Testimony before the Subcommittee on Intellectual Property of
the Senate Committee on the Judiciary

"Foreign Competitive Threats to American Innovation and Economic Leadership"

Matt Turpin

April 18, 2023

Chairman Coons, Ranking Member Tillis, and other members of the Committee, thank you for inviting me to testify.

Although I am a Senior Advisor at Palantir Technologies and a Visiting Fellow at Stanford University's Hoover Institution, the views I express here today are my own and are shaped by the last dozen years focused on U.S.-China policy during the Obama and Trump Administrations in the Department of Defense, the Commerce Department, and serving on the staff of the National Security Council as the China Director.

A decade ago, Admiral Dennis Blair and Governor Jon Huntsman chaired the Commission on the Theft of American Intellectual Property. Their work revealed that the United States suffered over $300 billion of annual economic loss due to IP theft and economic espionage primarily by the People's Republic of China (PRC), along with the loss of millions of jobs. The Commission's updates in 2017 and 2021 reveal that these losses have not substantially changed. That is over $3 trillion in losses for just the past decade and there is reason to believe that the number could be much higher.[1]

Starting in late 2017, the Office of the U.S. Trade Representative conducted an investigation under Section 301 of the Trade Act to examine unfair trade practices by the PRC, specifically whether the PRC Government's laws, policies, practices, or actions harm American intellectual property rights, innovation, and technology development. That investigation, which took place over six months, revealed four elements of Beijing's technology transfer regime:

1. The use of opaque administrative processes, joint venture requirements, foreign ownership limitations, and other mechanisms to require or pressure the transfer of valuable U.S. technology and intellectual property to the PRC;
2. PRC government actions and policies that deprive U.S. companies of the ability to set market-based terms in technology-related negotiations;
3. The PRC government direction and unfair facilitation of outbound Chinese investment targeting U.S. companies and assets in key industry and technology sectors; and

[1] *The Report of the Commission on the Theft of American Intellectual Property*, May 2013, https://www.nbr.org/program/commission-on-the-theft-of-intellectual-property/

4. The PRC government's support of economic espionage using human and cyber tradecraft, to include direct participation by PRC intelligence services like the Ministry for State Security.[2]

The IP Commission, the Section 301 Investigation, and dozens of criminal prosecutions by the U.S. Justice Department over multiple Administrations, expose a truth that many have been reluctant to acknowledge: the United States is the victim of a comprehensive and intentional campaign by the People's Republic of China involving criminal acts, espionage, market manipulation, and government policies which result in grave economic and national security harms.

We should face the reality that the cost of these harms exceed the benefit Americans gain from our economic relationship with China.

While often relegated to the conference tables of trade negotiations or court rooms for specific cases, this comprehensive state-sponsored campaign strikes at the very heart of our economy, and the economies of our Allies, and endangers the qualitative military advantage that constitutes our deterrence against both Beijing and Moscow.

Our economy, while broad and diverse, relies upon a foundation of innovation and technology leadership. That foundation is reinforced by a constitutional and legal superstructure, supervised by this Committee, that guarantees property rights, contracts, and transparency which incentivizes innovation and free markets over mercantilism and state control. Our legal and social structures create the environment for innovation, technological development, and prosperity that is the envy of the world. Gaining unfair access to our innovation economy remains a top priority for the PRC as it has yet to successfully create an alternative system.[3]

Our national security is built upon a qualitative military advantage which offsets the quantitative and/or geographic advantages of our potential adversaries. This qualitative advantage creates deterrence by persuading potential adversaries that the costs of military aggression will exceed the benefits they could gain. To create this qualitative military advantage, the U.S. military depends upon unequal access to technological advantages generated by our innovation economy.

In other words, as our innovation economy creates technological breakthroughs, the U.S. military and our allies field those breakthroughs first, maintaining a qualitative military advantage and providing us with the capability to deter aggression by rivals. This strategic logic

---

[2] *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*, Office of the United States Trade Representative, March 22, 2018, https://ustr.gov/issue-areas/enforcement/section-301-investigations/section-301-china/investigation

[3] That is not to say that the PRC cannot succeed or that it has not had success in some areas of innovation. On the whole, the PRC still relies on access to American and allied innovation economies to drive their own growth and prosperity.

has served as America's basic approach in deterring aggression since the end of the Second World War.

The Chinese Communist Party is attacking this dynamic system with its comprehensive campaign of forced technology transfer and economic espionage. Beijing seeks to rob the United States and its allies of these economic and national security advantages. In doing so, the PRC abuses its access to a globalized economic system, which is "expressly based on the principles of non-discrimination, market access, reciprocity, fairness and transparency" to create opportunities for itself at the expense of the United States and other open societies.[4] These opportunities provide Beijing with the means to remake the international system into one that protects the interests of authoritarian regimes and undermines those countries committed to democratic principles and market economies.

Our law enforcement and judicial systems are designed to deal with specific crimes, yet what we have experienced over the past three decades has be a coordinated, comprehensive, and consistent effort by the PRC to acquire the technology and knowhow necessary to confront and disadvantage the United States in the economic and military domains.

As this Subcommittee well knows, the United States has extensive layers of protection. We have a export control regimes for both weapons and dual-use items, we have a system for reviewing foreign direct investment into the United States, we restrict U.S. companies and individuals from doing business with or investing in some of the most egregious Chinese state-owned defense companies, and we have robust legal enforcement mechanisms which have successfully prosecuted individuals breaking our laws. Dedicated and hard-working Americans across Departments and Agencies go to work every day to protect us from this hostile campaign.

Unfortunately, the PRC adapts its strategy and tactics to exploit the gaps and seams in our protective layers more rapidly than we can adapt. Additionally, PRC entities, acting at the direction of the PRC Government, weaponize the U.S. legal system against Americans and our national interests, whereas our companies and individuals lack reciprocal access to PRC courts. To date, we have done relatively little to impose costs on those PRC entities that benefit from this campaign.

This is no longer a problem that can be relegated to trade negotiations, quiet diplomacy with Beijing, or individualized criminal prosecutions. The United States must consider a shift to holding the PRC, and its commercial entities, collectively responsible for their actions. Episodic and uncoordinated responses by individual Departments and Agencies, or from across individual companies and our research enterprise, are insufficient for the challenge.

Recommendations:

---

[4] *China's Trade-Disruptive Economic Model: Communication from the United States to Members of the World Trade Organization*, Office of the United States Trade Representative, July 11, 2018, https://docs.wto.org/dol2fe/Pages/SS/directdoc.aspx?filename=q:/WT/GC/W745.pdf

1. Identify the beneficiaries of IP theft, forced technology transfer, and economic espionage. Rather than focus on just the individuals and commercial entities that directly commit crimes, the United States should focus on determining those who benefit from these activities.

2. Closer coordination across law enforcement, the intelligence community, trade negotiators, the Defense Department, the defense industrial base, and the wider U.S. private sector to understand the tactics and techniques that PRC employs to cause economic and national security harms. The attachment to this testimony includes charts that describe some of the most egregious examples, but we must have a much better understanding and a broader awareness of these tactics across the U.S. Government, our research enterprise, and our business community.

3. Compel corporate and other private sector victims to be transparent about the loss of IP through theft and other forced technology transfer requirements. In too many circumstances, companies consider these losses as the 'cost of doing business' without a regard to the broader implications that these losses have on American economic prosperity, technological leadership, and national security. The whole of these losses is greater than the sum of the parts. In many cases, these private sector actors are transferring enormous risks on to the United States Government and the American people. This lack of transparency into the scope and scale of Beijing's activities prevents the United States from understanding our vulnerabilities and responding appropriately. It is not unreasonable to expect that the private sector be transparent when targeted by a hostile nation-state seeking to undermine American security and prosperity. But without a straightforward legal obligation to be transparent, it is unlikely that companies will volunteer the information.

4. Stop the importation of goods produced with, or which benefits from, stolen IP or economic espionage. Impose financial sanctions, export restrictions, and other economic impairments on these entities and the entities that enable these activities. Until the Chinese Communist Party perceives that the cost of these activities exceeds the gain that they receive, it is unrealistic to expect them to change their behavior. Taking these actions will most certainly have negative repercussions on U.S. companies and the PRC will retaliate. But of course, we are already suffering massive negative repercussions from the PRC's comprehensive campaign that we have largely become numb to.

Chairman Coons, Ranking Member Tillis, and other members of the Committee, thank you again for the opportunity to testify and I look forward to addressing your questions.

Attachment 1

Examples of harms committed by the
People's Republic of China against foreign companies.

Included are five charts detailing economic espionage, intellectual property theft, market manipulation, concealing ownership, and cyberattacks. These examples are based on publicly available information from prosecutions and other U.S. Government documents that reveal the tactics and techniques employed by the PRC Government and the entities it controls.

Chinese Ministry of State Security conducts Combined Cyber and Human Intelligence Campaign to Steal Jet Engine Technology between 2010 and 2015 for the Benefit of Chinese State-owned Enterprises

Ministry of State Security (Beijing)

Jiangsu State Security Bureau (Nanjing)

Cyber Group

Human Intelligence Group

Chai Meng
Section Chief (Cyber)
Jiangsu State Security Bureau

Xu Yanjun
Deputy Director
Jiangsu State Security Bureau

Arrested in Belgium & extradited to the U.S. in Oct 2018

In Custody

Yu Pingan
Malware Developer

"APT26" TURBINE PANDA

(Hacking Group conducting Cyber intrusion and exfiltration campaign on behalf of JSSB in order to benefit AVIC, COMAC and AECC)

Aviation Corporation of China (AVIC)

Commercial Aircraft Corporation of China (COMAC)

Aero Engine Corporation of China (AECC)

CFM = Joint Venture between GE and Safran to make commercial jet engines

SAFRAN

GE Aviation

cfm

In Custody

Tasked to install malware

Tian Xi
Safran Employee

In Custody

Tasked to maintain access

Gu Gen
Safran IT Employee

In Custody

Tasked for insider recruitment

Ji Chaoqun
US Army Reservist

In Custody

Tasked to steal turbine data

Zheng Xiaoqing
GE Employee

APT26 Intrusion and data exfiltration of CFM through Capstone Turbine

Capstone Turbine Corporation

Supplier

Capstone Turbine (Los Angeles-based)

Cyber Intrusion

December 2009, AVIC/COMAC picked CFM International as the engine provider for the C919, COMAC's first commercial jetliner.

AVIC, COMAC, and later AECC, provide JSSB with intelligence requirements, so that an AECC engine can replace CFM's engine.

In January 2010, the Jiangsu State Security Bureau begins their cyber intrusion campaign against Capstone Turbine, a Los Angles-based supplier to GE and CFM, using the JSSB's hacking group, APT26.

Data Exfiltration

Economic Espionage: Syntactic Foam

Trelleborg Offshore, a Houston-based subsidiary of the Swedish engineering firm, Trelleborg, manufacturers syntactic foam, a dual-use material controlled by the U.S. Commerce Department and used in offshore oil drilling as well as U.S. military submarines, aerospace platforms and stealth technology.

China's 12th Five Year Plan (approved March 2011) directed MIIT to develop indigenous components for deep-water buoyancy (1500-3000 meters below sea level). MIIT created a "National Team of Marine Engineering," directed COSTIND/HEU to support and provided funds to Zhejiang Province.

Ministry of Industry and Information Technology (MIIT)

COSTIND — Commission of Science, Technology & Industry for National Defense

KLSTND — Key Laboratory of Science and Technology for National Defense

Zhejiang Province

China's "National Team of Marine Engineering"

CBMF

Taizhou CBM Future New Material Science and Technology Co. Ltd
Established 2012 in Zhejiang, China

CBMF is sole shareholder

Sweden

TRELLEBORG

Houston, Texas

CBMI

CBM International
Established 2014 in Houston

Trelleborg Offshore

Harbin Engineering University (formerly: Harbin PLA Military Engineering Institute)

Graduate of and "Overseas" Professor for HEU Talent Program Member

Shan Shi
President of CBMI
Naturalized US Citizen residing in Houston

- Hired Ex-employees of Trelleborg Offshore
- Conspired with Ex-employees to violate NDAs
- Theft of Trade Secrets

Employed as "senior technical advisor" at CSIC

China National Offshore Oil Company

China Shipbuilding Industry Corporation

CBMF, CBMI, Shan Shi, and five others convicted of trade secret theft in July 2019. Mr. Shi sentenced to 16 months in February 2020

Deliberate Commercial Manipulation and Concealing State Control: Aixtron

PRC State Council

8.5% Control

Bureau of Finance (City of Xiamen)

100% Control

Jinyuan Investment Group

100% Control

Jinyuan Industry Development

97.5% Control

Xiamen Bohao Investment

Purchased Bonds ~ $42 million

Fujian San'An Group (Xiamen, Fujian Province)

San'An Optoelectronics

China Development Bank

Agricultural Bank of China

National Integrated Circuit Fund

35.2% Control

Sino IC Leasing Co., Ltd
(Established 2015)

$500 million

Loan guarantees

49% Control

51% Control

Fujian Grand Chip Investment

Liu Zhendong

100% Control

Grand Chip Investment S.a.r.l. (Luxemburg)

100% Control

Grand Chip Investment GmbH (Germany)

Offer to acquire Aixtron (May 23, 2016)

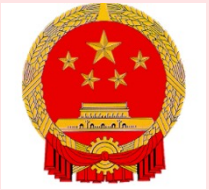
AIXTRON

San'An Group cancels large equipment order from Aixtron causing drop in Aixtron share price (September 12, 2015)

Aixtron was one of two global producers of machines required to produce semiconductors for photovoltaics and LEDs

ICW the German Government, President Obama blocked Grand Chip Investment GmbH on Dec 2, 2016
https://obamawhitehouse.archives.gov/the-press-office/2016/12/02/presidential-order-regarding-proposed-acquisition-controlling-interest

Concealing State Control: Lattice Semiconductor



PRC State Council

100% Control

中国民生银行 CHINA MINSHENG BANK

25% Control

100% Control

中国烟草 CHINA TOBACCO

12% Control

国新科创基金 China Reform Fund

50% Control

100% Control

中国国新控股有限责任公司 CHINA REFORM HOLDINGS CORPORATION LTD.

13% Control

Zhang Yongchong
(CEO of China Reform Holdings)

Sole LP

Legal Counsel

Legal Counsel

American Law Firm

- Registered Canyon Bridge
- Established website
- Leased temporary office in Palo Alto

CANYON BRIDGE

U.S. Incorporated Private Equity Fund
(Founded August 2016)

$1.3 billion acquisition offer
(November 2016)

LATTICE SEMICONDUCTOR

President Trump blocks acquisition based on a CFIUS recommendation in September 2017

Decade-long Cyber Intrusion & Theft Campaigns by the Chinese Ministry of State Security against Companies around the World

Source: U.S. District Court, Southern District of New York, Grand Jury Indictment, December 17, 2018

Engaged in a cyber intrusion campaign for over a decade to steal information and data from at least 45 companies in at least 12 U.S. states.

Engaged in a cyber intrusion campaign to obtain unauthorized access to the computer networks of at least ten Managed Service Providers (MSPs) in order to steal data from the clients of MSPs.

For just one of these MSPs, APT10 compromised and obtained unauthorized access to hundreds of companies in at least 12 countries.

Means and Methods of the "Technology Theft Campaign"

- The MSS used socially engineered "spear phishing" attacks to introduce malware on targeted computers.
- The installed malware included keystroke loggers which were used to steal usernames and passwords as the user typed them.
- The malware then automatically communicated with APT10, allowing MSS to maintain persistent remote access to victim computers over the internet.
- The MSS could then surveil victim computers for data of interest.
- Once identified, the MSS exfiltrated data of interest and had the ability to manipulate or destroy data.

Means and Methods of the "MSP Theft Campaign"

- The MSS used many of the same techniques from the "Technology Theft Campaign" to gain access to the computer networks of Managed Service Providers (MSPs).
- APT10 then installed customized malware (PlugX, RedLeaves, QuasarRAT) to defeat antivirus protection and steal user credentials in order to steal administrative credentials from the MSP.
- Once APT10 had stolen admin credentials for the MSP, APT10 initiated Remote Desktop Protocol (RDP) connections to the networks of the MSP's clients.
- This allowed the MSS to compromise and remove data from the computers of the MSP's clients without installing malware.

Countries Targeted

- Brazil
- Canada
- Finland
- France
- Germany
- India
- Japan
- Sweden
- Switzerland
- United Arab Emirates
- United Kingdom
- United States

Industry Sectors Targeted

- Banking and Finance
- Telecommunications Equipment Manufacturing
- Consumer Electronics Manufacturing
- Medical Equipment Manufacturing
- Packaging
- Advanced Manufacturing
- Aviation and Aerospace Manufacturing
- Consulting
- Healthcare
- Biotechnology
- Auto Manufacturing
- Oil and Gas Exploration
- Mining
- Maritime Technology