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