ability to make those moves, which I've talked about it in the written testimony.

I think we did that in the early 1980s with some of the software sabotage that helped the Soviets think twice about stealing American code. We may get back to that world, and I think that's not a bad idea. It's better than open confrontation. It's going to have to be a multifaceted look at economic and political competition going forward, exactly along the lines you lay out, sir.

Mr. ISSA. Thank you.

I'm going to ask one final question, and this one is clearly outside of the jurisdiction of any one Committee, but it's a step that might happen in the foreseeable future. Government has the ability to create regulations or standards. Usually, we do those in concert with industry. When we do them best, we do them in close concerts and collaboration with industry.

We also have the ability within that to require fitness or testing. We'll use the post-2009 stress testing of banks and so on. We haven't done that in cybersecurity. We've allowed it to grow with the idea that the FTC will absolutely cripple you after it happens, unless you're the government and all our clearances are now in hands of nefarious people.

Should we do it, and if so, would a combination of, if you will, a U.S. or even a U.S. and ally global umbrella of basic security layer that is there, and obviously this would be primarily implemented at the cloud level of each of the major cloud participants, many of whom have already on their own initiative done some of this, and then within the cloud community, currently we do not require, and essentially, we'll use Oracle or Microsoft or Amazon, any of them, we don't require them to look into the data bases of their clients for fitness.

Yet, because they're in the cloud and because that technology certainly could be implemented, these companies could have a basic standard of fitness that they would be able to do. The question is, should this be something that Congress looks specifically at and works in concert—Energy and Commerce and other Committees works in concert so that we develop those two tools, the umbrella of protection and the system of fitness?

Dr. JENSEN. So, the good news is, after I answer this, I actually know someone who might be sitting at this table who is an expert on the cloud. So, I'll defer to the cloud part. I think the stress testing, the key would be to do this before something like the 2008 financial crisis, and that's going to be a hard sell, but it's something we thought a lot about on the Cyberspace Solarium Commission.

So, I served as the Senior Research Director on that, and one of the things that kind of lingered over a lot of those recommendations was always this idea of how do you actually work across multiple jurisdictions even within our own elective institutions, but then also with your partners, and I think some of those are starting to bear fruit.

So, the first step was you had to put the ONCD in place to try to, as like Engles said, "be the quarterback," that's still playing itself out but working across to kind of do that. The second level that they're just starting is really this idea of maybe not security cooperation but cyberspace security cooperation, and not obviously the Cyber National Mission Force but teams from DHS and FBI who work with partners.

In all of this, whether it's stress testing or red teaming, the key is—which is actually how Threat Hunt really got started—is to let smart people try to break your system so that you can learn from it. So, whatever the form it takes, if you can just hold onto that and make people play in a way they're open. The benefit of this is the stress testing because you mandate it, banks have to play, they probably pull their punches once in a while, but you know it, it's built up over time, you can monitor it. You would have to do something similar.

The hard question on the stress test would be how many players. There's a massive cyber exercise that takes place every two years, the Cyber Storm that's run there, you'd need something like that or even just to augment some of the requirements of Cyber Storm to get after it. I think the stress test is a phenomenal idea, and I defer on the fitness of the data in the cloud, sir.

Dr. BRENNAN. Thank you, Chair, for the question. If you remember, back in your days in the Army, we had a lot of readiness exercises we would do to be ready and prepared for these sorts of days when they eventually come. I think the cloud service providers have inherent incentives to make sure that their customers are protected. They have programs to constantly remind them of times and ways in which they maybe are not using all the security features of the cloud, and after spending more than seven years working with governments to implement cloud computing technology, I think the leading CIOs and CISOs, even in the Federal Government, believe that they're safer in the cloud.

Now, that said, if Nation States are going to attack us constantly and attack private citizens and private infrastructure, then I think we should also expect our government to protect us.

Mr. ISSA. OK. With that, because we do have conferences of both Republicans and Democrats going, and because there's an unknown question of the vote, I'm going to recess until a time certain, which will be 12:30, unless we are voting on the floor, in which case, extend your lunch.

So, with that, we stand in recess.

[Recess.]

Mr. ISSA. The Committee will come to order.

We'll now go into the—we don't know if anyone else is going to come back, but what you have to say is too important for us not to make the record complete. So, in spite of the fact that we neither have a Speaker nor are we well organized and with adult leaders, this Committee will attempt to do that.

So, I'm going to followup with a couple of questions, but if there are things you want to get out that come up from previous questions and so on, we're going to deal with this like an open forum to a great extent, and if other Members come in, we'll recognize them as they come in.

I want to ask you a broad question, and that is, if China goes unchecked on its current trajectory, what do you believe will be the result to American enterprise? Then the flip side of it is, if we are to act with legislation, regulations, and procedures, what are the most important among them, other than money, which is usually the answer that we get first? So, we'll go and—starting with Mr. Sheldon.

Mr. SHELDON. Thank you, Mr. Chair. I'll constrain my answer to just a couple topics that already came up this morning. First, I wanted to talk about promoting better defenses for people in small business. I think that was a really productive exchange. I just wanted to add a couple points. One is that it is the case that sometimes cybersecurity technologies just operate better at scale, and in addition to being costly, it just helps to be able to build a big, mature security program that can operate 24/7 by 365.

So, one thing that we encourage for policymakers to do is think about how to make accessible things like managed security services, which can kind of bring down that level of maturity that you only usually find in large companies down to very small companies. So, that's a thing that I would encourage for us. It's worth exploring how we can use tax incentives or other tax mechanisms to be able to promote the adoption of those types of technologies in small businesses.

Then the second thing, you asked a great question earlier this morning, from my point of view, on stress testing and thinking about how to get platforms to be able to govern the sort of areas of risk under their control. I think that over the past 15 years, there's been an interesting change in terms of how we've thought about trying to do that.

If you go back to a long time ago, there was some discussion around using internet service providers as the sort of enforcement point to try and protect individual companies or individuals. Then more recently, we've seen some interest in getting cloud service providers to do the same sort of thing. Of course, in both those cases, there's a countervailing interest in protecting individuals' privacy and company interests as well, and that's why the system that we have now is largely predicated on people trying to defend themselves.

There's a thing that's happening within the U.S. Government right now, and it's being driven by CISA, which I think is a really interesting and important way to square the circle, and that is to try and get more concepts like secure by design and secure by default adopted by major platform providers.

The idea behind that is to ensure that you have a situation where companies are accountable for delivering secure services to different users, and that so that vulnerable users aren't the ones bearing the responsibility solely for their own defense. That's a really important concept that we can help promote over time. Thanks.

Mr. ISSA. Dr. Jensen.

Dr. JENSEN. I'm excited to answer this question. Actually, at lunch we were talking about how he wished he could've answered the small business one, sir, so that was great.

I want to start with the first one about unchecked. I wonder what will break first, the Chinese Communist Party or the American economy. I am not an optimist for China's future at all. When you have a nation of 1.4 billion that suppresses basic human freedoms and women's right to even have a productive dialog in their society, that shows you things aren't going well.

Usually, authoritarian regimes are their most dangerous when they're at their death's door, and that means that they will use the competition with the United States as a way to possibly rally around the party, right, to basically come at us at every means possible. I think you've laid out a number of those scenarios, both very creative ways of tying us up legally, accelerating economic warfare, accelerating political warfare, getting us stuck in arms races that are important but ultimately self-defeating from a net assessment standpoint.

Now, how do we compete in that, and what can Congress, in particular, do to compete in that? Because I do think our servicemembers are ready for that challenge, have been planning for some time. I think it gets back to what we're talking about, how do you promote innovative new companies without overregulating them? I 100 percent agree, this is not a money question. This is a smart governance question and creating that kind of playing field, so whether it's—whatever the mechanism, credits, subsidies, there's better experts on that to figure out the right calibration for small businesses and universities, so that you make it harder for the Chinese Communist Party to get in, you alter the cost-benefit calculation.

I think tech standards are more than just secure by design. We need to start sending our top diplomats to the International Technical Union to negotiate new standards and as technology comes online. I do also think the stress testing—I don't know if Congress can mandate that, but whatever instrument you could use to push for more than just Cyber Storm large-scale games.

Mr. ISSA. Just in case you thought it was a made-up question, the concept of how we would do it is to reign in the Federal Trade Commission by creating a safe harbor. Almost every company of any size, their greatest fear is somebody will hack in, some employee will misuse their own authority, and then they will be under a consent decree for years at a very expensive oversight, even happens to very small companies, sometimes putting them out of business.

So, one of the questions we've had in the past—and, again, not completely within our jurisdiction, was the Federal Trade Commission has a great ability, except if you're in government, to beat the living hell out of you after you've already been hurt—

Dr. JENSEN. Yes.

Mr. ISSA. —by some sort of an event, but they do nothing or virtually nothing to tell you what to do to prevent it. They tell you, well, use the best standards. It's like, well, if it fails, by definition they're going to say you didn't meet whatever the best standards were.

Safe haven of a quote, "recognized stress test" and if you will, cloud compliant would seem to be where the government can say, if you do this, we will give you—even if something bad happens, and eventually it will, because nothing is perfect, we give you the safe haven, safe haven from litigation, safe haven from your own government. It doesn't mean you don't have to fix it, it doesn't mean you don't have to make people whole. That was where we saw the soft hand.

Dr. JENSEN. Yes.

Mr. ISSA. The late Colin Powell always said that the way he got problems solved, including in Haiti, was he went down there, and he explained to the dictator that the carrot he was offering is if he left, he wouldn't use the stick. That is sort of what we're saying, is we already have a stick.

Dr. JENSEN. Yes.

Mr. ISSA. Let's find a way to tell people that if they meet standards, we won't use—we won't be allowed to use the stick.

Dr. JENSEN. So, final point to build off that, I think there's something also then, too, to pooling cyber statistics and having transparent data. So, we for years have had the ability to have near misses reported anonymously to the FAA that lets make aviation safer. If we don't start pooling cyber statistics and anonymizing them, we're not going to have a sound set of data to actually be able to price risk. It would be like trying to run the American economy without accurate inflation data, accurate GDP data, accurate unemployment data.

Then, the last would be visibility in supply chains. I'd defer to other folks on that, but how do I make sure that what we produce and is patent protected isn't being bought by front companies and given to our competitors.

Dr. BRENNAN. Chair Issa, back to your first question about if China goes unchecked, I think as we look back on the end of the cold war, there's one story line that says the American economy bankrupted the USSR. So, you can analogize to a world where China tries to fight a war of economic attrition with all the waste and abuse they can try to get into our system through cyber-attacks, theft of intellectual property, et cetera. So, that's a very bleak side of the story, and we definitely have to keep investing in the institutions and government that protect us from that.

On the more positive front, I think our public sector employees need more help. There are now advanced persistent threats that they face every day. The volume of information that they're trying to process on behalf of us all is orders of magnitude larger than what we imagined or had to deal with as young people. They don't have AI-ready data. They just have data.

So, we really need to start working on the more than 700 AI-related initiatives that agencies and departments have identified already. They need to start getting experience around it, and especially how to apply modern security practices to this AI-ready data that are going to create in the new applications that they're going to build to deliver better services to us all.

Mr. ISSA. Thank you.

Dr. Hannas.

Dr. HANNAS. In terms of reigning in China, let me speak to what I know—I think I know best. You're not going to stop the informal technology transfer that's happening. It's been going on since the 1800s by some measure. It's become part of the national psyche, and it's not going to go away, unlike Japan and South Korea and even United States, which once they became developed nations, technologically proficient, they stopped borrowing from abroad.

Mr. ISSA. You're saying informal, so you're saying more universities who publish what they've done and that are shocked that it suddenly disappears into Chinese hues?

Dr. HANNAS. It's a term of art. Informal, extralegal transfer, the kinds of—anything that we don't want to happen that's being transferred is—

Mr. ISSA. So, you're talking about theft?

Dr. HANNAS. Yes, I guess so.

Mr. ISSA. OK. I just want to make sure that—because obviously one of the things that we'd really do, we'd publish in *New England Journal of Medicine* all kinds of things that are very valuable. It costs a lot, and we do, in fact, create a take-it-if-you-want-it environment, but you're talking about over and above that, there's always been somebody sneaking in, getting you to hire one of their people for six months to get to know and then run back.

Dr. HANNAS. We identify three major categories of informal—of technology transfer, legal, illegal, and extralegal, which splits the difference. Extralegal, we don't know whether it's legal or not because we're not observing it. We can, but we don't. We're not equipped to do it, which gets to my point, you won't stop the informal tech transfer, but you can get out in front of it with the right amounts of data.

Chinese scientists, administrators, particularly when they're speaking in Chinese, although they know darn well they're being monitored, they don't feel it in their gut. I'm sure they're listening to me saying this right now and shaking their heads. That's the truth. They say the darnedest things in their open-source materials, and it can all be captured. We've run pilot programs to do that.

So, you can understand what's going to happen in the areas of technology transfer by identifying their needs, first, what do they need—what do they need to acquire that they can't develop on their own, and then also identifying beforehand and monitoring the venues through which they fill these needs, and it's all doable.

As far as the AI development effort, ditto for that. I can't say that I can recommend any policies for how to mitigate it. I'd be speculating. What I can do is say emphatically that if you want to understand where they're going, you can't do it without data. We don't have that data at present. We have snippets here and there from which we could extrapolate. We don't have a whole picture.

Mr. ISSA. I've got a followup question. Currently, what they call a BIS controls the Department of Commerce. It's a major undersecretary position. It controls exports. It's your export control, if you will. It's an export control for hardware effectively. When you look at software, things available on the internet, there isn't, in fact, a specific agency, and that agency is not charged with, for example, saying that this technology or time on this computer is, in fact, a national asset.

So, currently, if I'm sitting in China and I simply rent time on a generative AI computer, if you will, I can actually take what somebody else has developed, and it's fine. I'm just buying it. Yet, that could allow me to develop some of the most sinister items, even if I didn't have the capability in my home country. I'm speaking of China, but I'm also speaking of non-State players anywhere in the world who simply have somebody that's willing to give them the dollars.

What concern do you think we have, and how should we thwart it with—and I'm including non-State actors, because I think we've concentrated on China, that's the primary, but I think this is a broader question of export controls on our AI capability. We'll go the other direction this time.

Dr. HANNAS. I'll take a first crack at that. I've seen so-called military technology control lists come and go. I don't personally think that there is much to be gained by putting together a list of technologies, hardware or software, that are, quote, "at risk, because they're almost always obsolete at the time that they're published," on the one hand. On the other hand, you have to do something. You have to identify what you care about and what you don't care about, so you know what to emphasize.

The bigger issue here is, and you put your finger on it, is this whole notion of, basic science, where that stuff is already patented, not hardware, not machinery, not weapons, but the technologies that are underlying that as they're in the developmental stage. We for a long time, as a country, have drawn like a line there.

Correct me if I'm wrong, colleagues, but my understanding is that we have pretty much let that be open market free reign. It's not something we want to restrict. Now, the National Science Foundation, for example, for the first time is starting to take into account that maybe we need not to be so open in this area.

That's the U.S. side. I can tell you, again, that China understands this perfectly well, and they identify in their open pronouncements the need for them to access technology while it's still in the early stages and while it's still basic science. The one thing they don't really do well is basic science, and for that reason they're eager to acquire it.

Dr. BRENNAN. If I could add to that, I would say, it's important to have this security mindset and overlay exist within each of our agencies and departments, especially as they think about the types of data and types of applications we'll need, each agency and departments continuing to go through a digital transformation in many respects, and they ultimately are closest to how to properly protect and control this data.

I agree with my co-panelists that we want to preserve an open society where people can study what they need to study, learn what they want to, and then create the inventions that we need next, but we should now be mindful of the fact that there is an active, persistent effort to try to steal all that from us.

So, organizations like the Department of Commerce, organizations like CFIUS and others, really need to be close to this problem, and we need to rely on them to come up with the right regulations and rulemaking, because they're so close to the right disciplines and domains that they manage.

Dr. JENSEN. Chair, I think in two extremes you've kind of heard it. You either can lock it all down, in which case, the cost is you will be less innovative just because there's fewer people exchanging information; or you can completely open it up, right, and then you buy innovation through letting people exchange ideas, but with the clear risk of slippage into other nefarious actors.

Obviously, those are extremes, and the challenge of legislation is how to find something in the middle. I think the key to something in the middle should always be an eye on trusting our ability to out innovate our adversaries. The fact that they aren't good at basic research should mean we double down in basic research. Then separately, probably find a way, which would be outside of this Committee, to basically go after it through title 50 means where give them indirect costs for stealing certain things. I just don't think export controls will work in a global supply chain as well as they have maybe historically.

Mr. ISSA. With that, I'm pleased to introduce our acting Ranking Member for his round of questions, the gentleman from California, Mr. Lieu.

Mr. LIEU. Thank you, Chair Issa.

Thank all of you, to the witnesses, for being here.

So, there is this issue I was briefed on earlier where countries like China or Germany and so on will say come to our courts and we'll enforce IP, and then the court will basically set or essentially agree to a worldwide rate for that IP. So, you have a Chinese court educating disputes between a U.S. company and, let's say, a Scandinavian company. It seems sort of absurd to me that this happens, and I don't know why companies here have to listen in Chinese courts, but it ends up there's an agreement that they have to follow. What do you say to sort of try to solve that problem?

Dr. JENSEN. I guess, Congressman, I'll listen to a Chinese court when they listen to their own citizens. I guess, the starting point would be—I think triadic patents are still an important vehicle, because otherwise, if we let any one country just recognize the patent, we see what's happened in the past with those ridiculous curves where it's the number of patents granted by any one country. So, I think finding ways to make sure that you have multiple country recognized versus any one country recognized and then held over the U.S. corporation or any U.S. entity that's being taken to task.

Mr. LIEU. Let me ask you this, are you generally aware of this problem that has started to occur now in countries like China or Germany or other places where they say come to our courts and we're going to set this worldwide rate?

Dr. BRENNAN. It's not an area that we've dealt with on a scale. In general, the idea of people shopping for a venue and then trying to get a consent decree that conforms to the policy they're trying to establish is a tactic that we'll see more of. I think it's important that we continue to push in the World Trade Organization and other international venues the protection of intellectual property and national rights.

There is an effort to have a separate world order that China is trying to organize with Russia, the Taliban, the other organizations they've invited to the Belt and Road Initiative recently. That's not a part of the world order that we want to be part of, so we need to continue to push back with our ideals and values.

Mr. LIEU. OK. Thank you.

So, another question I have is that American businesses are often targeted by China for their intellectual property, either as a cost of doing business in country or through cyber intrusion. Is China targeting artificial intelligence technologies in this way, and have they been successful, if any of you know?

Mr. SHELDON. I can speak to that. Thank you, Congressman. We have seen interest from Chinese threat actors that we associate with a nation State in targeting industries like semiconductors, cloud service providers, and even companies have been doing applied R&D or productization of AI technologies for the purposes of intellectual property theft.

Mr. LIEU. OK. Thank you.

So, the National Institute for Standards and Technology, otherwise known as NIST, describes trustworthy AI as incorporating validity and reliability, accountability, and privacy, among other essential building blocks. In its 2019 AI guidelines, the EU included ethics principles for trustworthy AI. Do you believe Congress should incorporate trustworthy AI into its legislative proposals? What's your view on that?

Dr. BRENNAN. Congressman, thank you for that question. We definitely support the administration and the leading companies around the world who are developing these models in embedding ethical and responsible AI principles in what we're doing. The NIST's AI risk management framework is a great articulation of that, and we also see it being implemented through model regulations and organizations like the U.S. Department of Defense.

In order to really achieve ethical responsible AI, it's important to have humans in the loop at every step and to have test and evaluation methods that rely on benchmark tests that are often created by academic organizations or Federally funded research and development corporations to ensure objectivity.

Mr. LIEU. Even if other countries like China, if they were to not adopt any sorts of guardrails or frameworks like what NIST has put out, do you believe the United States and specifically Congress should still do so?

Dr. BRENNAN. Congressman, I think it's very important for the United States to continue to lead in this regard. In my testimony, I talked about it being more important to get it right than to be first and to create the kind of governance framework that other countries around the world will respect and want to implement.

The alternative is, if we do not continue to lead, China will continue to promote the kinds of regulations that they've been drafting, which include language like you cannot use artificial intelligence to subvert the People's Republic of China, Chinese Communist Party, and the other values that the Chinese Communist Party upholds.

Mr. LIEU. Thank you.

Then my final question to Mr. Sheldon: How has China's acquisition of data through Chinese-based applications, purchases from data brokers, and cyber intrusions assisted the PRC in the development of artificial intelligence, and can you explain this strategy of mass data acquisition?

Mr. SHELDON. Thank you, Congressman. I think we should have an expectation that China will continue to aggregate large data sets for a variety of different purposes. In some instances, it could be the case that there are future-use cases that they haven't even resolved yet that they want to have data stores on hand, and obviously the advent of AI makes data that they have been able to aggregate much more valuable.

So, it seems clear that some of the data stores that they have targeted over the last number of years have informed counterintelligence-use cases, R&D-use cases, and other technological development, and then there could be future ones as well, and we should be alert for that.

Mr. LIEU. Thank you. I yield back.

Mr. ISSA. Well, a time often comes, even in our hearings, when they have to come to an end. I want to thank our witnesses for their testimony.

As is the practice of the Committee, we're going to hold open for five days for additional questions, if you'll agree to take them and respond, additionally any additional thoughts including publications that you think would be helpful. If you submit them, we'll place them in the record.

With that, I thank you again, and we stand adjourned.

[Whereupon, at 1:01 p.m., the Subcommittee was adjourned.]

All materials submitted for the record by Members of the Subcommittee on Courts, Intellectual Property, and the Internet can be found at: *https://docs.house.gov/Committee/Calendar/ByEvent.aspx?EventID=116383*.

○