CHINA'S CYBER CAPABILITIES: WARFARE, ESPIONAGE, AND IMPLICATIONS FOR THE UNITED STATES

HEARING

BEFORE THE

U.S.-CHINA ECONOMIC AND SECURITY REVIEW COMMISSION

ONE HUNDRED SEVENTEENTH CONGRESS
SECOND SESSION

THURSDAY, FEBRUARY 17, 2022

Printed for use of the
United States-China Economic and Security Review Commission
Available via the World Wide Web: www.uscc.gov

UNITED STATES-CHINA ECONOMIC AND SECURITY REVIEW COMMISSION

WASHINGTON: 2022

U.S.-CHINA ECONOMIC AND SECURITY REVIEW COMMISSION

ALEX WONG, *CHAIRMAN*
KIMBERLY T. GLAS, *VICE CHAIR*

Commissioners:
CAROLYN BARTHOLOMEW
BOB BOROCHOFF
ROBIN CLEVELAND
JEFFREY FIEDLER
AARON FRIEDBERG
RANDALL SCHRIVER
DEREK SCISSORS
MICHAEL R. WESSEL

The Commission was created on October 30, 2000 by the Floyd D. Spence National Defense Authorization Act of 2001, Pub. L. No. 106–398 (codified at 22 U.S.C. § 7002), as amended by: The Treasury and General Government Appropriations Act, 2002, Pub. L. No. 107–67 (Nov. 12, 2001) (regarding employment status of staff and changing annual report due date from March to June); The Consolidated Appropriations Resolution, 2003, Pub. L. No. 108–7 (Feb. 20, 2003) (regarding Commission name change, terms of Commissioners, and responsibilities of the Commission); The Science, State, Justice, Commerce, and Related Agencies Appropriations Act, 2006, Pub. L. No. 109–108 (Nov. 22, 2005) (regarding responsibilities of the Commission and applicability of FACA); The Consolidated Appropriations Act, 2008, Pub. L. No. 110–161 (Dec. 26, 2007) (regarding submission of accounting reports; printing and binding; compensation for the executive director; changing annual report due date from June to December; and travel by members of the Commission and its staff); The Carl Levin and Howard P. ''Buck'' McKeon National Defense Authorization Act for Fiscal Year 2015, Pub. L. No. 113–291 (Dec. 19, 2014) (regarding responsibilities of the Commission).

The Commission's full charter and statutory mandate are available online at: https://www.uscc.gov/charter.

CONTENTS

THURSDAY, FEBRUARY 17, 2022

CHINA'S CYBER CAPABILITIES: WARFARE, ESPIONAGE, AND IMPLICATIONS FOR THE UNITED STATES

Panel I: China's Perspective on and Capabilities for Cyberwarfare

Panel II: China's Goals and Capabilities for Cyberespionage

Panel III: U.S. Responses to the China Cyber Challenge

CHINA'S CYBER CAPABILITIES: WARFARE, ESPIONAGE, AND IMPLICATIONS FOR THE UNITED STATES

THURSDAY, FEBRUARY 17, 2022

U.S.-CHINA ECONOMIC AND SECURITY REVIEW COMMISSION

Washington, D.C.

The Commission met in Room 430 of Dirksen Senate Office Building, Washington, DC and via videoconference at 9:00 a.m., Chairman Alex Wong and Commissioner Carolyn Bartholomew (Hearing Co-Chairs) presiding.

OPENING STATEMENT OF CHAIRMAN ALEX WONG HEARING CO-CHAIR

CHAIRMAN WONG: Good morning. Welcome to the second hearing of the U.S.-China Economic and Security Review Commission's 2022 annual report cycle.

I want to start by saying happy birthday, a very happy birthday to our fellow Commissioner, Bob Borochoff. He is choosing to spend his birthday like we all aspire to, having a deep discussion about China's cyber capabilities.

But thank you all for joining us; some people tuning in as well and foremost our witnesses today who put a lot of time and effort and expertise into their testimony.

It's been a decade since this Commission has squarely addressed in a hearing the status of China's cyber capabilities. A decade is a long time in normal human experience, but it's a lifetime when talking about digital technology. In that time the digital world has rapidly evolved and the dependence of our societies, our economies, and our militaries on computing power and modern telecommunications has broadened and deepened. This makes it every more important for this Commission to examine China's cyber capabilities today as they apply to the military and intelligence spheres.

China has invested heavily in the cyber realm in the past 10 years. How does China plan to bring its cyber capabilities to bear in a crisis or conflict? How does this change the landscape of deterrence and of a possible conflict involving China? How does China's growing cyberespionage capabilities affect U.S. counterintelligence activities and efforts by private U.S. companies to protect their intellectual property? And as the United States continues to work with governmental and non-governmental partners to develop norms and conventions in the digital space how does the world account for China's conduct and what may be China's fundamental disagreement over whether the nature of the internet is to be open or closed?

I look forward to today's testimonies coming from both academics steeped in the study of the cyber realm and experts who have engaged in the day-to-day challenge of securing U.S. networks. There is much to discuss and much to consider for recommendations to the U.S. Congress.

I'll now turn the floor over to my colleague and co-chair for this hearing, Commissioner Carolyn Bartholomew.

PREPARED STATEMENT OF COMMISSIONER ALEX WONG
HEARING CO-CHAIR

Hearing on “China’s Cyber Capabilities: Warfare, Espionage, and Implications for the United States”

Opening Statement of Chairman Alex Wong

February 17, 2022

Washington, DC

Good morning, and welcome to the second hearing of the U.S.-China Economic and Security Review Commission’s 2022 Annual Report cycle. Thank you all for joining us, and thank you especially to our witnesses for the time and effort they have put into their testimonies.

It’s been a decade since this Commission has squarely addressed in a hearing the status of China’s cyber capabilities. A decade is a long period in normal human experience. But it’s a lifetime when talking about digital technology. In that time, the digital world has rapidly evolved, and the dependence of our societies, our economies, and our militaries on computing power and modern telecommunications has broadened and deepened.

This makes it ever more important for this Commission to examine China’s cyber capabilities today as they apply to the military and intelligence spheres. China has invested heavily in the cyber realm in the past ten years. How does China plan to bring its cyber capabilities to bear in a crisis or conflict? How does this change the landscape of deterrence and of a possible conflict involving China? How does China’s growing cyber espionage capabilities affect U.S. counterintelligence activities and efforts by private U.S. companies to protect their intellectual property? And as the United States continues to work with governmental and non-governmental partners to develop norms and conventions in the digital space, how does the world account for China’s conduct, and what may be China’s fundamental disagreement over whether the nature of the Internet is to be open or closed?

I look forward to today’s testimonies, coming from both academics steeped in the study of the cyber realm and experts who have engaged in the day-to-day challenge of securing U.S. networks. There is much to discuss, and much to consider for recommendations to the U.S. Congress.

I will now turn the floor over to my colleague and co-chair for this hearing, Commissioner Carolyn Bartholomew.

OPENING STATEMENT OF COMMISSIONER CAROLYN BARTHOLOMEW HEARING CO-CHAIR

COMMISSIONER BARTHOLOMEW: Thank you very much, Chairman Wong.

Good morning, everyone. Thank you for joining us today. Thank you particularly to our witnesses for the knowledge and expertise they're sharing with us. We look forward to learning from them.

In addition to cyberwarfare this hearing will explore China's motivations and capabilities for cyberespionage. In contract to cyberwarfare which aims to infiltrate and compromise an adversary's computer networks, cyberespionage is a clandestine operation to access and steal classified or otherwise sensitive data for political or military purposes or to illicitly acquire intellectual property to gain a competitive or economic advantage over an adversary.

In 2005 this Commission started raising concern about China's cyber activities. It was becoming clear then that China's theft of intellectual property was moving from counterfeiting CDs and other physical goods to online theft of trade secrets. China's tradecraft at that time was ham-handed and relatively unsophisticated. Since then there has been an alarming rise in the frequency and the sophistication of China's state-sponsored and state-affiliated cyberespionage activity as well as its targeting.

China's cyber actors have deliberately and aggressively pursued targets across a spectrum of industries including technology, defense, energy, health care, education, and other key sectors in pursuit of trade secrets and of sensitive information. One of the most recent and egregious examples, the Microsoft Exchange hack in July 2021, compromised email servers and consequently the sensitive information of tens of thousands of organizations in the United States and around the world.

In the health care sector, Chinese cyberespionage campaigns have targeted hospitals and research institutions for data that could confer competitive advantages in science and technology. In May 2020, the FBI disclosed that it was investigating the targeting and compromise of U.S. organizations conducting COVID-19-related research by PRC-affiliated cyber actors and non-traditional collectors. Reported breaches of health care insurer Anthem, Inc., of Equifax, Marriott, and perhaps most worryingly, the Office of Personnel Management, all demonstrate China's vast campaign to target and acquire Americans' private data through cyberespionage.

The threat of China's cyberespionage activities is not only a U.S. challenge, but also a global one which underscores the need for collective action and security cooperation with U.S. partners and allies. In July 2021, the Biden Administration informed that the United States is working with an unprecedented group of allies and partners including the European Union, the U.K., and NATO to address the threat of China's irresponsible and de-stabilizing behavior in cyberspace.

Today's witnesses will provide insight into China's intent and capabilities for cyberespionage and critically what the United States and partners can do to address this challenge effectively.

Finally, before we begin I'd like to remind you all that the testimonies and transcript for today's hearing will be posted on our website, which is uscc.gov. Also please mark your calendars for the Commission's upcoming hearing on China's energy policies and practices, which will be on March 17th.

I will now turn the floor back over to Chairman Wong to introduce your first panel.

PREPARED STATEMENT OF COMMISSIONER CAROLYN BARTHOLOMEW
HEARING CO-CHAIR

Back to the Table of Contents

Hearing on "China's Cyber Capabilities: Warfare, Espionage, and Implications for the United States"

Opening Statement of Commissioner Carolyn Bartholomew

February 17, 2022

Washington, DC

Good morning, everyone. Thank you for joining us today. Thank you, particularly, to our witnesses for the knowledge and expertise they are sharing with us. We look forward to learning from them.

In addition to cyberwarfare, this hearing will explore China's motivations and capabilities for cyberespionage. In contrast to cyberwarfare, which aims to infiltrate and compromise an adversary's computer networks, cyberespionage is a clandestine operation to access and steal classified or otherwise sensitive data for political or military purposes, or to illicitly acquire intellectual property to gain a competitive or economic advantage over an adversary.

In 2005, this Commission started raising concern about China's cyber activities. It was becoming clear that China's theft of intellectual property was moving from counterfeiting CDs and other physical goods to online theft of trade secrets. China's tradecraft at that time was ham-handed and relatively unsophisticated. Since then, there has been an alarming rise in the frequency and the sophistication of China's state-sponsored and state-affiliated cyberespionage activity, as well as its targeting.

China's cyber actors have deliberately and aggressively pursued targets across a spectrum of industries, including technology, defense, energy, healthcare, education, and other key sectors in pursuit of trade secrets and of sensitive information. One of the most recent and egregious, the Microsoft Exchange hack in July 2021, compromised email servers and consequently the sensitive information of tens thousands of organizations in the United States and around the world. In the healthcare sector, Chinese cyberespionage campaigns have targeted hospitals and research institutions for data that could confer competitive advantages in science and technology. In May 2020, the FBI disclosed that it was investigating "the targeting and compromise of U.S. organizations conducting COVID-19-related research by PRC-affiliated cyber actors and non-traditional collectors." Reported breaches of healthcare insurer Anthem Inc., Equifax, Marriott, and, perhaps most worryingly, the Office of Personnel Management, all demonstrate China's vast campaign to target and acquire Americans' private data through cyberespionage.

The threat of China's cyberespionage activities is not only a U.S. challenge, but also a global one which underscores the need for collective action and security cooperation with U.S. partners and allies. In July 2021, the Biden Administration affirmed that the United States is working with an "unprecedented group of allies and partners – including the European Union, the United Kingdom, and NATO" to address the threat of China's "irresponsible and destabilizing behavior in cyberspace."

Today's witnesses will provide insight into China's intent and capabilities for cyber espionage, and critically what the United States and partners can do to address this challenge effectively.

Finally, before we begin I would like to remind you all that the testimonies and transcript from today's hearing will be posted on our website, which is www.uscc.gov. Also, please mark your calendars for the Commission's upcoming hearing on China's energy policies and practices, which will be on March 17. I will now turn the floor back over to Chairman Wong to introduce our first panel.

PANEL I INTRODUCTION BY CHAIRMAN ALEX WONG

CHAIRMAN WONG: Thank you, Carolyn.

Our first panel has a series of wonderful experts here to talk about China's perspective on its capabilities for cyberwarfare. First we'll hear from Winnona DeSombre with the Atlantic Council and Harvard's Belfer Center. Second we'll hear from Dean Cheng, who is here in D.C. with the Heritage Foundation. And third we will hear from John Chen, with Exovera's Center for Intelligence and Research Analysis, as well as the Atlantic Council.

Ms. DeSombre?

OPENING STATEMENT OF WINNONA DESOMBRE, NON-RESIDENT FELLOW, ATLANTIC COUNCIL, FELLOW, BELFER CENTER, HARVARD UNIVERSITY

MS. DeSOMBRE: Thank you, Chairman Wong.

Chairman Wong, Commissioner Bartholomew, other distinguished members of the Commission, it's an honor to be testifying before you today.

I've been asked to brief you on China's efforts to become a cyber superpower, how China and the U.S. compare in metrics of cyber power, and China's offensive cyber capabilities in contrast to those of the United States.

I'll discuss five main points and offer four recommendations to the Commission.

Point 1. China is a major peer adversary in cyberspace. Its offensive cyber capabilities rival or exceed those of the United States. And I'm happy to go into open source metrics of this such as vulnerability research during the Q&A due to lack of time. But the U.S. Intelligence Community has openly stated that China possesses substantial cyber-attack capabilities and can launch cyber-attacks that at a minimum cause localized temporary disruptions to critical infrastructure.

On the defensive side, China's cyber defenses can detect some U.S. operations and in some cases turn our own tools against us. A Chinese Ministry of State Security contractor was found using NSA hacking tools a full year before these tools were leaked to the public which suggests the contractor observed these tools being used against Chinese targets and was able to recreate it based off of observations and analysis alone.

Point 2. In addition to highly robust offensive capabilities China has built asymmetric capabilities that the U.S. is constrained from developing by international or domestic law. The U.S. prioritizes operational tradecraft in cyberspace, does not conduct economic espionage, and has clear authorities on who can or cannot conduct military operations, especially in cyberspace.

The Chinese government on the other hand developed cyber programs that steal American IP alongside more traditional operations and does not care whether they're caught. This apathy enables the regime to conduct far more frequent operations, which while are easy to detect, are far more effective and successful than one would expect.

So most recently Commissioner Bartholomew did mention the Microsoft Exchange issue. When China's use of this software flaw was outed publicly by the White House, China did not stop their operations. In fact, they sped up their operational tempo trying to compromise as many U.S. companies and computers as possible before these corporations were able to protect themselves.

Point 3. Beyond offense/defense dynamics, Xi Jinping has dramatically escalated Chinese rhetoric and capabilities around cyber power. He's modernized his military for technological power projection and has shifted propaganda priorities to pursue global information dominance. This shift has already been found and seen by U.S. cybersecurity experts as well. Information operations targeting China's domestic issues originally have been shifted strategically abroad over the last two years to sow discord and project power.

Xi Jinping is also fundamentally changing the nature of the cyberspace in which we operate, the world’s cyber infrastructure, by pursuing dominance within Chinese private sector in the international market and simultaneously weaning the Chinese market off of Western technology.

Point 4. While China and the United States both suffer from a cyber personnel shortage, China's multi-stakeholder approach to personnel development, its relationships with corporate and academic institutions through military-civil fusion, and its emphasis on developing asymmetric capabilities will enable it to overcome these issues short term.

The U.S. by contrast is not nearly as well-equipped. We're looking to fill one-third as many jobs, but are held back by clearance backlogs and other policies that discourage engineers from entering government service as well as visa processing issues that prevent engineering talent from coming to the United States at all.

And finally, Point 5. Based on industry observations, the U.S. does not currently have adequate cyber defenses, personnel, supply chain security, or international technical and standards leadership to rival China long term in cyberspace. On top of this given how secretive cyber is as a domain, China's capabilities likely exceed the findings that I've compiled here.

My recommendations to Congress therefore to ensure adequate U.S. capabilities in response to China's superpower goals are as follows: (1) Bolstering U.S. cyber defenses; (2) Appropriating funds to secure the global supply chain; (3) Diversifying the cybersecurity jobs pipeline; and (4) Working with allies to support the U.S. values in the information domain. I'll go into each one.

So for Recommendation 1, if breaking into U.S. systems were more difficult, China would have to expend many more resources ensuring its cyber capabilities were up to the task. Creating federal mandatory breach notification laws, threat information sharing for critical infrastructure sectors to the government, as well as expanding patching requirements for federal contractors will be excellent steps in the right direction.

For Recommendation 2, in order to secure the global supply chain Congress must appropriate additional funds to semiconductor foundries in the CHIPS Act, as well as allocate funding for research into federal software bills of materials. Directing research into detection and interception of malicious software in the open source before it becomes a problem is key. And language in the current America COMPETES Act going through Congress right now can be altered to accomplish this goal.

For Recommendation 3, To keep up with China's rapidly growing cyber personnel Congress should reform the security clearance process, loosen restrictions on contractors to hire foreign talent, expand the H1-B visa quota for cybersecurity talent, fund cybersecurity education at levels similar to the National Defense Education Act during the space race, and expand the U.S. Digital Service tour of duty model to public cyber defense jobs.

And finally, for Recommendation 4, Congress should encourage U.S. and allied leadership in international standards bodies like the ITU which will continue to show support for a free and open internet. In addition, Congress can move beyond naming and shaming to impose costs on these Chinese cyber threat groups by asking the Department of Commerce or Treasury to add Chinese institutions connected to cyber operations to the entities list and sanctions list, respectively. Note that this does have some substantial risks and has to be paired with clear guidelines on how Chinese institutions can get themselves removed from the list to encourage more responsible behavior.

Thank you again, Commissioners, for inviting me to testify. I hope that these five points and four recommendations are a good framework for the rest of today and I look forward to your questions and the remarks of my other panelists.

PREPARED STATEMENT OF WINNONA DESOMBRE, NON-RESIDENT FELLOW, ATLANTIC COUNCIL, FELLOW, BELFER CENTER, HARVARD UNIVERSITY

Back to the Table of Contents

February 17, 2022

Winnona DeSombre

Research Fellow - Atlantic Council & Harvard Belfer Center

Testimony before the U.S.-China Economic and Security Review Commission

Hearing on “China’s Cyber Capabilities: Warfare, Espionage, and Implications for the United States”

….

Executive Summary

Commissioner Wong, Commissioner Glas, other distinguished members of the Commission, it is an honor to testify before you today on China's cyber capabilities. I have been asked to brief you on Chinese leaders' efforts to become a "cyber superpower", how China and the U.S. compare in metrics of cyber power, and China's offensive cyber capabilities in contrast to the United States.

I have **5 main points** to make in this testimony:

1. China is a major peer adversary in cyberspace. Its offensive cyber capabilities rival the United States', its operations demonstrate clear development of asymmetric capabilities that enable it to achieve strategic goals, and its cyber defensive capabilities are robust.

2. Xi Jinping has dramatically escalated Chinese rhetoric and capabilities around cyber power. He has modernized his military, shifted propaganda priorities to pursue global information dominance, and is remaking the international supply chain with Chinese companies.

3. China has asymmetric capabilities that the U.S. is currently constrained from developing via international or domestic law, on top of their already impressive arsenal, for both economic espionage and national security use. They use their private sector for cyber operations, and blatantly disregard any efforts to name and shame their behavior.

4. While China and the United States both suffer from a cyber personnel shortage, China's enablement of private sector offensive security contractors and academic institutions, and emphasis on asymmetric capabilities, will allow it to grow capabilities despite these issues.

5. The United States does not currently have adequate cyber defenses, personnel, supply chain security, or international technical and standards leadership to rival China long-term.

To ensure adequate capabilities in response to China's cyber superpower goals, Congress must:

- **Bolster US cyber defenses** by creating federal mandatory breach notification laws, threat information sharing requirements and patching requirements for critical infrastructure;
- **Appropriate funds to secure the global supply chain**, particularly towards semiconductor foundries and open source detection and response efforts in the America COMPETES act;
- **Diversify the US cyber security jobs pipeline** by loosening foreign talent restrictions, increasing cyber visa quotas, doubling education budgets, and expanding the U.S. Digital Service "tour of duty" model to public sector cyber defense jobs; and
- **Work with allies to support U.S. values in the information domain** by encouraging US and allied leadership in the ITU and by asking the Department of Commerce to add Chinese institutions connected to cyber operations to the entities list.

China and the Importance of Cyberspace

How do Chinese leaders view the importance of cyberspace?

The Chinese Communist Party (CCP) wants China to become a “cyber superpower”[1], and is well on its way to achieving that goal. CCP leaders have a clear understanding of the domain and how to use cyber power to achieve existing strategic goals – particularly goals within domestic surveillance, defense, information dominance, economic growth, technical standards, and especially offensive capabilities.[2]

Cyber is a prioritized domain in China’s rhetoric, regulation, and action. Becoming a cyber superpower or cyber powerhouse is explicitly stated within their newest Five Year Plan - encompassing plans for economic expansion, national security, talent training, international trade, and more[3]. This comprehensive cyber strategy has already been incorporated into regulatory processes at ministry[4], party[5], and provincial[6] levels of government.

The CCP believes that the U.S. is more vulnerable in cyberspace, and that they can develop asymmetric capabilities that would give them a distinct wartime advantage.[7] We observe this in their mismatch between rhetoric and action – for instance, China espouses ideals of cyber sovereignty[8] while abusing the free and open Internet to sow disinformation in the United States.[9]

Xi Jinping and China’s Preparations for Cyberwarfare

Xi Jinping has dramatically escalated Chinese rhetoric around cyber security and warfare, stating openly that “without cyber security, there is no national security”.[10] Prior Chinese leaders focused largely on domestic matters: military IT[11], domestic cyber sovereignty[12], and control over domestic virtual society[13]. By contrast, **Xi has pushed China to reach for cyber power** by developing a modernized military, shifting propaganda priorities to global information dominance, and remaking the international supply chain with Chinese companies.

Xi Jinping has completely reorganized the People’s Liberation Army, downsizing the land-based army it has relied on for decades to create a Strategic Support Force that focuses on cyber, space, and electronic warfare.[14] This reorganization has accelerated a shift in military posture from land-based territorial protection to extended power projection[15], with joint forces and technology as key enablers. To compliment the new joint force, Xi has advanced a strategy of military-civil fusion (MCF), restructuring Chinese science and technology enterprise to simultaneously innovate for both economic and military development.[16] These two strategies marry well with Xi’s push past “informationization” to “intelligentization”[17] of the PLA, which will integrate artificial intelligence and human computer interaction into military decision making.[18]

Xi Jinping has also stressed the importance of "discourse power"[19] and information dominance[20] in cyberspace. This is a marked shift of priorities from domestic censorship to global information control, and this shift has already been noted by U.S. cybersecurity experts: information operations stemming from China targeting domestic issues have been strategically redirected towards the West over the last two years to sow discord and project power abroad.[21]

Furthermore, Xi Jinping is fundamentally changing the world's cyber infrastructure by pursuing Chinese private sector dominance in international markets, while weaning China off of Western technology. The "Made in China 2025"[22] plan is aimed at making China the key player in the high-tech global supply chain - rapidly shifting Chinese technology off of Taiwanese and U.S. manufactured chips[23], while the Belt and Road Initiative ensures that Chinese private sector technology firms are involved in key infrastructure deals[24] throughout Western Asia, Africa, the Middle East, and Europe.

China, the United States, and Cyberwarfare

US policy papers often refer to China as a near-peer competitor in cyberspace. But make no mistake: **China is a major peer adversary in cyberspace.** As the DOD has openly stated, China is "the only country that can pose a systemic challenge to the United States in the sense of challenging us, economically, technologically, politically and militarily".[25] This is especially clear in the cyber domain: The country's offensive cyber capabilities rival or exceed that of the United States, and its cyber defensive capabilities are able to detect many U.S. operations – in some cases turning our own tools against us. On top of this, China also uses asymmetric capabilities that the United States is constrained against using by either international or domestic law, achieving large tactical advantages.

Chinese Offensive Cyber Capabilities

While China has not yet been attributed to a major disruptive cyber attack, the U.S. intelligence community has openly stated that China "possesses substantial cyber-attack capabilities …[and] can launch cyber attacks that, at a minimum, can cause localized, temporary disruptions to critical infrastructure within the United States".[26] Some capabilities are readily observable in the open source: for example, one critical measure of offensive cyber capabilities is a country's ability to find and exploit software vulnerabilities. A software vulnerability is a security flaw or weakness in software that could be exploited by an attacker. They are crucial tools for cyber operations, especially if the flaw has yet to be fixed in most software products, or if the vendor is unaware of the vulnerability in their product at all.

Hackers in China find vulnerabilities in U.S. software at an alarming rate, and China actively exploits these vulnerabilities in its cyber operations before they can be fixed. Every year, China holds a hacking competition, the Tianfu Cup, for their top hackers to find vulnerabilities. However, unlike equivalent competitions elsewhere, which commonly disclose the flaws directly to impacted companies, **flaws found at Chinese hacking competitions are given to the Chinese government before companies even hear about them**[27]. A flaw in Apple software reported at Tianfu Cup[28] in 2018 was used in Chinese cyber espionage campaigns for two months before the vulnerability was discovered and fixed. How many vulnerabilities does China find compared to the international community? In 2021, Tianfu Cup reported 30 successful demonstrations exploiting new vulnerabilities in US software products, including Windows 10, Apple iOS, Safari, and Chrome.[29] This was 40% more than the number of successful demonstrations at Pwn2Own (an equivalent international competition with U.S. turnout) that same year.[30]

Outside of competitions, **Chinese companies are punished when they disclose vulnerabilities to vendors without first consulting the Chinese government**: when an engineer at Alibaba found a vulnerability in Log4j, he reported it directly to Apache (the U.S. vendor responsible) instead of to the Chinese government. This was one of the most serious vulnerabilities last year, impacting millions of websites and applications.[31] Instead of rewarding the engineer, the Chinese government suspended its information-sharing partnership with Alibaba Cloud for six months and cited improper disclosure of Log4j as the primary reason.[32]

Control over the information environment is also a critical measure of wartime cyber capability – indeed, the Allied Powers used various forms of propaganda[33] and disinformation[34] during World War II against the Nazi regime. **China has used the modern Internet ecosystem to successfully craft pro-China narratives abroad and prevent anti-Chinese messages from being propagated**. Its propaganda apparatus is attempting to produce targeted content that promotes pro-China narratives in the West, specifically for "international youths"[35], and hired a New Jersey consulting firm to spread pro-Beijing content for the 2022 Olympics via online influencers.[36] Tiktok, a popular Chinese social media app, actively censors content unfavorable to Beijing.[37] China also has a sprawling covert propaganda network conducting disinformation operations on social media, which has begun to develop measurable international reach.[38]

China's Asymmetric Capabilities: Playing a Different Game in Cyberspace

In addition to highly robust offensive cyber capabilities, **China has built asymmetric capabilities that the United States is constrained against developing by international or domestic law.** The United States prioritizes operational tradecraft in cyber operations[39], does not conduct economic espionage, and has clear authorities on who can and cannot conduct military operations in cyberspace.[40] The Chinese government develops cyber programs that do not care whether they are found and attributed, continues to steal American intellectual property in cyberspace alongside more traditional operations, and directly hires corporations to conduct cyber operations on behalf of the regime.

Chinese cyber units continue to conduct economic espionage against companies in the U.S. and globally. Despite the 2015 US-China Cyber agreement in which both countries agreed to refrain from stealing intellectual property[41], China has been flagrantly violating the agreement over the last eight years.[42] While the 2015 agreement initially resulted in intellectual property being stolen at a slower observable rate[43], this is no longer the case.

China no longer cares about being named and shamed in cyberspace. **This apathy enables the regime to conduct far more frequent cyber operations[44] that, while easy to detect, are still wildly successful**. By altering malware readily found online[45] or by using vulnerabilities with known fixes since 2017[46], China demonstrates that it does not care enough about getting caught to spend the time and money required to develop more stealthy capabilities across all their cyber programs.[47] In fact, they make themselves easy to find - some cyber operations attributed to China have been found using tools known by the cyber security industry as belonging to the PLA since 2013.[48] However, these basic operations still successfully penetrate U.S. organizations for both economic espionage and intelligence gathering purposes. **In more recent cases, China has sped up their operational tempo after their cyber operation was discovered.** When the White House publicly announced flaws[49] in Microsoft Exchange used by Chinese hackers, the number of observed attacks from China using the vulnerability skyrocketed – suggesting that China ramped up the campaign to compromise as many computers as possible before U.S. companies could protect themselves.[50]

Finally, **China's civilian commercial entities are heavily involved in Chinese cyber operations**. The CCP's "military-civil fusion" strategy has enabled large numbers of civilian companies like Baidu and Alibaba[51] to participate in classified military research and development.[52] In addition, Chinese contractors have directly engaged in cyber operations for the Chinese government.[53] Chinese telecom and infrastructure companies like Huawei have been implicated in Chinese cyber espionage campaigns in the past.[54] This is particularly alarming given that these same companies are key elements in China's Belt and Road Initiative abroad, and previous infrastructure projects that involved Huawei – like the 2012 African Union building project – were found sending signals back to China.[55]

China's Defensive Capabilities – Large Scale and Able to Detect Western Operations

China also has well established and **large-scale defensive capabilities that are able to detect some Western cyber operations**. It has a cyber security industry of power players providing the full gamut of cyber security products and services[56], and the industry is growing larger. On top of putting in place extensive cyber security regulations for Chinese businesses[57], the Ministry of

Industry and Information Technology (MIIT) also plans on boosting development of and demand for cyber security products, expecting the sector to be worth more than $38.6 billion by 2023.[58]

Two Chinese cyber security firms in particular: Antiy Labs[59] and Qihoo360[60], have openly published analyses of NSA and CIA cyber operations. While these reports are heavily bolstered by the Shadowbrokers and Vault7 leaks respectively and do not provide enough information for independent researchers to validate their claims, Antiy and Qihoo are two of the oldest antivirus companies in China and therefore likely have the data visibility that would make these claims credible. **Chinese MSS contractors have also been able to observe and recreate U.S. made cyberweapons**: one contractor was found using NSA hacking tools a full year before the tools were made public via the Shadowbrokers leak, suggesting that the contractor observed the hacking tools being used against Chinese targets and recreated the tool from those observations.[61]

U.S. Advantages over China in Cyberspace

The U.S. still has power over China in cyberspace. The United States has first mover advantage – U.S. companies own vast swaths of international fiber optic cable, provide some of the world's largest online platforms and produce some of the most widely used technological devices. The United States has a global network of alliances with intelligence partnerships spanning the globe, many of which are in China's sphere of influence. Most importantly, the United States has some of the world's top technical talent and most innovative technology companies.

The CCP knows all of this – and is actively attempting to chip away at those advantages. The Chinese government has pushed policies of technological self-sufficiency to reduce reliance on U.S. technology.[62] This stems from a clear party leadership understanding that their reliance on U.S.-produced operating systems and microprocessors is an urgent security vulnerability. In addition, China actively pushes its own technology companies to expand internationally and leapfrog over their U.S. counterparts. Chinese officials have also squeezed U.S. companies and allies – technology giants like Apple have been pressured use Chinese hardware and invest directly into the country[63], and U.S. intelligence partners have been pressured economically for security and trade concessions.[64]

On top of all this, China is inherently changing the playing field on which we currently operate in cyberspace, through pursuing leadership positions in international technical standards bodies.[65]` Changing the technical standards for how the Internet operates would nullify the United States' first mover advantage over China entirely over time.

China and the U.S. vis-a-vis Cyber Personnel

One global issue impacting both China and the United States is the global shortage of talented cybersecurity personnel. While China and the United States both suffer from a personnel shortage, **China's multi-stakeholder approach to personnel development, its relationship with corporate and academic institutions, and its emphasis on developing asymmetric capabilities will enable it to overcome these issues** in the short term, while developing a formidable force long term.

The CCP is well aware of its shortage of cyber security professionals - estimating the deficit at 1.4 million jobs.[66] This is three times as much as the current deficit estimate in North America.[67] **Considering how effective current Chinese cyber capabilities are despite this deficit, China will likely overcome potential issues stemming from this shortage**.

China's cyber talent is currently bolstered by linking research universities to military and intelligence organizations via military-civil fusion: at least 15 Chinese civilian universities have been implicated in cyberattacks, illegal exports or espionage thus far, and over 150 are able to contribute to classified weapons and defense projects/[68] In addition, China has purchased surveillance tools[69] (and potentially vulnerabilities[70]) from foreign contractors to bolster its capabilities domestically. China's MIIT has also artificially boosted demand of cyber security products by mandating that key industries devote 10% of their IT budget to cyber security within the next two years.[71]

The United States, by contrast, is not nearly as well equipped. The United States is also looking to fill its shortage of approximately 300-400 thousand cyber security jobs, but it is held back by policies that discourage engineers from coming into government service. These include: lack of upward mobility, noncompetitive pay, and long security clearance processing backlogs.

To make matters worse, visa processing issues discourage engineering talent from coming to the US entirely, preventing U.S. institutions from taking advantage of such talent. As a result, the United States has a smaller personnel gap, but far more difficulty in filling it - and it may only get worse: if left unaddressed, the labor shortage is expected to grow by at least 20% every year.[72]

Comparative Indexes of CCP Cyberpower - a Red Herring

Do not be fooled by indexes that say otherwise - **in cyberspace, China is a major peer player.** Indexes that attempt to measure Chinese and U.S. cyber power suffer from **three pitfalls**: choosing irrelevant or incorrect proxies, believing the fallacy of sophistication, and using overly Western measurements of power.

Finding proxies for cyber power is incredibly difficult – this is especially the case for offensive cyber capabilities, which are often deliberately hidden away from the prying eyes of researchers. Thus, finding relevant proxies requires deep knowledge of a country's cyber governance and its cybersecurity industry. Due to lack of industry experience, researchers creating cyber power indexes may use misleading proxy data for China's robust cyber capabilities. For example, the IISS cyber power index used semiconductor sale[73] as a proxy for cyber empowerment and dependence - when semiconductor *manufacturing*[74] is far more important for supply chain security.[75]

Researchers also fall into the fallacy of sophistication when measuring cyber attacks – comparing the Stuxnet worm: an incredibly complex piece of software designed to target Iranian nuclear centrifuges allegedly created by the U.S. and Israel[76], to lower-level attacks perpetrated by the Chinese government. Given how vulnerable the U.S. already is in cyber defense, as well as the well-worn arsenal of online attacks available to our adversaries that barely require technical skills – such as disinformation, phishing scams, or dropping USBs in a parking lot[77], this is a false dichotomy. Whether a cyber operation is sophisticated or artful is far less important than whether a cyber operation achieves the intended goal.

Fundamentally, using Western metrics of cyber power to measure China's cyber power misses the point that China's goals in cyberspace are inherently different from Western goals. As Western powers talk about their cyber capabilities with increasing openness, some indexes[78] may decide that China's lack of open offensive cyber doctrine is the same as not having an offensive cyber doctrine. This is an extreme assumption considering the People's Liberation Army (PLA) reorganization, well-honed Ministry of State Security (MSS) cyber operations structures, and its well-developed offensive security industry exports. Indexes that look for openly available strategy documents and international partnership agreements may be missing Chinese goals entirely.

Recommendations for Congressional Action

Based on current open source observations, the United States does not currently have adequate cyber defenses, personnel, supply chain security, or international technical and standards leadership to rival China long-term in cyberspace. **In addition, given how secretive cyber is as a domain, China's capabilities likely exceed the findings compiled here**. To ensure adequate U.S. capabilities in response to China's cyber superpower goals, Congress must:

1) Bolster US Cyber Defenses

If breaking into United States systems were more difficult, China would have to expend many more resources ensuring its cyber capabilities were up to the task. Creating federal mandatory breach notification laws pertaining to U.S. critical infrastructure, mandating threat information sharing for critical infrastructure sectors to the government, and expanding patching requirements[79] to federal contractors will be excellent steps in the right direction.

2) Appropriate Funds to Secure the Supply Chain

In order to ensure security and integrity of the global supply chain, Congress must appropriate additional funds to semiconductor foundries in the CHIPS act[80], as well as allocate funding for research into federal software bill of materials and other key areas where Chinese cyberwarfare may impact the U.S. economy. Directing research into detection and interception of malicious software in open source before it becomes a problem is key – language in the America COMPETES Act can be altered to accomplish this goal[81].

3) Diversify the US Cyber Security Jobs Pipeline

To keep up with China's rapidly growing cyber personnel, Congress should loosen restrictions on contractors to hire foreign talent in the EU or elsewhere, expand the H1-B visa quota for cyber security and engineering talent, double Cybercorps Scholarship for Service funding from 20 million to 40 million dollars[82], fund cyber security education at levels similar to the National Defense Education Act during the space race, and expand the U.S. Digital Service "tour of duty" model[83] to public cyber defense jobs.

4) Work with Allies to Support U.S. Values in the Information Domain

Encouraging US and allied leadership in international standards bodies like the ITU will continue to show support for a free and open Internet. In addition, Congress can move beyond naming and shaming to impose costs on Chinese cyber threat groups by asking the Department of Commerce or Treasury to add Chinese institutions connected to cyber operations to the entities list and sanctions list. This would effectively ban them from using U.S.-produced operating systems and microprocessors, which Chinese firms currently rely heavily on. Note that this must be paired with clear guidelines on how Chinese institutions could get themselves removed from the list to encourage more responsible behavior.

Works Cited

[1] DigiChina. "Lexicon: 网络强国 Wǎngluò Qiángguó." Accessed February 8, 2022. https://digichina.stanford.edu/work/lexicon-网络强国-wangluo-qiangguo/.

[2] Voo, Julia, Irfan Hemani, Simon Jones, Winnona DeSombre, Dan Cassidy, and Anina Schwarzenbach. "Harvard Belfer National Cyber Power Index 2020." Harvard Belfer Center, September 2020. https://www.belfercenter.org/publication/national-cyber-power-index-2020.

[3] Center for Security and Emerging Technology. "CSET Original Translation: China's 14th Five-Year Plan." Accessed February 8, 2022. https://cset.georgetown.edu/publication/china-14th-five-year-plan/.

[4] DataGuidance. "China: MIIT Issues Notice on the 14th Five-Year Plan for Information and Communication Industry," November 16, 2021. https://www.dataguidance.com/news/china-miit-issues-notice-14th-five-year-plan.

[5] DigiChina. "Translation: 14th Five-Year Plan for National Informatization – Dec. 2021." Accessed February 8, 2022. https://digichina.stanford.edu/work/translation-14th-five-year-plan-for-national-informatization-dec-2021/.

[6]"Outline of the 14th Five-Year Plan (2021-2025) for National Economic and Social Development and Vision 2035 of the People's Republic of China_ News_ 福建省人民政府门户网站." Accessed February 8, 2022. https://webcache.googleusercontent.com/search?q=cache:86P649lhIskJ:https://www.fujian.gov.cn/english/news/202108/t20210809_5665713.htm&hl=en&gl=us&strip=1&vwsrc=0.

[7] Federation Of American Scientists. "China's Science of Military Strategy (2013)." Accessed February 8, 2022. https://fas.org/blogs/secrecy/2015/08/china-sms/.

[8] Peterson, Dahlia. "How China Harnesses Data Fusion to Make Sense of Surveillance Data." *Brookings* (blog), September 23, 2021. https://www.brookings.edu/techstream/how-china-harnesses-data-fusion-to-make-sense-of-surveillance-data/.

[9] "ATA-2021-Unclassified-Report.Pdf." Accessed February 8, 2022. https://www.dni.gov/files/ODNI/documents/assessments/ATA-2021-Unclassified-Report.pdf.

[10] New America. "Translation: Xi Jinping's April 20 Speech at the National Cybersecurity and Informatization Work Conference." Accessed February 8, 2022. http://newamerica.org/cybersecurity-initiative/digichina/blog/translation-xi-jinpings-april-20-speech-national-cybersecurity-and-informatization-work-conference/.

[11] Council on Foreign Relations. "The 18th Party Congress and Chinese Cyberpower." Accessed February 8, 2022. https://www.cfr.org/blog/18th-party-congress-and-chinese-cyberpower.

[12] "China's Internet Governance_ A New Conceptualization.Pdf." Accessed February 8, 2022. https://dukespace.lib.duke.edu/dspace/bitstream/handle/10161/18308/

[13] Tanner, Murray Scot, Peter W Mackenzie, CNA Corporation, Marine Corps University (U.S.), and Press. *China's Emerging National Security Interests and Their Impact on the People's Liberation Army*, 2015. https://search.ebscohost.com/direct.asp?db=mth&jid=JOEQ&scope=site.

[14] "Costello and McReynolds - CHINA STRATEGIC PERSPECTIVES 13.Pdf." Accessed February 8, 2022. https://ndupress.ndu.edu/Portals/68/Documents/stratperspective/china/china-perspectives_13.pdf.

[15]"Saunders - Chairman Xi Remakes the PLA Assessing Chinese Mil.Pdf." Accessed February 8, 2022. https://ndupress.ndu.edu/Portals/68/Documents/Books/Chairman-Xi/Chairman-Xi.pdf.

[16] "What Is Military Fusion - Department of State." Accessed February 8, 2022. https://www.state.gov/wp-content/uploads/2020/05/What-is-MCF-One-Pager.pdf.

[17] "How Does China Aim to Use AI in Warfare?" Accessed February 8, 2022. https://thediplomat.com/2021/12/how-does-china-aim-to-use-ai-in-warfare/.

[18] Defense One. "How Chinese Strategists Think AI Will Power a Military Leap Ahead." Accessed February 8, 2022. https://www.defenseone.com/ideas/2021/09/how-chinese-strategists-think-ai-will-power-military-leap-ahead/185409/.

[19] "Doshi et. al - China as a Cyber Great Power Beijing's Two Voices in Telecommunications." Accessed February 8, 2022. https://www.brookings.edu/wp-content/uploads/2021/04/FP_20210405_china_cyber_power.pdf.

[20] Burke, Edmund, Kristen Gunness, Cortez Cooper, and Mark Cozad. *People's Liberation Army Operational Concepts*. RAND Corporation, 2020. https://doi.org/10.7249/RRA394-1.

[21] Nimmo, Ben, Camille François, C Shawn Eib, and Léa Ronzaud. "Spamouflage Goes to America,"https://graphika.com/reports/spamouflage-dragon-goes-to-america/.

[22]Council on Foreign Relations. "Is 'Made in China 2025' a Threat to Global Trade?" Accessed February 8, 2022. https://www.cfr.org/backgrounder/made-china-2025-threat-global-trade.

[23] Reuters. "Taiwan Chip Industry Emerges as Battlefront in U.S.-China Showdown." Accessed February 8, 2022. https://www.reuters.com/investigates/special-report/taiwan-china-chips/.

[24] Council on Foreign Relations. "China's Digital Aid: The Risks and Rewards." Accessed February 8, 2022. https://www.cfr.org/china-digital-silk-road.

[25] U.S. Department of Defense. "Official Talks DOD Policy Role in Chinese Pacing Threat, Integrated Deterrence." Accessed February 8, 2022. https://www.defense.gov/News/News-Stories/Article/Article/2641068/official-talks-dod-policy-role-in-chinese-pacing-threat-integrated-deterrence/.

[26] U.S. Office of the Director of National Intelligence. "Annual Threat Assessment of the US Intelligence Community". Accessed February 8, 2022. https://www.dni.gov/files/ODNI/documents/assessments/ATA-2021-Unclassified-Report.pdf.

[27] War on the Rocks. "China Flaunts Its Offensive Cyber Power," October 22, 2021. https://warontherocks.com/2021/10/china-flaunts-its-offensive-cyber-power/.

[28] Patrick Howell O'Neill. "How China Turned a Prize-Winning IPhone Hack against the Uyghurs." Accessed February 8, 2022. https://www.technologyreview.com/2021/05/06/1024621/china-apple-spy-uyghur-hacker-tianfu/.

[29] The Record by Recorded Future. "Windows 10, IOS 15, Ubuntu, Chrome Fall at China's Tianfu Hacking Contest," October 17, 2021. https://therecord.media/windows-10-ios-15-ubuntu-chrome-fall-at-chinas-tianfu-hacking-contest/.

[30] The Record by Recorded Future. "Pwn2Own 2021 Hacking Contest Ends with a Three-Way Tie," April 9, 2021. https://therecord.media/pwn2own-2021-hacking-contest-ends-with-a-three-way-tie/.

[31] "Why Is the Log4j Cybersecurity Flaw the 'Most Serious' in Decades?" *New York Post* (blog), December 20, 2021. https://nypost.com/2021/12/20/why-is-the-log4j-cybersecurity-flaw-the-most-serious-in-decades/.

[32]Greig, Jonathan. "Chinese Regulators Suspend Alibaba Cloud over Failure to Report Log4j Vulnerability." ZDNet. Accessed February 8, 2022. https://www.zdnet.com/article/log4j-chinese-regulators-suspend-alibaba-partnership-over-failure-to-report-vulnerability/.

[33] History. "Inside America's Shocking WWII Propaganda Machine," December 19, 2016. https://www.nationalgeographic.com/history/article/world-war-2-propaganda-history-books.

[34] Matthew Shaer. "Fighting the Nazis With Fake News." Smithsonian Magazine. Accessed February 8, 2022. https://www.smithsonianmag.com/history/fighting-nazis-fake-news-180962481/.

[35] Recorded Future. "Elephants Must Learn to Street Dance: The Chinese Communist Party's Appeal to Youth in Overseas Propaganda," February 3, 2022. https://www.recfut.com/elephants-street-dance-chinese-communist-party-appeal-youth-overseas-propaganda/.

[36] "Chinese Government Deploying Online Influencers amid Beijing Olympics Boycotts." OpenSecrets News, December 13, 2021. https://www.opensecrets.org/news/2021/12/chinese-government-deploying-online-influencers-amid-beijing-olympics-boycotts/.

[37] Alex Hern. "Revealed: How TikTok Censors Videos That Do Not Please Beijing." *The Guardian*, September 25, 2019, sec. Technology. https://www.theguardian.com/technology/2019/sep/25/revealed-how-tiktok-censors-videos-that-do-not-please-beijing.

[38] Nimmo, Ben, Ira Hubert, and Yang Cheng. "Spamouflage Breakout," Accessed February 8, 2022. https://public-assets.graphika.com/reports/graphika_report_spamouflage_breakout.pdf.

[39] Adams et al. "Responsible Cyber Offense." Lawfare, August 2, 2021. https://www.lawfareblog.com/responsible-cyber-offense.

[40] LII / Legal Information Institute. "10 U.S. Code § 394 - Authorities Concerning Military Cyber Operations." Accessed February 8, 2022. https://www.law.cornell.edu/uscode/text/10/394.

[41] U.S.–China Cyber Agreement. Accessed February 8, 2022. https://sgp.fas.org/crs/row/IN10376.pdf

[42] Marketplace. "China's State-Backed Cyberattacks Are Part of a Larger Plan," December 9, 2021. https://www.marketplace.org/2021/12/09/chinas-state-sponsored-industrial-espionage-is-part-of-a-larger-system/.

[43] NBC News. "Are Chinese Hackers Slowing Down Their Cyber Attacks on the U.S.?" Accessed February 8, 2022. https://www.nbcnews.com/tech/tech-news/are-chinese-hackers-slowing-down-their-cyber-attacks-u-s-n601961.

[44] "A Peek into BRONZE UNION's Toolbox." Accessed February 8, 2022. https://www.secureworks.com/research/a-peek-into-bronze-unions-toolbox.

[45] Ibid

[46] ComputerWeekly.com. "Nation State APT Groups Prefer Old, Unpatched Vulnerabilities." Accessed February 8, 2022. https://www.computerweekly.com/news/252483043/Nation-state-APT-groups-prefer-old-unpatched-vulnerabilities.

[47] DeSombre et al. "Countering Cyber Proliferation: Zeroing in on Access-as-a-Service - Atlantic Council," March 1, 2021. https://www.atlanticcouncil.org/in-depth-research-reports/report/countering-cyber-proliferation-zeroing-in-on-access-as-a-service/.

[48] Security Affairs. "Attackers behind Operation Oceansalt Reuse Code from Chinese Comment Crew," October 19, 2018. https://securityaffairs.co/wordpress/77228/apt/operation-oceansalt.html.

[49] Temple-Raston, Dina. “China’s Microsoft Hack May Have Had A Bigger Purpose Than Just Spying.” *NPR*, August 26, 2021, sec. Investigations. https://www.npr.org/2021/08/26/1013501080/chinas-microsoft-hack-may-have-had-a-bigger-purpose-than-just-spying.

[50] Greenberg, Andy. “Chinese Hacking Spree Hit an ‘Astronomical’ Number of Victims.” *Wired*. Accessed February 8, 2022. https://www.wired.com/story/china-microsoft-exchange-server-hack-victims/.

[51] “Myths and Realities of China’s Military-Civil Fusion Strategy.” Accessed February 8, 2022. https://www.cnas.org/publications/reports/myths-and-realities-of-chinas-military-civil-fusion-strategy.

[52] “What Is Military Fusion - Department of State.” Accessed February 8, 2022. https://www.state.gov/wp-content/uploads/2020/05/What-is-MCF-One-Pager.pdf.

[53] CyberScoop. “DOJ Reveals Indictment against Chinese Cyber Spies That Stole U.S. Business Secrets,” November 27, 2017. https://www.cyberscoop.com/boyusec-china-doj-indictment/.

[54] Bloomberg. “Chinese Spies Accused of Using Huawei in Secret Australia Telecom Hack,” December 16, 2021. https://www.bloomberg.com/news/articles/2021-12-16/chinese-spies-accused-of-using-huawei-in-secret-australian-telecom-hack.

[55]Solomon, Salem. “After Allegations of Spying, African Union Renews Huawei Alliance.” VOA. Accessed February 8, 2022. https://www.voanews.com/a/after-allegations-of-spying-african-union-renews-huawei-alliance/4947968.html.

[56] Cybercrime Magazine. “China Cybersecurity Companies,” September 18, 2018. https://cybersecurityventures.com/china-cybersecurity-companies/.

[57] Bird, Bird LLP-Amanda Ge, James Gong, Tiantian Ke, and Clarice Yue. “China Data Protection and Cybersecurity: Annual Review of 2021 and Outlook for 2022 (II).” Lexology, January 26, 2022. https://www.lexology.com/library/detail.aspx?g=0a24afb9-7f27-4b18-9486-3ba3ddc688e6.

[58] South China Morning Post. “China Drafts Plan to Grow Its Cybersecurity Industry as Threats Grow,” July 13, 2021. https://www.scmp.com/tech/policy/article/3140963/china-drafts-three-year-plan-boost-its-cybersecurity-industry-amid.

[59] “FROM EQUATION TO EQUATIONS - Antiy Labs | The Next Generation Anti-Virus Engine Innovator.” Accessed February 8, 2022. https://www.antiy.net/p/from-equation-to-equations/.

[60] Qihoo360. “The CIA Hacking Group (APT-C-39) Conducts Cyber-Espionage Operation on China’s Critical Industries for 11 Years.” Accessed February 8, 2022. https://blogs.360.cn/post/APT-C-39_CIA_EN.html.

[61] Symantec Threat Hunter Team. “Buckeye: Espionage Outfit Used Equation Group Tools Prior to Shadow Brokers Leak.” Accessed February 8, 2022. https://symantec-enterprise-blogs.security.com/blogs/threat-intelligence/buckeye-windows-zero-day-exploit.

[62] “Doshi et. al - China as a Cyber Great Power Beijing’s Two Voices in Telecommunications.” Accessed February 8, 2022. https://www.brookings.edu/wp-content/uploads/2021/04/FP_20210405_china_cyber_power.pdf.

[63] AppleInsider. “Apple Made Secret 5-Year $275B Deal with Chinese Government.” Accessed February 8, 2022. https://appleinsider.com/articles/21/12/07/apple-made-secret-5-year-275b-deal-with-chinese-government.

[64] BBC News. “Five Eyes: Is the Alliance in Trouble over China?,” May 4, 2021, sec. Asia. https://www.bbc.com/news/world-56970640.

[65] “The International Telecommunication Union: The Most Important UN Agency You Have Never Heard Of.” Accessed February 8, 2022. https://www.csis.org/analysis/international-telecommunication-union-most-important-un-agency-you-have-never-heard.

[66] Center for Security and Emerging Technology. “China’s National Cybersecurity Center.” Accessed February 8, 2022. https://cset.georgetown.edu/publication/chinas-national-cybersecurity-center/.

[67] ISC2. “ISC2 Cybersecurity Workforce Study 2021” Accessed February 8, 2022. https://www.isc2.org//-/media/ISC2/Research/2021/ISC2-Cybersecurity-Workforce-Study-2021.ashx.

[68] Joske, Alex. “The China Defence Universities Tracker.” Accessed February 8, 2022. https://www.aspi.org.au/report/china-defence-universities-tracker.

[69] DeSombre et. al. “Surveillance Technology at the Fair: Proliferation of Cyber Capabilities in International Arms Markets,” Atlantic Council, November 8, 2021. https://www.atlanticcouncil.org/in-depth-research-reports/issue-brief/surveillance-technology-at-the-fair/.

[70] Uren, Tom. “Srsly Risky Biz: Thursday, November 11.” Substack newsletter. *Seriously Risky Business* (blog), November 10, 2021. https://srslyriskybiz.substack.com/p/srsly-risky-biz-thursday-november-3a2.

[71] South China Morning Post. “China Drafts Plan to Grow Its Cybersecurity Industry as Threats Grow,” July 13, 2021. https://www.scmp.com/tech/policy/article/3140963/china-drafts-three-year-plan-boost-its-cybersecurity-industry-amid.

[72] KOAA. “Deep Dive: Cybersecurity Professional Shortage a Serious Concern for National Security,” June 8, 2021. https://www.koaa.com/news/deep-dive/cybersecurity-professional-shortage-a-serious-concern-for-national-security.

[73]IISS. “Cyber Capabilities and National Power: A Net Assessment.” Accessed February 8, 2022. https://www.iiss.org/blogs/research-paper/2021/06/cyber-capabilities-national-power.

[74] “Government Incentives and US Competitiveness in Semiconductor Manufacturing 2020.” Accessed February 8, 2022. https://www.semiconductors.org/wp-content/uploads/2020/09/Government-Incentives-and-US-Competitiveness-in-Semiconductor-Manufacturing-Sep-2020.pdf.

[75] Reuters. “Taiwan Chip Industry Emerges as Battlefront in U.S.-China Showdown.” Accessed February 8, 2022. https://www.reuters.com/investigates/special-report/taiwan-china-chips/.

[76] Zetter, Kim. “An Unprecedented Look at Stuxnet, the World’s First Digital Weapon.” *Wired*. Accessed February 8, 2022. https://www.wired.com/2014/11/countdown-to-zero-day-stuxnet/.

[77] Shevchenko, Sergei. “Agent.Btz - A Threat That Hit Pentagon.” Accessed February 8, 2022. http://blog.threatexpert.com/2008/11/agentbtz-threat-that-hit-pentagon.html.

[78] IISS. “Cyber Capabilities and National Power: A Net Assessment.” Accessed February 8, 2022. https://www.iiss.org/blogs/research-paper/2021/06/cyber-capabilities-national-power.

[79] TechCrunch. “US Federal Agencies Told to Patch Hundreds of Security Bugs.” Accessed February 8, 2022. https://social.techcrunch.com/2021/11/03/cisa-directive-hundreds-security-patches/.

[80] Congress.gov. "H.R.7178 - 116th Congress (2019-2020): CHIPS for America Act." June 11, 2020. https://www.congress.gov/bill/116th-congress/house-bill/7178.

[81]Congress.gov. "Text - H.R.4521 - 117th Congress (2021-2022): Bioeconomy Research and Development Act of 2021 [America COMPETES Act of 2022]." February 4, 2022. https://www.congress.gov/bill/117th-congress/house-bill/4521/text.

[82] "CyberCorps(R) Scholarship for Service (SFS) (Nsf21580) | NSF - National Science Foundation." Accessed February 8, 2022. https://www.nsf.gov/pubs/2021/nsf21580/nsf21580.htm.

[83] United States Digital Service. "Apply to USDS." Accessed February 8, 2022. https://usds.gov/apply.

OPENING STATEMENT OF DEAN CHENG, SENIOR RESEARCH FELLOW IN ASIAN STUDIES, HERITAGE FOUNDATION

CHAIRMAN WONG: Thank you, Ms. DeSombre. And you were under time, which is usually not the case.

But let me turn to Dean Cheng.

MR. CHENG: Chairman Wong, Co-Chairman Bartholomew, thank you for the opportunity to be here today. My name is Dean Cheng. I'm a senior research fellow at the Heritage Foundation. The views I express in this testimony are my own and should not be construed as representing any official position of the Heritage Foundation.

In response to the questions that I was asked to address I want to focus my spoken testimony this morning on two aspects: Chinese military doctrine regarding information warfare and Chinese thoughts on information deterrence.

With regard to the first we have an interesting opportunity to watch the Chinese evolve their approach and their doctrine as the PLA is in the midst of a doctrinal revision. This is reflected in the November 2020 issuance by the PLA of the Chinese PLA Joint Operation's gangyao test version. Gangyao, translated by the Chinese's program, is somewhat akin to our field manuals and joint publications from the Joint Chiefs of Staff, but have the authority of doctrine. They are a key part of the Chinese system of rules and regulations helping to create a more standardized approach to various policy issues.

In this case the decision to issue new gangyao reflects the Chinese assessment that modern warfare is undergoing fundamental changes including changes to the international security environment where China faces greater threats, shifts in how warfare is conducted, and changes in the PLA's own organizational structure. The combination of changes have been so profound in their view that we are seen as entering a “new era,” requiring significant adjustments across the PLA including in terms of doctrine and eventually training.

To accommodate these changes, the gangyao specifically goes to the question what kind of war will the PLA have to fight and how will the PLA fight these wars? And what is striking is that the Chinese themselves note that they exploit foreign experience in part because they themselves have not fought a war since 1979.

As important, they therefore take into account the new iteration of the so-called new historic missions. In 2004, then head of China, Hu Jintao, issued what were known as the new historic missions to the PLA. Those remain in force. Notable for this hearing is that the PLA is charged with providing quote/unquote, strategic support for maintaining national interests, including the ability to establish dominance over the maritime, outer space, and electromagnetic domains.

These new gangyao therefore: (1) are aimed at facilitating establishing this dominance; (2) they seek to exploit changes in the PLA's organizational structure.

On December 31st, 2015 the PLA underwent the greatest organizational shift in its history, touching every aspect of the PLA: how it is managed, how it is organized for war fighting, and even new services. Here one of the most important aspects is this creation of the PLA Strategic Support Force.

The PLA Strategic Support Force is charged with the conduct of electronic warfare, network warfare, and space warfare. This is essentially China's information warfare force and these new gangyao clearly seek to exploit the creation of this information warfare force.

In particular what is notable is that the PLA SSF is responsible for conducting what they term integrated network and electronic warfare. This is much more. And this is specifically called out in a recent Chinese textbook, The Science of Military Strategy, 2020 Edition, that integrated network and electronic warfare is much more than traditional computer network warfare. While it touches on computers and computer networks it involves attacking the adversary's broader system of systems, military and civilian information networks. It will occur in wartime, but also in time of crisis and peace time. It involves physical hardware, software, human cognition and interpretation.

With this last element it is notable that the PLA SSF incorporated Base 311. Base 311 is a political warfare unit responsible for the conduct of what the Chinese term the three warfares: psychological warfare, public opinion warfare; and legal warfare. Essentially we need to recognize that in attacking our networks a key element in the Chinese concept of the network is the human factor, that it is not simply zeroes and ones. It is not simply computers. It is the human element of interpreting what is on the screen. Do you believe the emails on your screen? Do you believe that your email went to the right place and conversely that the tweet, the Instagram, the TikTok actually is a reflection of reality?

PLA writings indicate that key targets then for network and electronic warfare, as well as psychological warfare, includes national and military decision makers, strategic early warnings systems, military information networks, energy, financial, and transportation networks. And we should expect that these gangyao will call for operations against all of these elements providing greater detail.

Moving then onto a key mission area for the PLA SSF, it will be information deterrence. Alongside nuclear conventional space deterrence the PLA talks about the importance of information deterrence. Here it is important to realize the Chinese term weishe, which is commonly translated as deterrence, is much better translated as coercion. It is compelling an adversary to do something they don't want to do, which can be positive; do what I want, or negative; don't do what I don't want.

In this regard information deterrence like space deterrence is not about preventing actions in space or in the cyber realm. It is about using information operations such as those I outlined earlier; or space operations, to effect and achieve a political end. I want you not to aid Taiwan. I will engage in space operations or information operations to get you to do as I wish. This therefore includes both network and electronic warfare, as well as the psychological aspects.

We see this already being effected in some ways by the Russians in thinking about should the U.S. intervene in Ukraine? There is great fear already about the potential attacks on American networks by the Russians. The Chinese very clearly are going to be watching our response to the Ukraine situation and fit that in accordingly.

Very briefly with regards to congressional options and actions, what I would note here is that given the very comprehensive Chinese approach the role of Congress in achieving a military response is arguably overreach and extending into the micromanagement aspect. Given Congress' power of the purse and the ability to create laws what I would suggest is that much more useful would be striking at China through financial and other aspects that would signal, relatively asymmetrically, that their actions in the cyber realm have consequences.

Thus, for example, why does a Chinese company - why are Chinese companies able to list on the American Stock Exchanges when they are not required to comply with Sarbanes-Oxley and why would trade in intellectual property that has been stolen be treated any differently than dealing in stolen DVD players - do people still use DVD players - computers and the like?

RICO racketeering charges are commonplace against networks of criminal actions. I would suggest that just because it is a state-owned enterprise, just because it's intellectual property does not - should not provide immunity from that.

I thank the Commission for the opportunity to be here today.

PREPARED STATEMENT OF DEAN CHENG, SENIOR RESEARCH FELLOW IN ASIAN STUDIES, HERITAGE FOUNDATION

[PLA Perspectives on Network Warfare in “Informationized Local Wars”]

Testimony before
U.S.–China Economic and Security Review Commission

[February 17, 2022]

Dean Cheng

Senior Research Fellow for Chinese Political and Security Affairs,

The Heritage Foundation

My name is Dean Cheng. I am the Senior Research Fellow for Chinese Political and Security Affairs at The Heritage Foundation. The views I express in this testimony are my own, and should not be construed as representing any official position of The Heritage Foundation.

The People’s Republic of China (PRC), including the Chinese People’s Liberation Army (PLA) has not fought a war since 1979. However, the PLA has been a careful observer of other people’s wars since at least the 1990s. By observing American wars, including the First Gulf War (1990), the invasion of Afghanistan (2001), and the Iraq War (2003); NATO’s conflict in the Balkans (1990s); and Russian conflicts in Georgia (2008) and Syria, the PLA reached certain conclusions about the likely characteristics of any future wars it will be engaged in.

PLA Assessment of War in the Information Age

The most important is that victory or defeat in future wars will be a function of the ability to exploit information. Indeed, in the eyes of both the Chinese Communist Party as well as the PLA, as the world has entered the Information Age, the currency of international power, including economic and military capacity, is increasingly a function of the ability to harness information. The growing importance of information in the realm of defense is reflected in the evolution of the PLA’s “military strategic guidelines (*junshi zhanlue fangzhen*; 军事战略方针).” These guidelines are the closest equivalent to the U.S. National Military Strategy, and provide guidance for PLA “force development, planning, and disposition.”[1]

Since 1993, the PLA’s military strategic guidelines have twice been modified; in each case, the modifications have reflected the growing role of information in future warfare. In 1993, the PLA was intent on preparing for “local wars under modern, high-technology conditions.” This shifted to preparing for “local wars under informationized conditions” in 2004, and then to preparing to fight and win “informationized local wars” in 2015. In essence, the PLA has steadily sharpened its focus from high technology in general to information technology as the centerpiece of future warfighting capabilities.

[1] Joel Wuthnow, “What I Learned From the PLA’s Latest Strategy Textbook,” ***Jamestown Foundation China Brief*** (XXI, 11, May 25, 2021), https://jamestown.org/program/what-i-learned-from-the-plas-latest-strategy-textbook/

The rise of the Information Age, where the gathering, analysis, and exploitation of information has become essential, has seen the concomitant rise of "informationized warfare (*xinxihua zhanzheng*; 信息化战争)." This is defined as system-of-systems conflict involving the use of informationized weapons and associated tactics in the land, sea, air, outer space, and network and electronic spaces. It is marked by a reliance on networked information systems, and is viewed by the PLA as the basic form of warfare in the Information Age. [2]

This growing emphasis on information technology is in turn tied to the PLA's analysis of how future wars will be fought.

First, based on Chinese assessments of American, NATO, and Russian wars, the PLA deems it likely that its future wars will likely be *joint*. For the PLA, however, the concept of "jointness" has in turn steadily evolved from involving multiple different services operating in close physical proximity and at roughly the same time, to operations across multiple domains under a single command structure, in accordance with a single plan. The PLA's forces will need to interoperate in not only the traditional land, sea, and air domains, but also outer space and the electromagnetic domain.

To conduct joint operations successfully, however, it is essential that the participating forces in any future operations have the ability to *share information* and forge a *common situational awareness*. This in turn requires the ability to handle vast amounts of data, including from not only myriad military sensors (of all the services), but also local and national sources, which may include not only military but political, financial, and economic information. The PLA must be networked, not only among its component services and branches, but also with local and national infrastructure and governments. The integrated joint operations envisioned by the PLA therefore requires not only a single, unified command structure, but an integrated information network for sharing and fusing information from all sources and then distributing that information rapidly to all the participating forces across all the domains. As one Chinese author notes, "Future joint operations are built upon the foundation and with the support of networked informational systems-of-systems."[3]

At the same time, it is presumed that an adversary will be similarly networked, both within their military forces and to their broader respective local and national governments, infrastructure, and institutions. In particular, the United States is seen as being experienced with handling massive amounts of data and fielding a thoroughly networked military and broader economy. Those networks are therefore essential targets for the PLA and the broader Chinese network warfare community.

The ability to establish control of information and information flow at a particular time and within a particular space is the essence of establishing "information dominance (*zhi xinxi quan*; 制信息权)."[4] It entails the ability to collect more information, manage it faster, and employ it more precisely than the adversary.[5] The side that enjoys information dominance can then seize and retain the initiative, and force the adversary into a reactive mode, losing the ability to influence the outcome of an

[2] All Army Military Terminology Management Commission, *Chinese People's Liberation Army Terminology* (Unabridged Volume), (Beijing, PRC: Military Science Publishing House, 2011), p. 48.

[3] TANG Renjiang, "The More We Emphasize Jointness, the More We Must Push Regulation-Based Administration," *PLA Daily* (November 23, 2020) http://www.qstheory.cn/qshyjx/2020-11/23/c_1126773694.htm

[4] All Army Military Terminology Management Commission, *Chinese People's Liberation Army Terminology* (Unabridged Volume), (Beijing, PRC: Military Science Publishing House, 2011), p. 79.

[5] Chinese Military Encyclopedia 2nd Edition Editorial Committee, *PLA Encyclopedia,* 2nd Edition, *Military Strategy* (Beijing, PRC: China Encyclopedia Publishing House, 2007), p. 68.

engagement. Information dominance is built upon both defending one's own networks and attacking and degrading the adversary's.

In light of the military strategic guidelines, and in support of the efforts to undertake joint operations and establish information dominance in future conflicts, the PLA has been undertaking an extensive, multi-faceted modernization program. The most visible element has been the steady improvement in the PLA's arsenal. From anti-ship ballistic missiles to domestically produced aircraft carriers to stealth fighters and light tanks, the current PLA has enjoyed a steady flow of new equipment over the past three decades, to the point that this is arguably the most well-equipped and sophisticated force ever fielded by the People's Republic of China.

As important, this modernization effort has included substantial acquisitions of platforms and systems that can help establish information dominance. In major PLA parades in 2009 and again in 2015, for example, the PLA Air Force fly-by was led by airborne early warning (AEW) aircraft.[6] The PLA has tested a variety of space weapons, including kinetic kill vehicles and now service satellites that can disrupt or destroy an adversary's satellites.[7]

PLA Reorganization

This equipment modernization was complemented on December 31, 2015, when the PLA underwent the most extensive reorganization since its founding. Almost every aspect of its structure was affected. The various measures are encapsulated in the Chinese statement, "The Central Military Commission manages the overall; the war zones are responsible for warfighting; the services are responsible for [military force] building (*junwei guanzong, zhanqu zhuzhan, junzhong zhujian；军委管总，战区主战，军种主建*)." Each aspect included elements to improve the ability of the PLA to undertake more informationized operations.

In terms of the *Central Military Commission* (CMC), the reorganization saw an expansion from the previous four general departments to fifteen departments, commissions, and offices.

Name	Chinese Name	Chinese characters
CMC General Office	Junwei bangong ting	军委办公厅
CMC Joint Staff Department	Junwei lianhe canmou bu	军委联合参谋部
CMC Political Work Department	Junwei zhengzhi gongzuo bu	军委政治工作部
CMC Logistics Support Department	Junwei houqin baozhang bu	军委后勤保障部
CMC Equipment Development Department	Junwei zhuangbei fazhan bu	军委装备发展部

[6] "Warplanes Fly Over Tianamen Square in Rehearsal," Xinhua (September 22, 2009) https://covid-19.chinadaily.com.cn/china/2009-09/22/content_8722768.htm and Alexander Neil, "China Parade to Display Past and Future," BBC (September 1, 2015) https://www.bbc.com/news/world-asia-34105252

[7] Brett Tingly, "A Chinese Satellite Just Grappled Another and Pulled It Out of Orbit," The Drive (January 27, 2022) https://www.thedrive.com/the-war-zone/44054/a-chinese-satellite-just-grappled-another-and-pulled-it-out-of-orbit

CMC Training and Management Department	Junwei xunlian guanli bu	军委训练管理部
CMC National Defense Mobilization Department	Junwei guofang dongyuan bu	军委国防动员部
CMC Discipline Inspection Commission	Junwei jilu jiancha weiyaun hui	军委记律检查委员会
CMC Politics and Law Commission	Junwei zhengfa weiyuan hui	军委政法委员会
CMC Science and Technology Commission	Junwei kexue jishu weiyuan hui	军委科学技术委员会
CMC Strategic Planning Office	Junwei zhanlue guihua bangongshi	军委战略规划办公室
CMC Reform and Organization Office	Junwei gaige he bianzhi bangongshi	军委改革和编制办公室
CMC International Military Cooperation Office	Junwei guoji junshi hezuo bangongshi	军委国际军事合作办公室
CMC Audit Office	Junwei shenjishu	军委审计署
CMC Office Affairs and General Administration	Junwei jiguan shiwu guanli zongju	军委机关事务管理总局

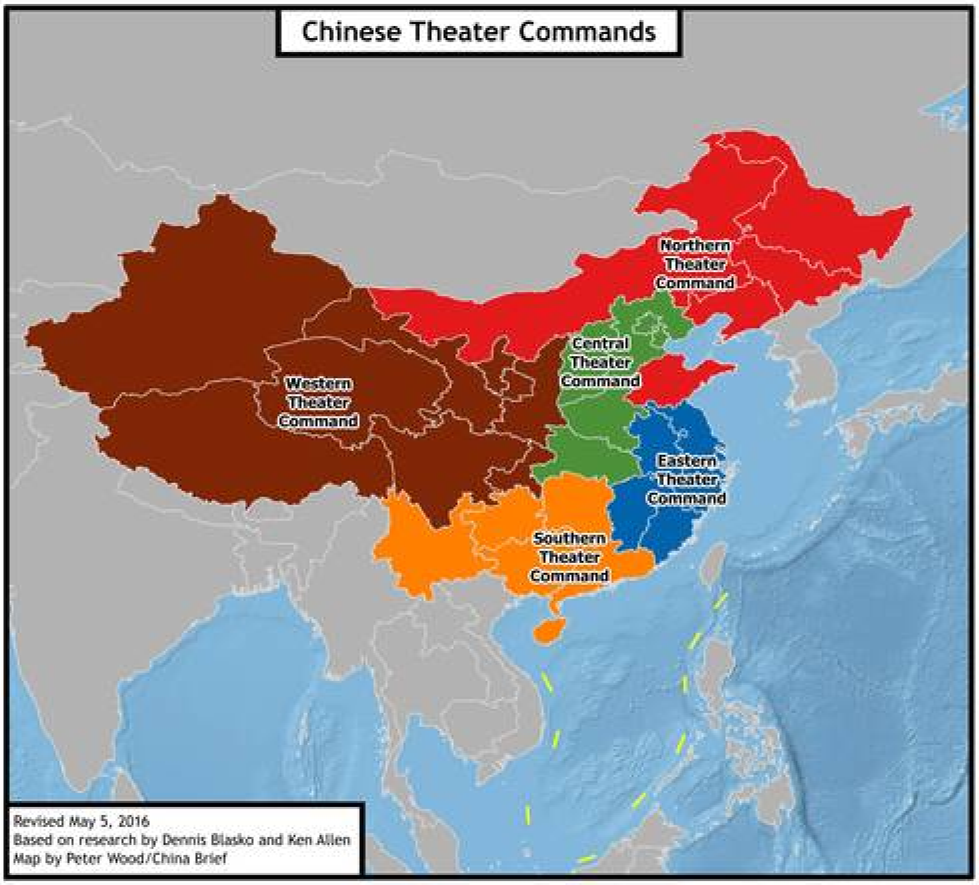
Notably, the previous General Staff Department, responsible for war planning and overall command of the PLA, has now become the CMC Joint Staff Department. This highlights the importance of joint operations in the PLA's vision of future conflicts, and underscores the need for PLA commanders to think in terms of the entire military and not just the ground forces (which had previously dominated the staffing of the CMC).

Meanwhile, the previous General Political Department (GPD) has had its functions divided among the CMC Political Work Department, the CMC Discipline Inspection Commission, and the CMC Politics and Law Commission. This would suggest that the new CMC Political Work Department will focus on such tasks as the conduct of political warfare (including the "three warfares" of public opinion warfare, psychological warfare, and legal warfare), while criminal and anti-corruption investigations (also previously a GPD responsibility) may now be the task of the CMC Discipline Inspection Commission. Political warfare is seen as an integral part of establishing information dominance.

The creation of some of the new departments and commissions also reflects the elevation of key areas to prominence. In particular, the establishment of the CMC National Defense Mobilization Department reflects the growing importance of not only mobilization planning for the PLA, but also the effort at integrating civilian and military efforts in a variety of areas. Chinese concepts of mobilization extend beyond mobilization of manpower and some industrial facilities to the ability to employ key infrastructure for military ends, and the mobilization of key personnel, equipment, and facilities to supplement military forces. This would be especially important in the context of "civil-military fusion" of information warfare resources, including Chinese telecoms, cyber security firms, and information technology industries.

In terms of the new *war zones* (or theaters or theater commands), the reorganization saw the PLA transition from seven military regions (MRs) to five war zones (WZs). These are:[8]

Name	**Likely focus**
Northern War Zone	Mongolia, Russia, Korean peninsula
Eastern War Zone	Taiwan, Japan, East China Sea
Southern War Zone	South China Sea, Southeast Asia
Western War Zone	India, South Asia, Central Asia, "counterterrorism" in Xinjiang and Tibet
Central War Zone	Strategic reserve, support to other war zones



[9]

Unlike the previous MRs, these WZs are headed by new, joint headquarters that are permanent establishments. This means that the associated staffs are regularly operating together, and would already be familiar with each other in event of war. As important, whereas all the MRs had always

[8] Office of the Secretary of Defense, ***Military and Security Developments Involving the People's Republic of China 2021*** (Washington, DC: Department of Defense, 2021), p. 97, https://media.defense.gov/2021/Nov/03/2002885874/-1/-1/0/2021-CMPR-FINAL.PDF

[9] http://www.jamestown.org/single/?tx_ttnews%5Btt_news%5D=45069&no_cache=1#.V-FwUzVGRuo

been headed by ground force officers, several of the WZs are now headed by PLA Air Force and PLA Navy officers, emphasizing again the importance of joint operations.

Finally, the reorganization saw *the establishment of new services*, as well as the promotion of the Chinese nuclear forces from the Second Artillery "super-branch" to the PLA Rocket Forces. Relative to the goal of fighting "informationized local wars," a key organization is the new PLA Strategic Support Force (PLASSF). This entity brings China's space, network warfare, and electronic warfare forces under a single structure. The PLASSF's forces are responsible for achieving space dominance (*zhi tian quan;* 制天权), network dominance (*zhi wangluo quan;* 制网络权) and electronic dominance (*zhi dianzi quan;* 制电子权), which are in turn essential to establishing information dominance.

Notably, the PLASSF also incorporated Base 311 from the previous GPD. Base 311 was responsible for conducting political warfare, especially the "three warfares." "The 311 Base is the PLA's sole organization that is publicly known to focus on psychological warfare."[10] Political warfare, by influencing perceptions and assessments of military and political decision-makers, complements all other operations.

The PLASSF is very much the PLA's Information Warfare Force.

It is likely that there is a PLASSF contingent at each of the new WZ joint headquarters. This would be consistent with the presumption that future wars will entail cyber warfare, electronic warfare, and space warfare.

The PLASSF is especially noteworthy as it marks a truly innovative approach to the challenges of information warfare and modern conflict more broadly. The PRC is following a distinctly different path than either Russia or the United States. The Russian military, for example, established the Russian Aerospace Forces by combining the Russian Air Force and the Russian Aerospace Defense Force. Russian cyber forces do not appear to be part of the Russian Aerospace Forces.

Similarly, in the United States, there is no single service or combatant command that combines space, electronic warfare, and computer network warfare operations. Fielding of space forces is the responsibility of a new service, the United States Space Force (USSF), while the conduct of military space operations is the responsibility of US Space Command (USSPACECOM), a unified combatant command. Computer network operations are the responsibility of Cyber Command (USCYBERCOM), another unified combatant command, drawing upon the various services for cyber-capable forces. CYBERCOM shares some tasks with the National Security Agency, an intelligence organization and not a military force. Electronic warfare, meanwhile, is the responsibility of individual services.

Doctrinal Evolution

Alongside new equipment and a new organizational structure has been the promulgation of new doctrine. In November 2020, the PLA issued the "Chinese PLA Joint Operations Gangyao (Test)." (*zhongguo renmin jiefangjun lianhe zuozhan gangyao (shixing)*; 中国人民解放军联合作战纲要 [试行]) "Gangyao" (translated by the Chinese as "programs") are somewhat akin to field manuals, but have the authority of doctrine. They are a key part of the Chinese system of rules and regulations, helping to create a more standardized approach to various policy issues.[11] They also provide more specific

[10] John Costello and Joe McReynolds, ***China's Strategic Support Force: A Force for a New Era*** (Washington, DC: NDU Press, 2018), p. 17.

[11] All Army Military Terminology Management Commission, *Chinese People's Liberation Army Terminology* (Unabridged Volume), (Beijing, PRC: Military Science Publishing House, 2011), p. 569.

details, fleshing out the military strategic guidelines.[12] As with past military "gangyao," the PRC government has not released any version for public examination, but there has been significant discussion of these new ones.

According to PLA analyses, the sustained, ongoing development of information technologies, including artificial intelligence, big data, and cloud computing, have combined to create "new circumstances (*xin xingshi*; 新形势)" for military operations. The result has been essentially a military scientific revolution, requiring new operational forms and theories, and potentially further alterations of the PLA's organization.[13]

In particular, the development of these three technologies has opened a new stage in PLA thinking about the requirements for modernization. Where the PLA had long focused on becoming "fully mechanized and fully informationized," it now includes a new modernization goal of "intelligence-ization (*zhineng hua*; 智能化)."[14] The concept entails incorporating more artificial intelligence and machine learning into various platforms and systems. Building atop big data and cloud computing, the concept of "intelligence-ization" would seem to focus on allowing more data processing to occur within weapons and platforms, to better handle the huge amounts of data that are now flowing through the various networks.

These new "gangyao" apparently reflect these new circumstances. At a Chinese Ministry of Defense press conference, a PLA Defense Ministry spokesman observed that these new "gangyao" are necessary, both because of the PLA's reorganization and because of major changes in the global military situation. Thus, these new "gangyao" address the foremost issue: What kind of war will the PLA have to fight, and how will it fight that war?

According to the spokesman, the new "gangyao" provide more concrete guidance on how to conduct joint operations, especially in the face of new challenges and threats. Given the new organizations and structures within the PLA, these new "gangyao" are expected to clarify and strengthen the chain of command, including the relative roles of the CMC and the war zone command structures. As important, "it emphasizes the application of new types of combat strength."[15] The spokesman also notes that, in striving to meet the goal of a fully modernized PLA by 2027, the new "gangyao" will help the processes of mechanization, informationization, and intelligence-ization to be both accelerated and melded.

PLA Approach to Network Operations

Given the evolution of the PLA's view of the role of information in future wars, it is essential to note that the PLA's approach to information dominance does not appear to focus solely on cyber operations.

[12] Han Lin, Wei Bing, and Liu Jianwei, "Pushing Joint Operations Training to a Higher Level—'Chinese PLA Joint Operations Gangyao (Test)' Implementation After a Year," *PLA Daily* (January 5, 2022) http://www.mod.gov.cn/topnews/2022-01/05/content_4902340.htm

[13] FANG Xiaozhi, "These Five Years, What New Achievements have Chinese National Defense and Army-Building Reform Gained"? Overseas Network (December 29, 2018) https://k.sina.cn/article_3057540037_b63e5bc502000eb49.html

[14] XIAO Tianliang, Chief Editor, *Science of Military Strategy* (Beijing, PRC: National Defense University Press, 2020), p. 334, and PRC Ministry of Defense press conference transcript (November 26, 2020) http://www.mod.gov.cn/jzhzt/2020-11/26/content_4874643.htm

[15] PRC Ministry of Defense press conference transcript (November 26, 2020) http://www.mod.gov.cn/jzhzt/2020-11/26/content_4874643.htm

Indeed, it is important to recognize that the Chinese term "*wangluo zhan* (网络战)," while translated as "cyber war," is more accurately rendered as "network warfare."

Network warfare occurs in the realm of "network space (*wangluo kongjian*; 网络空间)," a term that roughly parallels that of "cyberspace." However, network warfare is seen as moving beyond just computer networks, although computer network warfare remains an integral element of network warfare. In relation to information warfare at the campaign level, it occurs within networks that are part of the overall battlefield (which can extend to outer space and deep into the two sides' homelands as part of the command and control, and logistical and support infrastructures).[16]

For the PLA, network warfare, also termed "network conflict (*wangluo duikang*; 网络对抗)," is comprised of the range of activities that occur within networked information space, as the two sides seek to reduce the effectiveness of the adversary's networks, while preserving one's own.[17] It includes not only offensive and defensive components, but also reconnaissance of adversary and others' networks.

The purpose of network warfare is to establish "network dominance (*zhi wangluo quan*; 制网络权)." When one has network dominance, the full range of one's own networks (not just computer networks) can operate smoothly and the information on those networks is safeguarded while being rapidly moved and applied; meanwhile an adversary's networks are prevented from doing the same. Some of the networks that are integral to network warfare include the command and control network, intelligence information network, and air defense network. [18] In Chinese writings, network space is sometimes described as the sixth domain (alongside land, sea, air, outer space, and the electromagnetic spectrum). In other cases, however, it is seen as the fifth domain, encompassing the electromagnetic spectrum.

Because of the importance of these various networks in the conduct of joint operations, informationized local wars will inevitably entail network warfare. For the weaker player, it is an especially potent means of neutralizing or weakening a stronger adversary's capabilities. One Chinese analysis observes that in the Balkan conflicts of the 1990s, although the Serbian forces were generally outmatched by NATO, they were nonetheless able to repeatedly penetrate various NATO networks and degrade their operations. The Chinese write that the Serbs were able to penetrate the networks of the aircraft carrier USS *Theodore Roosevelt* and British Meteorological Office, affecting air operations.[19] Another Chinese analysis similarly observes that the disparities in conventional strength between NATO and Serbia were not paralleled on the Internet, where Serbian forces successfully attacked various NATO and individual member states' web-sites.[20] Networks are so central to the

[16] YE Zheng, *Science of Information Operations Teaching Materials* (Beijing, PRC: Military Science Publishing House, 2013), p. 28.

[17] All Army Military Terminology Management Commission, *Chinese People's Liberation Army Terminology* (Unabridged Volume), (Beijing, PRC: Military Science Publishing House, 2011), p. 286, and YE Zheng, *Science of Information Operations Teaching Materials* (Beijing, PRC: Military Science Publishing House, 2013), p. 24.

[18] YE Zheng, *Science of Information Operations Teaching Materials* (Beijing, PRC: Military Science Publishing House, 2013), p. 24, 25.

[19] YUAN Wenxian, *Joint Campaign Information Operations Teaching Materials* (Beijing, PRC: Military Science Publishing House, 2009), p. 14.

[20] YUAN Wenxian, *The Science of Military Information* (Beijing, PRC: National Defense University Press, 2007), p. 73.

PLA's concept of modern warfare that one Chinese article suggests that informationized warfare is not possible without networks.[21]

While network warfare can yield powerful effects, PLA analysts seem to see it, and all other operations, as primarily embedded within a broader array of actions, as part of system-of-systems warfare (*tixi zuozhan*; 体系作战). Given the increasingly complex nature of modern warfare, individual platforms and even individual systems (*xitong*; 系统), by themselves, are unlikely to be decisive. Rather, conflicts are decided by the ability of rival arrays of systems, systems-of-systems (*tixi*; 体系), to out-perform each other.[22]

Systems-of-systems, in turn, are the product of integration through information flow. An effective information network allows information gathering, networking of forces and capabilities, and generation of synergies, to create a system-of-systems operational capacity that is substantially greater than what individual systems can bring to bear.[23] Success in future conflicts will therefore require all the various networks (information gathering, communications, command and control, weapons, logistics), drawn from all the participating services and operating across the various domains, to be able to work together, both in human as well as technical terms.[24]

Disrupting the adversary's networks, on the other hand, leads to the disintegration of their system-of-systems construct. This will significantly reduce their effectiveness, even if individual systems are able to function. Consequently, network warfare is an integral part of preserving one's own system-of-systems while degrading the adversary's.

An essential element of forging system-of-system effects is to integrate network and electronic warfare. This is the embodiment of the Chinese concept of unified joint operations. According to the PLA, electronic warfare, (*dianzi zhan*; 电子战), is the effort by each side to degrade and disrupt the adversary's electronic systems, while preserving one's own. [25] While electronic warfare is nominally aimed at equipment such as radars, communications systems, weapons control and guidance systems, and electronic countermeasures and electronic counter-countermeasures, it is actually about dominating the "electromagnetic space (*dianci kongjian*; 电磁空间)," or electromagnetic spectrum, ranging from super low frequencies to ultraviolet, including the visible light spectrum. [26]

Because electronics are now integrated into the very function of most weapons, electronic warfare now occupies a much more central role in establishing information dominance. Indeed, electronics have assumed a growing proportion of the cost and sophistication of modern weapons; some of the most expensive elements of modern warships and combat aircraft are the onboard electronics, rather than the metal. As one PLA analysis noted, electronics represent 20% of the cost of a modern warship,

[21] "How to Break Network 'Points' in System-of-Systems Operations," PLA Daily (May 2, 2017) http://military.people.com.cn/n1/2017/0502/c1011-29247744.html

[22] BAI Bangxi, JIANG Lijun, "Systems of Systems Conflict Is Not the Same as Systems Conflict," *National Defense Newspaper* (January 10, 2008).

[23] "How to Break Network 'Points' in System-of-Systems Operations," PLA Daily (May 2, 2017) http://military.people.com.cn/n1/2017/0502/c1011-29247744.html

[24] Li Yingming, Liu Xiaoli, et. al., "An Analysis of Integrated Joint Operations," *PLA Daily* (April 12, 2005)

[25] WANG Hui, *Foundational Knowledge, Considerations, and Explanations of Informationized Warfare* (Beijing, PRC: Military Science Publishing House, 2009), p. 180.

[26] All Army Military Terminology Management Commission, *Chinese People's Liberation Army Terminology* (Unabridged Volume), (Beijing, PRC: Military Science Publishing House, 2011), p. 255.

24% of the cost of a modern armored fighting vehicle, 33% of a military aircraft, 45% of a missile, and 66% of a satellite.[27]

As network warfare expands and electronic warfare systems are networked, the Chinese see network warfare and electronic warfare as inextricably linked. Indeed, Chinese military theorists were among the earliest adopters of the concept of "integrated network-electronic warfare (INEW)," and see INEW as a fundamental characteristic of information warfare and the informationized battlefield. [28]

The PLA defines the INEW concept (which it at times translates as "network-electronic integration warfare)" as a form of information warfare where one implements information attacks against the enemy's networked information systems through highly melded electronic warfare and network warfare."[29] It is those information warfare methods that use a combination of electronic warfare and network warfare techniques to attrit and disrupt the adversary's networked information systems, while defending one's own, in order to secure information dominance over the battlefield. For the PLA, INEW is the main expression of information warfare.[30]

As one Chinese analysis notes, in future conflicts, the electromagnetic spectrum will be the key influence upon the operation of network-space, with network and electronic warfare organically linked, operating under a single unified direction.[31] Therefore, network warfare will be affected by efforts aimed at dominating the electromagnetic spectrum, while the ability to operate electronic systems will be directly affected by efforts to penetrate and damage networks. The two elements are seen as mutually complementary in a unified effort to degrade the enemy's system-of-systems. Neither electronic warfare nor network warfare alone can comprehensively disrupt that system-of-systems, but given the mutually supporting nature of the two different types of warfare in terms of attack concepts, attack methods, and operating environments, they constitute a highly effective integrated attack methodology.

One Chinese volume observes:

> From a technical angle, electronic warfare and network warfare can be greatly complementary. Electronic warfare emphasizes attacking the signal layer, with the use of strong electromagnetic energy to drown out target signals. Network warfare emphasizes attacking the information layer, using disruptive information flow, transported into the enemy's network systems, as the means of attack.[32]

[27] WANG Hui, *Foundational Knowledge, Considerations, and Explanations of Informationized Warfare* (Beijing, PRC: Military Science Publishing House, 2009), p. 179.

[28] Academy of Military Science Operations Theory and Regulations Research Department and Informationized Operations Theory Research Office, *Informationized Operations Theory Study Guide* (Beijing, PRC: Military Science Publishing House, November, 2005), p. 101.

[29] All Army Military Terminology Management Commission, *Chinese People's Liberation Army Terminology* (Unabridged Volume), (Beijing, PRC: Military Science Publishing House, 2011), pp. 262-263.

[30] Chinese Military Encyclopedia 2nd Edition Editorial Committee, *PLA Encyclopedia,* 2nd Edition, *Military Command* (Beijing, PRC: China Encyclopedia Publishing House, 2007), p. 327.

[31] YE Zheng, *Concepts of Informationized Operations* (Beijing, PRC: Military Science Publishing House, 2007), p. 157 and YE Zheng, *Science of Information Operations Teaching Materials* (Beijing, PRC: Military Science Publishing House, 2013), p. 27.

[32] YE Zheng, *Science of Information Operations Teaching Materials* (Beijing, PRC: Military Science Publishing House, 2013), pp. 28-29.

In the Chinese view, as individual facilities and their attendant information systems are networked together, the physical infrastructure upon which information passes and the information itself become an integrated whole. INEW is an effort to unify the concrete physical aspects and virtual aspects of information warfare, merging them into a single concept of operations.[33] By undertaking attacks on both of these elements, it is more likely that one can establish information dominance. INEW therefore envisions using electromagnetic attack and defense and information attack as the main techniques for degrading adversary ability to gather and exploit information, treating networked information systems as the domain of operations. Successful conduct of integrated network and electronic warfare should lead to dominance of the entire battlefield information space (*zhanchang xinxi kongjian*; 战场信息空间).

Notably, Chinese INEW targets include key parts of strategic command and control networks. According to one recent PLA textbook, key strike targets (*zhongdian daji mubiao*; 重点打击目标) for INEW include national and military decision-making elements, strategic early warning systems, military information networks, and financial, energy and transportation networks.[34]

The central point of the Chinese conception of INEW is the incorporation of targeting (and defense) of the ***physical element*** of the information networks into network warfare. This is what makes INEW more than simply adding electronic warfare techniques to network warfare; it expands information warfare beyond the predominantly virtual world of data to include the physical, tangible world. In the context of the greater emphasis on unified joint operations, INEW is envisioned as a key example of the new kind of unified jointness necessary to successfully fight informationized local wars.[35]

Indeed, alongside INEW is integrated network and firepower operations. Given the importance of the physical element of information networks, kinetically attacking key information and communications nodes, including server farms and command posts, can potentially disrupt information flow as much as corrupting the data or jamming transmitters and receivers.

Chinese Concepts of Information Deterrence

In addition to fighting and winning future "informationized local wars," the PLA, and the broader Chinese information and network warfare capacity, are charged with effecting deterrent strategies. As with actual conflict, the PRC's concept of deterrence is highly holistic. Beijing has been pursuing "multidomain deterrence" for many years, and information deterrence has long been one element of this broad approach.

According to Chinese analyses, the rapid advances in information technology coupled with globalization have wrought a fundamental shift in the world's socio-economic situation. We now live in the Information Age, with information being the primary currency of international power. "Outer space and information space and network and electromagnetic space have become the new main focal

[33] Academy of Military Science Operations Theory and Regulations Research Department and Informationized Operations Theory Research Office, *Informationized Operations Theory Study Guide* (Beijing, PRC: Military Science Publishing House, November, 2005), p. 101

[34] XIAO Tianliang, Chief Editor, *Science of Military Strategy* (Beijing, PRC: National Defense University Press, 2020), p. 235

[35] YE Zheng, *Science of Information Operations Teaching Materials* (Beijing, PRC: Military Science Publishing House, 2013), p. 28.

points for major powers interested in developing their economy and increasing their comprehensive national power. It has become the new 'high ground' for maintain security."[36]

The growing role of information and associated technologies has led to "information deterrence" becoming a new aspect of deterrence, or *weishe* (威慑). Just as information itself has become an instrument of conflict, the ability to threaten a nation's information systems directly affects societal stability, popular livelihood, and national survival.[37] According to Chinese analyses, "information deterrence" conceptually includes deterrence in the cyber realm, but goes further, encompassing all aspects of information and information operations.

"Information deterrence (*xinxi weishe*; 信息威慑)" is defined in the PLA's terminological reference volume as, "a type of information operations activity in which one compels the adversary to abandon their resistance or reduce the level of resistance, through the display of information advantage or the expression of deterrent/coercive information."[38] As with other PLA writings on deterrence, the Chinese approach to information deterrence does not differentiate between a coercive and a dissuasive effect.

The 2007 edition of the *PLA Encyclopedia* defines "information deterrence" as those activities in which "threats that employ information weapons or which implement information attacks against an opponent, lead to shock and awe and constrain the adversary."[39] Interestingly, this definition notes that "information deterrence" relies in part upon warning an adversary of the serious consequences of an attack (including through demonstration), creating fears that will influence the other side's cost-benefit analysis. The purpose of information deterrence, again, is to allow the deterring side to "achieve a particular political goal (*dadao yiding de zhengzhi mubiao*; 达到一定的政治目标)," ***not*** to prevent the other side from acting in the information domain.

Another Chinese study guide defines it as "a national display of information advantage or the ability to employ information operations to paralyze an adversary's information systems, so as to threaten that adversary. This serves to constrain the other side, as part of the deterrent/coercive goal."[40] What is clear across these various definitions is that "information deterrence," like the broader Chinese conception of deterrence in general, includes both dissuasion and coercion, and embodies the idea of deterring ***through*** information operations, rather than deterring operations ***in*** information space.

Chinese Information Deterrence Activities

From the Chinese perspective, the importance of information in the successful conduct of warfare means that one can also employ threats against the adversary's ability to obtain and exploit information

[36] XIE Xiang, *National Security Strategy Teaching Materials* (Beijing, PRC: Military Science Publishing House, 2013), p. 126.

[37] XIAO Tianliang, General Editor, *The Science of Strategy* (Beijing, PRC: National Defense University Publishing House, 2015), p. 123.

[38] All Army Military Terminology Management Committee, Academy of Military Sciences, *Chinese People's Liberation Army Terminology* (Unabridged Volume), (Beijing, PRC: Military Science Publishing House, 2011), p. 262.

[39] Chinese People's Liberation Army National Defense University Scientific Research Department, *Chinese Military Encyclopedia*, 2nd Edition, *Military Strategy* (Beijing, PRC: Chinese Encyclopedia Publishing House, 2007), p. 283.

[40] AMS Operations Theory and Regulations Research Department and Informationized Operations Theory Research Office, *Informationized Operations Theory Study Guide—400 Questions about Informationized Operations* (Beijing, PRC: Military Science Publishing House, 2005), p. 15.

in order to deter and coerce them. Among states with roughly equivalent levels of information technology, given the widespread penetration of the Internet into all aspects of life, the potential ability to massively disrupt the adversary's entire society provides an opportunity to engage in deterrence. Indeed, on a day-to-day basis, Chinese writings suggest they believe that information deterrence is already in effect among equal players, precisely because the scale of disruption that would otherwise erupt would be enormous, while few states are confident of their ability to avoid such disruptions.[41]

However, where there is a distinct imbalance in information capabilities, it is harder for the weaker side to effect information deterrence. Conversely, the side that may be weaker in terms of conventional military power but who has significant network warfare capabilities may well be able to paralyze and disrupt the more conventionally capable side, and at least impose greater costs, if not actually defeat them.[42]

In the Chinese view, the ability to successfully conduct offensive information operations is therefore the most important means of implementing information deterrence. A demonstrated capability of exploiting information to one's own end, even if not employed, will nonetheless arouse concerns in the adversary. To this end, network offensive power, the ability to conduct effective computer network attack operations is essential, as it is seen as the foundation for information deterrence.[43]

This is in part because computer network attack (CNA) capabilities are relatively inexpensive, yet able to exploit a variety of means of attack, especially since computer networks now permeate so many aspects of society, the economy, and national security. Consequently, there is an unprecedented ability to employ CNA to paralyze and disrupt an adversary across much of its society. Moreover, there is a wide range of capabilities that can be employed, and a variety of vulnerabilities that can be exploited. These elements make network security difficult, both in terms of establishing counters but also establishing attribution.[44]

Consequently, the implicit threat underlying information deterrence is harder to counter than conventional, nuclear, or space deterrence. Indeed, the uncertainty confronting all states even now about the ultimate effect of information operations, and especially attacks against each other's information networks, is believed to be a major factor in forestalling the occurrence of large-scale network conflict.[45]

Chinese analysts seem to believe that this uncertainty creates the opportunity for robust information deterrence. In event of a crisis, PLA analysts suggest that one could remind an adversary of one's ability to plant computer viruses or otherwise undertake information attacks, in order to warn them to

[41] Academy of Military Science Military Strategy Research Office, *The Science of Military Strategy* (Beijing, PRC: Military Science Publishing House, 2013), p. 196.

[42] Academy of Military Science Operations Theory and Regulations Research Department and Informationized Operations Theory Research Office, *Informationized Operations Theory Study Guide* (Beijing, PRC: Military Science Publishing House, November, 2005), pp. 15-16.

[43] Academy of Military Science Operations Theory and Regulations Research Department and Informationized Operations Theory Research Office, *Informationized Operations Theory Study Guide* (Beijing, PRC: Military Science Publishing House, November, 2005), p. 15.

[44] XIAO Tianliang, General Editor, *The Science of Strategy* (Beijing, PRC: National Defense University Publishing House, 2015), p. 123.

[45] Academy of Military Science Military Strategy Research Office, *The Science of Military Strategy* (Beijing, PRC: Military Science Publishing House, 2013), p. 190.

cease and desist their resistance. At a minimum, such moves are considered likely to affect the adversary's will to fight.

At the same time, a clearly demonstrated ability to defend and safeguard one's information resources and systems can also serve to deter an adversary. If the adversary is unable to successfully attack one's information systems, then their ability to establish information dominance is likely to be extremely limited. In which case, their ability to establish dominance over other domains (e.g., air, space, maritime) is also likely to be very constrained, reducing their chances of successfully achieving whatever strategic objectives they might have. Under such circumstances, the adversary is likely to be deterred from initiating aggression, or may be coerced into submitting.

A Possible Information Deterrence Ladder

Given Chinese writings about deterrence activities in the space and nuclear domains, it is possible that there is a "deterrence ladder" for information operations. Chinese writings suggest such a construct is indeed being explored.[46] One article by a PLA expert from the Chinese military's Academy of Military Sciences lays out such a conceptual ladder for information deterrence.[47]

- *Deterrence through network technology experimentation* (*wangluo kongjian jishu shiyan weishe*; 网络空间技术试验威慑) The first, basic step for information deterrence is to undertake testing and development of new technologies associated with network warfare. This includes cyber weapons, but also new offensive methods and tactics. As important, one should allow such efforts to be revealed through the media, thereby informing the rest of the world of one's capabilities. A strong foundation in information technology and training is essential. As important, because of the rapid pace of development in this field, new breakthroughs may occur at any time; uncertainty about that can also support deterrent policies.
- *Deterrence through network equipment displays and demonstrations* (*wangluo kongjian zhuangbei zhanshi weishe*; 网络空间装备展示威慑) Where the first step of information deterrence is demonstrating technological capabilities, the second step involves demonstrating a broader array of network warfare capabilities, including equipment development plans, prototype testing, and equipment production. This approach will deliberately reveal to an adversary China's overall capabilities (rather than individual pieces of equipment or programs), as well as demonstrate that they are part of a broader, integrated development effort. Specific elements of this rung include the publication of white papers (such as the Chinese defense white paper), newspaper and magazine articles, and other official releases of information.
- *Deterrence through network operational exercises* (*wangluo kongjian zuozhan yanxi weishe*; 网络空间作战演习威慑). Simply displaying network capabilities, and discussing them, may not deter a potential adversary. The next rung on the Chinese information deterrence ladder is therefore to undertake operational exercises. This can involve forces deploying and operating in a real environment or a simulated one. The article suggests that public exercises involving forces in the field are typically defensive, while more offensive operations are undertaken in simulated environments, such as national cyber test ranges. The article specifically mentions the American "Schriever" space wargames as an example of how the United States displays and develops network warfare capabilities and signals its resolve to employ them.

[46] All references in this section, unless otherwise noted, are drawn from Yuan Yi, "AMS Expert Discloses Network Space Deterrence," China Military Web (January 6, 2016), http://news.xinhuanet.com/mil/2016-01/06/c_128599390.htm

[47] The People's Liberation Army Academy of Military Science is the leading brain trust for the PLA. It is comparable to a combination of the RAND Corporation, the US Army's Training and Doctrine Command (for the entire PLA), the Inspector General directorate, and some aspects of the Command and General Staff College (for the entire PLA).

- *Deterrence through actual network operations* (*wangluo kongjian zuozhan xingdong weishe*; 网络空间作战行动威慑). In both the nuclear and space contexts, the highest level of deterrent action is the actual employment of nuclear and space capabilities respectively, intended to signal an adversary the critical nature of the situation, and to demonstrate resolve. As important, employment of such weapons can affect the initial campaign, if the target is sufficiently valuable. This article suggests a similar mindset may exist for information deterrence, i.e., that the highest rung would be the employment of actual network warfare capabilities against an adversary's systems. This might involve a direct attack against key adversary networks, in order to preempt an enemy attack, or in response to an adversary's probe, as retaliation (and a demonstration of capability). The articles provided by the article suggest a more psychological focus, as they include disrupting email networks, generating a flood of text messages, and attacks against the power grid.

Interestingly, in the 2020 edition of the PLA National Defense University's *Science of Military Strategy*, network deterrence is described as primarily comprising strategic-level network deterrence (*zhanlue ji wangluo weishe*; 战略级网络威慑) and tactical-level network deterrence (*zhanshu ji wangluo weishe*; 战术级网络威慑).[48] The former is about displaying network offensive capabilities that could disrupt an adversary's key strategic networks, including political, economic, and military targets. Specific examples cited include the adversary's C4ISR networks, national transportation nodes, and national communications networks. By displaying the ability to strike an enemy's strategic targets, the expectation is that the enemy will be dissuaded from proceeding.

Tactical level network deterrence, on the other hand, is apparently primarily oriented towards discouraging criminals, hackers, and other lower-scale threats from operating, thereby maintaining the stability and operability of one's networks in peacetime.

It is important to keep in mind that in all these discussions, information deterrent activities are not occurring in isolation, but would be coordinated with a host of comparable activities in other domains and fields. These would involve not only military forces (e.g., naval exercises, space exercises), but also diplomatic and political pronouncements, economic measures, etc. This is especially likely to be the case at the higher rungs on the ladder.

At the same time, however, because China confronts a variety of potential adversaries, its leaders must constantly strive to engage in multilateral deterrence. Therefore, the Chinese leadership may not necessarily engage only in deterrent activities against, say, the United States or Japan, even in the midst of a crisis with those states. Heightened operations or limited offensive information operations, in the deterrent context, may be undertaken against third parties, both in order to demonstrate capability and resolve against the main target, but also to signal those third parties (and others) that China has sufficient capability to degrade them as well.

* * * * * * * * * * * * * * * * * * *

[48] XIAO Tianliang, Chief Editor, *Science of Military Strategy* (Beijing, PRC: National Defense University Press, 2020), p. 152.

Program revenue and other income 14%

The top five corporate givers provided The Heritage Foundation with 1% of its 2020 income. The Heritage Foundation’s books are audited annually by the national accounting firm of RSM US, LLP.

OPENING STATEMENT OF JOHN CHEN, LEAD ANALYST, CENTER FOR INTELLIGENCE AND RESEARCH ANALYSIS, SOS INTERNATIONAL (SOSi)

CHAIRMAN WONG: Thank you, Mr. Cheng.

Let's turn to John Chen.

MR. CHEN: Good morning, Co-Chair Wong, Co-Chair Bartholomew, members of the Commission, and Commission staff. Thank you for inviting me to appear before you today. I've been asked to speak about China's military capabilities for cyberwarfare with a focus on the organization, command and control, and capabilities of the People's Liberation Army's Strategic Support Force, or SSF.

Before I wade into the details though, I'm going to frame my remarks by briefly revisiting the May 2021 Colonial Pipeline cyber-attack, so apologies in advance for making everyone relive that trauma.

The pipeline's computerized equipment fell victim to a ransomware attack that forced the pipeline to shut down. And I think everyone remembers the panic buying and the lines of cars at gas stations and all the people learning firsthand about the corrosive properties of gasoline while storing it in plastic bags.

Now imagine if that cyber-attack was perpetrated by a determined and well-resourced state adversary with advanced cyber capabilities and that the panic that had ensued had been deliberately encouraged or boosted by a concerted disinformation effort saturating social media, perhaps during election season as an October surprise. Without overstating that scenario, I think we can all agree that the Colonial Pipeline attack could have been much worse. It is the SSF's job to make exactly these kinds of scenarios much worse in a conflict.

Formed during the PLA's sweeping 2016 reforms by combining cyber intrusion, psychological warfare, and space information units under a single organizational umbrella, the SSF is charged with achieving information dominance on the battlefield. More specifically, high-level PLA writings and features of the SSF's organization and command and control suggest a strong emphasis on using multiple cyber means to achieve political effects against an adversary.

For context, the SSF is one of several agencies of the Peoples Republic of China carrying out cyber activities ranging from defensive network monitoring and censorship to cyber intrusions and espionage, all the way up to cyberwarfare operations. These activities are generally carried about by the Ministry of Public Security, Ministry of State Security, and the SSF, respectively, though there is considerable overlap as today's other speakers will likely attest.

All of these actors nominally report to a group of centralized Chinese Communist Party bureaucracies, all headed by Xi Jinping. The SSF is distinct from its sister agencies, though, in that it alone has an acknowledged mandate to prosecute cyberwarfare, roughly defined as the use of cyber methods to generate effects against an adversary as part of a conflict.

This mandate is expressly strategic and its primary objective is political. Strategic SSF missions target political, economic, social, and financial infrastructure using cyber-enabled methods to generate political outcomes favorable to the CCP. These extremely sensitive missions are nominally to be prosecuted only at the behest of the CCP's top leadership.

The SSF is organized and commanded accordingly. Its network warfare elements are arranged in something of a bifurcated structure with a high degree of centralized control. Some portion of its most capable cyber organizations, commonly attributed as advanced persistent threats, are centrally commanded, organized as bases and bureaus directly reporting to the SSF's high command and the Central Military Commission.

Other technical reconnaissance bases commanding lower-level brigades and detachments appear to have regional affiliations corresponding with the PLA's five theater commands, but may also be subject to varying degrees of central control.

The SSF has also incorporated psychological warfare units into its organization, as my fellow speaker Dean mentioned, which gives that force an organic ability to carry out public opinion, psychological, and legal warfare as part of a propaganda Three Warfares Campaign. Though the exact chain of command for these units remains unclear, these formations are likely directed at the highest levels of command as their operations require consensus within the PLA's political work apparatus.

This combination of network and psychological warfare units is not a coincidence and offers Xi Jinping a potent combined or boosted cyberwarfare capability in the SSF. On their own, cyber-attacks can deny, disrupt, degrade, or destroy critical infrastructure, while psychological operations like disinformation campaigns can seriously undermine an adversary's civil society. When employed together, however, these two capabilities could trigger a chain reaction of political and social effects resulting from human reactions to fear or uncertainty as we imagined earlier in our call back to Colonial Pipeline.

Success in these boosted combined operations depends on experienced planners, deep cultural expertise, smooth inner agency coordination, and exceptional trust and flexibility to adapt that operation on the fly.

While these reforms that created the SSF have begun to address some of these needs, it's not yet clear that the SSF can successfully pull off such a boosted campaign. For one, tight central control could reflect a lack of trust and seriously hinder the SSF's ability to coordinate strategic effects with the rest of the CCP's inner agency.

On top of that, the PLA's entire political work system was rebooted during the reforms. Has it recovered enough to successfully guide a demanding boosted operation? Maybe, but maybe not. Either way, it would be imprudent to count on possible SSF deficiencies as a bulwark against this kind of threat. Many experts rightly suggest measures to improve network security, but the U.S. Government must also defend the human terrain where these boosted operations can do much deeper damage.

In the short term, mandating the creation of an easily comprehensible, maybe a color-coded early warning system, would sensitize the public to forthcoming boosted attacks and allow the U.S. Government to slow down or disrupt the chain reaction of negative social effects.

In the medium term, increased civil defense outlays would familiarize emergency services and the general population with best practices in the event of critical infrastructure attacks.

Over the longer term, more robust funding for public affairs and transparency efforts would help blunt the impacts of a concerted disinformation campaign.

I want to wrap up by just foot stomping one point from above, which is that cyberwarfare is much more of a human endeavor than it usually gets credit for. The network compromises that enable cyberwarfare effects occur because somewhere somehow a human made a mistake, whether by opening the wrong attachment, or plugging in a flash drive, or overlooking a software flaw. It's fitting then that the most consequential impacts of a cyber-attack are not on the network itself, but are instead derived from the human reactions to the attack.

So I think we all recognize that the measures I've suggested are far from sufficient to neutralize the threat of a boosted attack, but they are worthwhile points for consideration to help mitigate the potential impacts of a serious cyber-attack in the future.

Thank you all very much for your time and I'm looking forward to the discussion ahead.

PREPARED STATEMENT OF JOHN CHEN, LEAD ANALYST, CENTER FOR INTELLIGENCE AND RESEARCH ANALYSIS, SOS INTERNATIONAL (SOSi)

EXOVERA

CIRA

CENTER FOR INTELLIGENCE
RESEARCH AND ANALYSIS

Testimony Before the U.S.-China Economic and Security Review Commission

Hearing on “China’s Cyber Capabilities: Warfare, Espionage, and Implications for the United States”

Thursday, February 17, 2022

John Chen
Lead Analyst
Center for Intelligence Research and Analysis
Exovera

Introduction

The People's Republic of China (PRC) has worked steadily to improve its capabilities for cyberwarfare over the past decades, especially within the armed wing of the ruling Chinese Communist Party (CCP), the People's Liberation Army (PLA). The PLA's Strategic Support Force (SSF) is a direct beneficiary of those efforts. Formed during the sweeping 2016 reorganization of the PLA, the SSF has the mandate, the organization, and the combined capabilities to prosecute layered strategic cyberwarfare operations to deny, destroy, disrupt, and degrade an adversary's critical infrastructure in pursuit of broader political and societal effects. PLA theorists have extolled the virtues of combining multiple different types of information operations in strategic cyberwarfare, and the SSF's organization combines cyber intrusion and espionage forces with psychological operations units accordingly to field a more effective force capable of waging and winning a modern conflict.

This testimony reviews the PRC's military capabilities for cyberwarfare, focusing on the organizational features and capabilities of the SSF. It begins with an overview of the PRC's main cyber actors and command authorities, before proceeding to a description of the SSF's organization and command and control. It then describes some of the SSF's emerging capabilities for both cyberwarfare and psychological operations and concludes with a brief discussion of recommendations for mitigating this threat.

The PRC's Cyber Actors

The PRC relies upon a vast constellation of bureaucracies to carry out its state-sponsored cyber operations. Among the most prominent of these are three civilian and military organizations: the Ministry of Public Security (MPS), the Ministry of State Security (MSS), and the People's Liberation Army's Strategic Support Force ((战略支援部队; SSF). The Ministry of Public Security (MPS)'s provincial Network Security Protection Detachments (网络安全保卫总队), for instance, secure the PRC's domestic network infrastructure by looking for intrusions and investigating internet crimes, the latter of which includes removing what the Chinese Communist Party (CCP) deems "harmful information."[1] The MSS runs cyber-enabled espionage and counter-espionage operations against all manner of foreign government agencies, companies, and dissidents through its provincial departments (国安厅), supported by penetration testers and tool developers housed within the various provincial and functional offshoots of its central-level 13th Bureau, otherwise known as the China Information Technology Evaluation Center (中国信息安全测评中心; CNITSEC).[2] For its part, the SSF prosecutes strategic information support and information operations to secure information dominance and enhance the PLA's ability to fight and win a modern war.[3]

Other agencies are charged with developing the infrastructure, human capital, and technology necessary for their sister organizations to do their work. The Ministry of Industry and Informatization Technology (工业和信息化部; MIIT) and its State

Administration of Science, Technology, and Industry for National Defense (国家国防科技工业局; SASTIND) together orchestrate a vast effort to equip the PRC's cyber agencies with leading-edge technology and supply them with elite talent. Perhaps the most visible aspect of this mission the MIIT and SASTIND administration of a web of research universities with close ties to the PRC's defense industry, including the so-called Seven Sons of National Defense (国防七子).[4]

At the apex of this cyber officialdom is a cluster of leadership organs responsible for directing and coordinating activities in the cyber domain according to the wishes of the PRC's highest leadership. The Central Military Commission (中共中央军事委员会; CMC) oversees the activities of the PRC's military cyber forces, namely the SSF.[5] The CCP Central Committee's Network Security and Informatization Commission (中共中央网络安全和信息化委员会) takes an expansive view of its remit to secure CCP rule by governing both cultural and technical aspects of information security, and acts through its associated office (办公室), which is also known by its equivalent state moniker the Cyberspace Administration of China (国家互联网信息办公室; CAC).[6] The CCP Central Committee's National Security Commission (中共中央国家安全委员会, NSC), a more opaque organizational actor, is likely also involved in directing the PRC's cyber activities to head off emerging national security threats.[7] Each of these bodies are headed by Xi Jinping, illustrating the emphasis with which Xi and the CCP view cyber activities in the context of regime and national security.

SSF Organization and Command and Control

Of the various PRC actors carrying out cyber operations, however, only the SSF has an openly acknowledged mandate to generate effects using the cyber domain expressly to win a conflict with a nation-state adversary. PLA theorists argue that the strategic cyberspace operations to be executed by the SSF are meant to affect an adversary's politics, economy, science and technology, culture, and foreign affairs.[8] Specifically, instructors from the SSF Information Engineering University and the PLA Academy of Military Sciences note that strategic cyber (or network) warfare is directed at the stability of an adversary's sovereignty and governance system, with clear political objectives that transcend the mere destruction or weakening of an opponent's military capability. To that end, they also argue that this strategic cyber warfare should focus on a wide range of targets in pursuit of desired political effects, including economic, political, and societal networks, as well as critical information infrastructure that supports a population's livelihood like the finance, transportation, and electrical power sectors.[9]

The far-reaching ramifications associated with this brand of strategic cyber warfare suggest that the SSF should answer to a highly centralized, tightly held civilian command authority. PLA instructors argue that strategic cyber warfare is a "severe escalation of interstate conflict (国家冲突严重升级)" concerning the overall national strategic situation, to be employed only when diplomatic, economic, and other methods are not effective. As a result, the ultimate decision authority to undertake strategic cyber warfare should only reside at the highest level of national civilian leadership, rather than with military command (由国家最高领导层而非军方掌控),[10] which places Xi Jinping firmly as the final arbiter of strategic cyberwarfare operations. While the SSF's most potent cyberwarfare formations, namely technical reconnaissance bureaus with advanced persistent threat (APT) capabilities subordinate to the SSF Network Systems Department, frequently target defense industry, media, telecommunications, and other organizations to support the PRC's peacetime cyber and economic espionage campaigns,[11] they would likely prosecute more sensitive missions against political or infrastructural targets at the sole behest of Xi Jinping through the CMC, in keeping with the desire for tight, centralized control over these capabilities.[12]

The SSF's civilian master theoretically commands a sprawling array of diverse organizational assets amalgamated specifically to meet the wide-ranging demands of achieving strategic effects against an adversary in cyberspace. PLA instructors prize the integration of multiple cyber-related disciplines within a strategic cyber force, writing that a convergence of intelligence collection, public opinion warfare, and psychological warfare forces is necessary to field a "combined national force" (国家合力) that can prevail in all-out conflict.[13] Many of these theoretical postulates are borne out in the SSF's force structure: the SSF's cyber forces come in a bewildering variety of flavors. The SSF's Network Systems Department likely oversees and supports centrally-led bases (基地) and bureaus (局) for psychological warfare (311 Base) and network intrusions, regionally-aligned (and possibly Theater Command affiliated) technical reconnaissance bases overseeing administrative divisions (处) and offices (科) as well as operational detachments (大队) and teams (队), and apparently jointly-manned electronic warfare and information communications brigades (旅).[14] The SSF can call upon regular, uniformed military organizations with a variety of service affiliations to execute cyberwarfare missions at strategic, operational, and tactical levels of conflict.

Beyond regular military assets, the SSF also avails itself of civilian resources to accomplish its objectives. Much of this activity can be grouped under military-civil fusion (MCF) efforts to develop and obtain cutting edge technologies. For instance, the SSF's Network Systems Department is a stakeholder in drafting technical standards with dual-use applications,[15] and its technical personnel regularly confer with academics and defense industry researchers to discuss best technical practices.[16] Researchers at the SSF Information Engineering University (SSF-IEU), a premier SSF training ground for its network warfare personnel, work with counterparts at MIIT-run universities on information security topics, among other collaborators and subjects.[17] When domestic MCF efforts prove insufficient to the tasks at hand, SSF units are not shy about procuring Western and other foreign products like antivirus software to support their efforts.[18]

The SSF's cyber forces also lean heavily upon civilian society to staff their ranks. Though it draws much of its human capital from PLA educational institutions like SSF-IEU, the SSF's cyber warfare component (through its pre-reform predecessor the 3PLA) also has a long history of recruiting technical talent from the PRC's top academic institutions, through special programs, rotational commitments from undergraduate students, and specialized information security competitions.[19] The SSF is also primed to take advantage of the new civilian personnel (文职人员) recruitment system that has replaced the occasionally maligned civilian cadre (文职干部) system.[20] When it is comparatively less able to exploit talent from top universities thanks to competition from the MSS, the SSF can also make use of part-time militia and reserve units, which are typically comprised of civilian personnel from government agencies like MIIT, MPS, and MSS, as well as academic researchers and specialists from state-owned telecoms and other private corporations.[21] In other, unspecified circumstances, the SSF may call upon "authorized forces" (授权力量) drawing from similar civilian entities to augment its capabilities, though details on the logistics and employment of these forces remain elusive.[22]

The SSF's ability to generate its desired effects in cyberspace is therefore reliant upon a well-coordinated but highly centralized command infrastructure capable of wielding both PLA and civilian assets for strategic cyberwarfare missions. PLA-authored texts depict notional coordination responsibilities between the SSF and its sister agencies, with central and local CAC, MPS, and MSS organizations coordinating their activities with strategic SSF components operating under the direct command of the CMC.[23] These support and coordination mechanisms are meant to ensure that the PRC's various cyber actors act in concert when strategic cyberwarfare is underway.

The SSF defied easy comparison to U.S. cyber forces when it was first stood up as part of the 2016 PLA reforms, but recent changes suggest that the SSF may be taking on organizational features more familiar to U.S. observers. For instance, analysts initially characterized the SSF as a distinct military quasi-service with some similarities to U.S. Strategic Command (USSTRATCOM), U.S. Cyber Command (USCYBERCOM), and eventually the U.S. Space Command (USSPACECOM).[24] In some ways, these comparisons still hold true: the SSF's Network Systems Department carries out many of the same functions that USCYBERCOM does, while the SSF's control over military space assets are somewhat similar to the responsibilities held by USSTRATCOM and USSPACECOM. The recent appearance of jointly manned SSF formations, however, could indicate that the organization is inching towards becoming a joint force command rather than a dedicated, distinct military service: the SSF apparently draws personnel from multiple PLA services, including the Air Force and Navy.[25]

The plainest and arguably most consequential difference between the SSF and U.S. cyber forces, however, is that the SSF is organized as the single, unified force within the PLA for seizing and maintaining information dominance, combining space, long-range technical sensing, cyber intrusion, and psychological warfare capabilities into a single force. This combination profoundly shapes the character of the cyberwarfare threat the SSF poses to the United States, as described below.

A "Boosted" Threat Profile

Assessing the SSF's cyberwarfare capabilities is difficult, as operational secrecy is a vital determinant of the effectiveness of cyber intrusions, online influence operations, and other information warfare capabilities. Nevertheless, the SSF's reliance on civilian personnel and infrastructure means that some of its researchers publish their work in academic and technical fora. These works can shed light on topics of interest within the SSF's cyber forces, giving observers a sense (however limited) of the SSF's peacetime cyber activities and its priorities in offensive and psychological operations.

In peacetime, the SSF engages in substantial information security research, occasionally of an obvious defensive bent, though much of this work is inherently dual use. In 2019, one SSF researcher specializing in industrial control systems published research on defensive methods that could be used to detect intrusions in electrical power infrastructure—a topic with clear offensive implications in attacking an adversary's systems.[26] Others specialize in studying methods for monitoring social media: over the last four years, SSF-IEU graduate students have studied spambot detection,[27] user identification across different social media networks, [28] and algorithmic detection of social media communities,[29] topics with cited applications for monitoring the PRC's domestic information environment during peacetime but also obvious applications for influencing foreign social media environments.

Decades of sustained investment, a seemingly endless trail of carnage left in the wake of cyber intrusions attributed to the SSF, and a robust research ecosystem supporting the development of tactics, techniques, and procedures (TTPs) indicate that the SSF's offensive cyberwarfare capabilities are formidable and improving. Perhaps one of the more significant indicators of the SSF's attempts to improve its TTPs is its persistent and progressively advancing interest in algorithmic research to support automation in its cyber intrusion methods. SSF-IEU researchers, for example, are apparently actively working on applying adversarial machine learning to cyber intrusion techniques. The academic works of one research cluster demonstrates a typical pattern of research and development surrounding these techniques: in 2019, SSF-IEU researchers surveyed adversarial example generation techniques for malware [30] and by September 2020, had demonstrated a publishable technique for spoofing network traffic using adversarial examples.[31]

While far less is publicly known about the SSF's capability for waging psychological warfare, evidence suggests it is also working to adapt machine learning and artificial intelligence to enhance social media influence operations. In 2016, a former SSF-IEU professor moved to a university run by the United Front Work Department, known for its overseas influence operations, and began publishing a series of articles on automated models for propagating propaganda messages as part of a broader psychological warfare campaign. His co-author was a researcher from the PLA 61716 Unit, also known as the 311 Base specializing in psychological operations.[32] Others have contributed to a large existing body of work on sentiment analysis in foreign languages, including a March 2021 article analyzing the tweets of selected U.S. cabinet members, members of Congress, and governors.[33] While these studies do not explicitly describe offensive applications of their research findings as part of a sustained campaign of online psychological warfare, they provide insights into areas of interest for the SSF's cyber operators.

Though SSF advances in each of these respective fields of information operations merit close observation, the potential use of these distinct types of operations together as part of a sequence of attacks may be much more effective than their application alone. When executed with the appropriate timing, combining different kinds of information operations like cyber intrusions and psychological operations can amplify or "boost" the effects of an initial network compromise and subsequent attack, generating fear, uncertainty, and doubt that can set off chain reactions and larger political consequences.[34] For instance, a single hypothetical cyberattack on Taipei's subway infrastructure could shut down popular transit lines, while a discrete social media influence campaign accusing subway officials of corruption could trigger outcry and political pressure among an engaged public. Launching intermittent cyberattacks against subway infrastructure amid a sustained online influence campaign tarnishing public transit officials during election season, however, would not only destroy hard infrastructure, but also undermine public confidence in a fare-dependent subway system, cratering its revenues and delaying needed repairs. The resultant public outcry over degraded service and perceived corruption could also trigger political repercussions at the polls. In examples like these, human cognition and responses are more important targets for SSF cyber operations than any network infrastructure.

The PLA's theoretical views of strategic cyberwarfare and the mixture of capabilities and responsibilities housed within the SSF's cyber forces suggest a strong emphasis on this kind of "boosted" or amplified *modus operandi*. SSF and PLA theorists focus not only on the development of technical capabilities, but also on the seamless application of multiple technical means to generate political effects far more consequential than the mere hacking of network infrastructure. Some note this emphasis explicitly, stating that strategic cyberwarfare is aimed at "a society's psychological and political system," and that the integration of "Three Warfares" specialists with technical network personnel to carry out public opinion warfare, psychological warfare, and legal warfare will only increase in pace and scope in the future.[35]

Key Determinants and Implications

The success and effectiveness of the SSF's cyber forces depend on several key determinants, some of which were direct results of the sweeping 2016 reforms of the PLA. As reforms were underway to enhance the Party center's (read: Xi Jinping) control over the PLA,[36] the official narrative surrounding the SSF made clear that it and its assets were to be controlled primarily by the CMC. This tightly held control could bear fruit for the PRC's leaders in a conflict by funneling all strategic reconnaissance information and sensors to a single centrally controlled organization, which could theoretically engender greater peacetime control over PLA activities. Closeness to the Party center could also improve coordination between the SSF and the PRC’s other cyber actors. On the other hand, however, this tight central control could severely hamstring military operations by forcing PLA Theater Commanders to rely on the CMC to access the SSF’s strategic reconnaissance capabilities. This conundrum has likely been partially resolved with the establishment of regionally aligned SSF technical reconnaissance bases, but the concentration of strategic cyber reconnaissance and warfare capabilities at the center may yet hinder the PLA’s ability to fight and win a modern conflict.

A second determinant of success was also precipitated by the 2016 reforms. The consolidation of disparate cyber intrusion and espionage units with psychological warfare formations under the SSF may improve its ability to plan and prosecute “boosted” strategic information operations for favorable political effect. The integration of psychological operations units with cyber forces as part of the 2016 PLA reform effort to build a more unified force for information warfare, and the SSF’s gradual embrace of a joint force construct will likely provide more routine and diverse planning opportunities for “boosted” strategic cyberwarfare activities. On the other hand, this integration almost certainly kicked off organizational disruptions and bitter bureaucratic rivalry between PLA services that did not want to surrender their cyber forces to another organization.

Better planning and smoother operations aside, the effectiveness of “boosted” cyberwarfare is dependent upon effective political work. The ability to quickly agree upon the desired political outcomes of a conflict and empower trusted actors to achieve these goals is vital for a successful “boosted” cyberattack. Unfortunately for Xi Jinping and the Party center, the PLA’s pre-2016 political work system was not exactly a paragon of a healthy and effective principal-agent relationship.[37] The degree to which the 2016 reforms were able to rehabilitate political loyalty to the Chinese Communist Party within the PLA will be a key determinant for success in using cyber operations to achieve favorable political outcomes.

Beyond the changes set in motion by the 2016 reforms, the SSF’s success will also depend in large part on its ability to effectively access civilian resources, but the jury is still out on this factor. While the SSF surely makes successful use of its civilian talent and infrastructure, some of this capability is manifested in legal mechanisms with decidedly mixed or unclear results. For instance, legal justifications for commandeering data and processing capabilities stemming from the PRC’s National Intelligence Law are reportedly wielded frequently by state authorities but generate dissatisfaction among private sector employees,[38] while the legal pathways (and effectiveness) for using “authorized forces” remain unclear. Compounding the problem, the SSF’s cyber militias and reserve units have not necessarily acquitted themselves well, lacking sufficient talent and struggling to integrate into operational-level exercises.[39]

Recommendations

The PRC boasts a vast array of highly capable cyber actors, each with distinct responsibilities and missions. Perhaps the most potent actor in the PRC's cyberwarfare activities is the SSF, which is organized and equipped to execute layered, "boosted" information operations against an adversary's society to generate political effects that can lead to victory in a conflict. While many experts rightly suggest measures to improve network security as a counter to cyberwarfare threats, the U.S. government will also need to assure societal resilience and better defend the human terrain upon which the SSF will attempt to create its most damaging effects. Congress can begin to address this threat in the following ways:

- **Establish an integrated public early warning capability.**

Congress should direct the Department of Homeland Security and other interagency partners to develop a public alert system for describing information operations level of threat to the nation. This system should include warnings about state-directed disinformation efforts and work in close cooperation with warning efforts about cyber intrusions generated by National Cyber Awareness System. A transparent, easily comprehensible, and discrete assessment of the information operations threat level against the United States could activate additional resources for information security and sensitize the public to the likelihood of specific disruptions to their communities, enabling better advance preparation and incident response.

- **Promote public affairs and civil defense outreach efforts.**

Congress should direct funds to local and state governments to improve both public communications capabilities to debunk or "pre-bunk" misinformation, as well as civil defense preparedness if cyberattacks destroy or degrade critical infrastructure. More frequent training exercises and distribution of emergency preparedness information, especially during times of heightened alert, can blunt the broader societal impact of "boosted" information operations.

- **Fund transparency, media literacy, and fact-checking partnerships in civil society.**

Congress should provide grant funding to non-governmental organizations to detect, label, debunk, or "pre-bunk" state-directed disinformation efforts. Think tanks, academic institutions, non-profits, community associations, and other organizations working to expose online influence operations can mitigate the impacts of a sustained state-backed disinformation campaign.

[1] For one example of provincial detachment responsibilities, see “Henan Provincial Public Security Department Network Security Protection Detachment [河南省公安厅网络安全保卫总队], Zhengzhou City Internet Crime and Harmful Information Reporting Platform [郑州市互联网违法和不良信息举报平台], June 24, 2016, http://www.zhengzhoujubao.com/detail.aspx?id=1477

[2] The Guangdong Information Technology Security Evaluation Center [广东信息安全测评中心] is one example of a provincial counterpart to the central CNITSEC. See Insikt Group, “Recorded Future Research Concludes Chinese Ministry of State Security Behind APT3,” May 17, 2017, https://www.recordedfuture.com/chinese-mss-behind-apt3/.

[3] John Costello and Joe McReynolds, “China’s Strategic Support Force: A Force for a New Era,” *China Strategic Perspectives* 13 (NDU Press: Washington, D.C.), pp. 35-44.

[4] Australian Strategic Policy Institute, “China Defence Universities Tracker,” accessed on February 6, 2022 at https://unitracker.aspi.org.au/.

[5] John Costello and Joe McReynolds, “China’s Strategic Support Force: A Force for a New Era,” *China Strategic Perspectives* 13 (NDU Press: Washington, D.C.), p. 1.

[6] For a discussion of the CAC’s expanding roles, see Jamie Tarabay and Coco Liu, “Obscure Cyber Agency Becomes Nemesis of China’s Tech Giants,” Bloomberg, July 13, 2021, https://www.bloomberg.com/news/articles/2021-07-13/xi-elevates-an-obscure-china-regulator-to-take-on-didi-big-tech.

[7] Joel Wuthnow, “A New Chinese National Security Bureaucracy Emerges,” *China Brief* Vol. 21, no. 23, November 23, 2021, accessed at https://jamestown.org/program/early-warning-brief-a-new-chinese-national-security-bureaucracy-emerges/.

[8] John Chen, Joe McReynolds, and Kieran Green, “The Strategic Support Force: A “Joint” Force for Information Operations,” in Joel Wuthnow et al., eds., *The PLA Beyond Borders* (NDU Press: Washington, D.C., 2021), p. 154.

[9] Li Jidong [李继东] and Chen Zhou [陈舟], “On Strategic Cyber Warfare [试论战略网络战],” *China Military Science* 2017, no. 6, p. 47. Li is an instructor at the SSF Information Engineering University, and Chen Zhou is a researcher at the Academy of Military Sciences Warfare Research Institute.

[10] Ibid.

[11] For examples, see Mandiant, “APT1: Exposing One of China’s Cyber Espionage Units,” February 19, 2013, and Crowdstrike, “Putter Panda,” available at https://cdn0.vox-cdn.com/assets/4589853/crowdstrike-intelligence-report-putter-panda.original.pdf.

[12] For theoretical explications of how this chain of command might work, see Wang Jinsong [王劲松], Wang Nanxing [王南星], and Ha Junxian [哈军贤], “Research on Cyberspace Operational Command System” [网络空间作战指挥体系研究], *Journal of Academy of Armored Force Engineering* [装甲兵工程学院学报], no. 5 (2016), p. 3., and Fan Yongtao [樊永涛], Wang Jinsong [王劲松], and Li Shikai [李世楷], “Problems and Solutions to the Cyberspace Operational Command Pattern” [网络空间作战指挥方式面临的问 题及对策], Journal of Academy of Armored Force Engineering, no. 5 (2017), 9.

[13] Li Jidong [李继东] and Chen Zhou [陈舟], “On Strategic Cyber Warfare [试论战略网络战],” *China Military Science* 2017, no. 6, p. 47.

[14] See John Chen, Joe McReynolds, and Kieran Green, “The Strategic Support Force: A “Joint” Force for Information Operations,” in Joel Wuthnow et al., eds., *The PLA Beyond Borders* (NDU Press: Washington, D.C., 2021), p. 166, and Kaifeng City Education Bureau [开封市教育局], “2017-2020 List of National Group Physical Education Advanced Units [2017-2020 年度全国群众体育先进单位名单],” September 26, 2021.

[15] Standards Administration of China [国家标准化管理委员会] and Central Military Commission Equipment Development Department [中央军委装备发展部], “Notice Regarding Specifications for Drafting Process of National Military-Civilian Dual-Use Standards [关于规范军民通用的国家标准制定程序的通知],” December 22, 2020, https://gkml.samr.gov.cn/nsjg/bzjss/202012/W020201230622946248292.pdf.

[16] “Military Measurement Unified Textbook Seminar Convenes at China Jiliang University [《军事计量统编教材》研讨会在我校召开],” China Jiliang University [中国计量大学], January 16, 2017, http://www.hmscxh.com/info/1133/10463.htm.

[17] For one example, see Yuan Qingjun [袁庆军] et. al., “An Improved Template Analysis Method Based on Power Traces Preprocessing with Manifold Learning [基于流形学习能量数据预处理的模板攻击优化方法],” *Journal of Electronics and Information Technology 电子与信息学报* 42, no. 8, pp. 1853-1861.

[18] Insikt Group, “China’s PLA Unit 61419 Purchasing Foreign Antivirus Products, Likely for Exploitation,” Recorded Future, May 5, 2021, https://www.recordedfuture.com/china-pla-unit-purchasing-antivirus-exploitation/.

[19] Joe McReynolds and LeighAnn Luce, “China’s Human Capital Ecosystem for Network Warfare,” in Roy Kamphausen, ed., *The People in the PLA 2.0* (Carlisle: PA, 2021), pp. 361-364.

[20] Ibid., p. 355

[21] Zuo Juan [左娟] and Jia Jie [贾杰], “Thoughts on Constructing and Strengthening Network Militias” [加强网络民兵建设的思考], National Defense [国防], no. 3 (2019), 58.

[22] Academy of Military Sciences Strategy Research Department [军事科学院战略研究部], eds., *The Science of Military Strategy* [战略学] (Beijing: Military Science Press, 2013), p. 196.

[23] See Wang Jinsong [王劲松], Wang Nanxing [王南星], and Ha Junxian [哈军贤], “Research on Cyberspace Operational Command System” [网络空间作战指挥体系研究], *Journal of Academy of Armored Force Engineering* [装甲兵工程学院学报], no. 5 (2016), p. 3., and Fan Yongtao [樊永涛], Wang Jinsong [王劲松], and Li Shikai [李世楷], “Problems and Solutions to the Cyberspace Operational Command Pattern” [网络空间作战指挥方式面临的问 题及对策], Journal of Academy of Armored Force Engineering, no. 5 (2017), 9.

[24] John Costello and Joe McReynolds, “China’s Strategic Support Force: A Force for a New Era,” *China Strategic Perspectives* 13 (NDU Press: Washington, D.C.), p. 9, Elsa Kania and John Costello, “The Strategic Support Force and the Future of Chinese Information Operations,” *The Cyber Defense Review*, Spring 2018, p. 108.

[25] For examples, see “Bearing in Mind Their Glorious History, the Military and People Build a Dream Together” [铭记光辉历史·军民同心筑梦], Shandong Network [山东网], July 21, 2018, available at http://www.sdwltv.com/soc/20180721/80281.html and “City Leaders Visit Officers and Soldiers Living Under Special Care Conditions” [州领 导走访慰问部队官兵和优抚对象], Yanbian Broadcasting and Television Station [延边广播电视 台], July 31, 2019, available at http://www.yb983.com/p/98894.html.

[26] Zhang Zhigang [张之刚], “Research on Smart Electrical Power Monitoring and Control Sensors [电力监控网络安全态势智能感知方法研究],” PhD degree dissertation, PLA Strategic Support Force Information Engineering University [战略支援部队信息工程大学], 2019.

[27] Qu Qiang [曲强], “Research on Spam User Detection on Social Networks [社交网络垃圾用户检测关键技术研究],” Master’s degree dissertation, PLA Strategic Support Force Information Engineering University [战略支援部队信息工程大学], 2019.

[28] Guo Xiaoyu [郭晓宇], “Research on User Identification Across Social Networks [跨社交网络用户身份识别技术研究],”Master’s degree dissertation, PLA Strategic Support Force Information Engineering University [战略支援部队信息工程大学], 2020.

[29] Ma Xiaofeng [马晓峰], “Research on Community Detection Algorithms in Social Networks [社交网络中的社区检测算法研究],” PhD dissertation, PLA Strategic Support Force Information Engineering University [战略支援部队信息工程大学], 2018.

[30] Wang Shuwei [王树伟] et al., “Review of Malware Adversarial Sample Generation on Generative Adversarial Networks [基于生成对抗网络的恶意软件对抗样本生成综述],” *Journal of Information Engineering University 信息工程大学学报* 20, no. 5, 2019, pp. 616-621.

[31] Hu Yongjin [胡永进] et al., “Method to Generate Cyber Deception Traffic Based on Adversarial Sample, [基于对抗样本的网络欺骗流量生成方法],” *Journal on Communications 通信学报* 41, no. 9, September 2020, pp. 59-70.

[32] Li Bicheng [李弼程], Hu Huaping [胡华平], and Xiong Yao [熊尧], “Intelligent Agent Model for Network Public Opinion Guidance [网络舆情引导智能代理模型],” *National Defense Technology 国防科技* 40, no. 3, June 2019, pp. 73-77.

[33] Chang Chengyang [常城扬], Wang Xiaodong [王晓东], and Zhang Shenglei [张胜磊], “Polarity Analysis of Dynamic Political Sentiments from Tweets with Deep Learning Method [基于深度学习方法对特定群体

推特的动态政治情感极性分析],” *Data Analysis and Data Discovery 数据分析与知识发现* 51, no. 3, March 2021, pp. 121-131. The study examined the Twitter posts of John Bolton, Donald Trump, Mike Pence, Robert O’Brien, Mike Pompeo, Steve Mnuchin, Frank Palone, Eric Swalwell, Richard Blumenthal, Joe Biden, Adam Schiff, Bernie Sanders, Nancy Pelosi, Gretchen Whitmer, Kamala Harris, Lawrence Summers, Andrew Cuomo, Sally Yates, Maria Cantwell, Edward Markey, and Elizabeth Warren.

[34] For a succinct explanation of this concept, see Joe Slowik, “Full-Spectrum Information Ops for Critical Infrastructure Attacks & Disruption,” Cyberwarcon, November 19, 2019, https://www.youtube.com/watch?v=n7XqxRXwFZ4.

[35] Li Jidong [李继东] and Chen Zhou [陈舟], “On Strategic Cyber Warfare [试论战略网络战],” *China Military Science* 2017, no. 6, p. 55.

[36] Phillip C. Saunders and Joel Wuthnow, “Large and In Charge: Civil-Military Relations Under Xi Jinping,” in *Chairman Xi Remakes the PLA: Assessing Chinese Military Reforms* (Washington, DC: NDU Press, 2019)

[37] James Mulvenon, “So Crooked They Have to Screw Their Pants On – Part 3: The Guo Boxiong Edition,” *China Leadership Monitor* 48 (Fall 2015), accessible at https://www.hoover.org/sites/default/files/research/docs/clm48jm.pdf.

[38] Zach Dorfman, “Tech Giants Are Giving China a Vital Edge in Espionage,” *Foreign Policy*, December 23, 2020, https://foreignpolicy.com/2020/12/23/china-tech-giants-process-stolen-data-spy-agencies/.

[39] Zuo Juan [左娟] and Jia Jie [贾杰], “Thoughts on Constructing and Strengthening Network Militias” [加强网络民兵建设的思考], National Defense [国防], no. 3 (2019), pp. 58-59.

PANEL I QUESTION AND ANSWER

CHAIRMAN WONG: Thank you, Mr. Chen. Appreciate your testimony.

We'll now move to the question and answer period, and I want to remind our Commissioners that I will be enforcing a time limit to ensure that everyone has a chance to have a robust conversation, but I also remind the Commissioners that if you don't have a question or you don't feel you have a worthy question, you are free to pass and we can come back to you, and come back to everyone else at the end when we have more time.

But given that we are in a hybrid virtual/in-person scenario, we're going to go in alphabetical order, and I am going to start with my co-chair for this hearing, Commissioner Bartholomew.

COMMISSIONER BARTHOLOMEW: Thank you very much.

Thank you to all of our witnesses for very interesting testimony. I was struck, Mr. Cheng, in particular your reference to Russia because it feels like we're certainly watching cyberwarfare unfolding in real time and the lessons that people can take away from that.

But, Ms. DeSombre, you made reference to encouraging responsible behaviors and I wondered if you could elaborate on that, especially in the context where it just seems like this is a universe where the activities are by nature adversarial. So how would we encourage responsible behaviors when all of the incentives for example are within the Chinese government's strategy of a warfare context?

MS. DeSOMBRE: Absolutely. Thank you, Commissioner, for the question.

So when I talk about responsible stakeholder behavior in cyberspace, I think something to note is that we're not talking about cyber as a domain in a vacuum when we're talking about cyber. We're talking about the infrastructure, the companies, and the economies that operate in the digital domain. And when we're talking about responsible behavior here, especially within an interconnected and interdependent environment, I think that we can look back on the 2015 Xi-Obama agreement, which arguably the Chinese government has not entirely abided by when we're talking about preventing economic espionage in cyberspace.

But the tool kit that resulted when the United States has decided that this individual or this corporation or this government has not abided by international norms - we've resulted in naming and shaming and sanctions. And there's certain pros and cons to these particular tools primarily because China no longer cares about whether or not it's being named and shamed if there's no imposition of cost afterwards. And the current sanction environment, especially when we're sanctioning individual PLA officers and the like, is not nearly as effective as we'd like it to be.

And so we're actually not seeing an unwillingness to - from China to come to the table to participate in the international economy with regards to cyberspace, but we're seeing an inability of the United States to pressure China into developing and collaborating in the way we would like.

And so I would actually suggest that when we're talking about responsible stakeholder-ship and international norms to focus more on what the U.S. values here, which is the free and open internet, lack of intellectual property theft, and try and come up with some scalable and tenable solutions to be able to pressure our adversaries, with our allies and hand-in-hand to be able to figure out these problems.

COMMISSIONER BARTHOLOMEW: Thanks. Thank you very much. I guess still I'm struck just with the concept of responsible stakeholders when we look like we're in an environment where being a responsible stakeholder particularly in this realm does not seem to be in the Chinese government's interest as far as it's defining its own interests. So it's a - I think it's a real challenge figuring out how to do that. Figuring out how to retain a free and open internet at a time when individual countries are clamping down on freedom of information is a real challenge. So I'm looking forward to learning more about activities that we can undertake to do that.

That's my only question right now. Thanks, Mr. Chairman.

CHAIRMAN WONG: Thank you, Carolyn.

We'll now move to Commissioner Borochoff.

COMMISSIONER BOROCHOFF: Good morning. I want to say thank you to the folks who have joined us today as witnesses.

And going back to you, Ms. DeSombre, I was also interested - and I think perhaps others of your colleagues have today mentioned the entity list. I'm curious, do we have the ability right now to identify specific actors? Do you know specific actors that you believe already qualify to be named to an entity list if we were inclined to do that? And then separately how do we identify them? What standards are we using? Because it seems like we have to wait for them to do something really bad before we can do it.

And then going directly to what Commissioner Bartholomew just said, are you suggesting then that probably the folks that get sanctioned by us in the entity list are going to change their behavior because we're going to economically name and - it's not just naming and shaming. It's punishing them financially. And I think that Mr. Cheng also commented along that line. So if you can answer how you would identify them and do we have a list?

And then, Mr. Cheng, if we have enough time I'd like to hear your answer to that as well.

MS. DeSOMBRE: Absolutely. Thank you, Commissioner Borochoff. So when we're talking about punishing these actors economically, we actually do have a small number of institutions that we have not yet sanctioned. There's a number of Chinese contracting organizations that have been outed publicly by research groups, as well as a couple of institutions, while a little bit more controversial, are related to the military-civil fusion program. So there are certain labs as well as other potentially more academic institutions that have been directly connected to cyber operations, however that does become a little bit more of a concern when you're targeting academics, right?

So when we're talking about the concerns about the lack of responsible stakeholder behavior, again I think it's important to know where China wants to collaborate economically with us in the digital domain. There's plenty of AI research actually that encompasses both Chinese and U.S. researchers working together collaboratively, however that seems to be more person-to-person than entity or corporation-to-corporation and being knowledgeable of that dynamic while also trying to crack down on some of these firms that are directly engaging in corporate espionage on behalf of the Chinese government.

MR. CHENG: So I would say that there are a variety of entities that we should - sorry, Chinese organizations that we should be thinking about and casting a very careful examination of because I suspect that they would then be found to be suitable.

To begin with, while there are a vast number of Chinese universities, there is an interesting subset of universities that do not belong to the Ministry of Education. They actually belong to the Ministry of Industry and Information Technology, China's military industrial complex oversight group. This includes Beijing University of Aeronautics and Astronautics, Nanjing University of Aeronautics and Astronautics, the Harbin Institute of Technology. There's about eight of these. These are direct feeders into the military industrial complex. Should they be able to engage in joint research with American academic institutions, which is a not an entities list issue? Should their students be simply accepted into a variety of our institutions?

Let me also draw attention here to China's use of its points of presence in North America to redirect the internet to China. Essentially the internet is a little bit like a vast air traffic control system. At the very top there are organizations whose servers are able to route traffic to and away from based on how much traffic there is.

So imagine that you were flying to London and your luggage it turned out would be best routed by way of Shanghai. The Chinese companies like China Telecom, a state-owned enterprise, has a presence in North America that allows them to redirect this. The FCC earlier this year did start to impose limits on China Telecom, but not for these reasons.

I would suggest that such bad behavior; and this has been much more well-documented by Professors Demchak and Shavitt in articles in relevant journals, would provide I think an important aspect to signal to Beijing responsible behavior includes not redirecting the internet to China where it can be recorded and broken at your leisure.

COMMISSIONER BOROCHOFF: Two great answers. Thank you very much.

CHAIRMAN WONG: Thanks, Bob.

We will now move to Commissioner Fiedler.

COMMISSIONER FIEDLER: Thank you. I have a number of questions. Let me start with a doctrine question that also involves proportionality. So we talk about attacks on civilian infrastructure often and we're worried about it. And in the Ukraine we may see it if something happens. But usually in a conventional conflict one doesn't attack your adversary's civilian infrastructure at the beginning of the conflict. Doctrine seems to be evolving whereby it's actually one of the first things one considers to do now. Talk to me about Chinese doctrine about attacking infrastructure.

MR. CHENG: What I would suggest, sir, is that attacks on civilian infrastructure – because they are seen as effecting significant strategic changes, undermining the adversary's psychological will to fight, the willingness to maintain a conflict by going after the civilian broader willingness - will to fight, but also disrupting supply infrastructures, et cetera. Transcom operates in conjunction with the civilian air traffic control network, et cetera - two things: One, these are legitimate targets of war. Two, that in a sense it achieves the ultimate goal, which is victory. And that the Chinese I suspect doctrinally are far more prepared to win ugly than to lose immaculately.

In this regard also, particularly from the cyber aspect, it doesn't necessarily inflict casualties. The Colonial Pipeline hack involved a lot of disruption, but the actual number of casualties effected, number of people who died is I would submit probably very close to zero.

The same arguably is true - the Chinese doctrine doesn't say “and we're going to shut down power grids and have hospitals be isolated.” Disrupting traffic signals in a city can be every bit as disruptive at times without necessarily directly inflicting casualties.

COMMISSIONER FIEDLER: So as - well, warfare has completely changed doctrinally, one. Two, the proportionality question leads right into miscalculation early in a conflict. So it's a very difficult thing to manage, it strikes me, whether it be us or them, how to inflict proportionally - how to escalate in a cyberwarfare scenario, which would be part and parcel of any conflict - how to escalate without the other side miscalculating.

MR. CHENG: Sir, very quickly, I would want to really emphasize the Chinese approaches to crisis stability are fundamentally different and arguably at odds with our understanding of crisis stability. During the Cold War it would be literally inconceivable, and I do understand the meaning of that word, that a NATO or Soviet Warsaw pact commander would send troops 10 miles across the inter-German border and occupy a feature in the other country. That officer would be summarily relieved if not executed.

China has repeatedly sent hundreds of troops across the border into nuclear-armed Indian territory, camped out and been resupplied over an extended period. This is a very different understanding of miscalculation, the dangers thereof, willingness to risk escalation with a nuclear-armed adversary. In that context particularly, because as my co-panelists have also noted, Chinese cyber actions almost certainly won't occur in a vacuum, but will occur alongside others.

What I would suggest is that their worries and their approach to the issue of miscalculation is fundamentally different from our own.

COMMISSIONER BARTHOLOMEW: Jeff, you're muted.

COMMISSIONER FIEDLER: I agree and I would like to have a second round if we have time.

CHAIRMAN WONG: Of course. Thank you, Jeff.

We're going to turn to Dr. Aaron Friedberg.

COMMISSIONER FRIEDBERG: Thank you very much and thanks to all of our witnesses for their excellent presentations. I'd like to start with a question for Ms. DeSombre. You made a point right at the beginning which seems to me extremely important, which is you made an assertion about China's capabilities relative to the capabilities of the United States. And it strikes me that this is a domain in which it's extraordinarily difficult to conduct any kind of net assessment that leads you to a reliable conclusion about who's ahead and in what regard.

Could you say more about your - the basis for your opinions in that regard, how you would go about conducting such an assessment? And then in addition, if you're aware, is there any kind of formal presumably classified net assessment of cyber balance that's being done inside the U.S. Government now?

MS. DeSOMBRE: So I am either fortunately or unfortunately an outsider in terms of the U.S. Government side. I have no knowledge of any classified net assessment. I will however say that current assessments and indices of Chinese cyber power are fairly flawed for a number of reasons, and I'm happy to go into that.

And so when we're talking about Chinese cyber power I like to - especially in warfare I like to think of offense, defense, and asymmetry. Fundamentally our - is China able to achieve its goals in each of these three realms regardless of how sophisticated the capability is? There's a lot of talk about sophistication in cyberspace, which is a red herring mostly because if defenses on our end are weak such that China does not need to expend that many resources to develop a capability that can cause an effect on us, what does it matter that they don't have sophisticated cyber capabilities?

So when I'm talking about the offensive side, China actually has both the sophistication as well as the capability to conduct low-level operations. From the open source metric side one of the bigger proxies in that regard is a - the vulnerability research ecosystem. So fundamentally when we're looking at how Chinese actors have evolved over time, there was a recent report that actually just came out a couple days ago that showed that when China uses vulnerabilities in software, the number of vulnerabilities that Chinese cyber threat actors have used have gone from 2 to 12.

Now what are these vulnerabilities for those who aren't as deeply day-to-day technical operations as I am? A vulnerability is ultimately a flaw in a piece of software that can be exploited for getting greater access into that software and largely used in offensive cyber operations, CNE, CNA. They can also be really big economic risks to these particular organizations or vendors that produce this software, and also a detriment to any corporation that ends up using it and relying on it.

So China, like many other members of the international community, actually holds vulnerability research hacking competitions. And so these competitions are where vulnerability researchers can go test their skills and show to the international community "I found a bug" in Adobe, Microsoft, Google, and get a lot of money for it.

Unlike the international community, which actually directly discloses these flaws to vendors so that way they can fix them, China requires all these bugs to go first to the Chinese government and likely actually results in the exploitation of these vulnerabilities in their cyber operations.

This year, or 2021, this past year the Chinese equivalent competition called the Tianfu Cup, resulted in 30 successful exploits of these vulnerabilities. And this is just the Chinese researcher community. The international equivalent, which has a large U.S. contingent, only found 21. So just by the virtue of the top tier sophistication alone, China is ahead.

On top of that they have all of these lower-level asymmetric capabilities that ultimately while are just like simple phishing emails, click on this link, still enable them to achieve their goal and break into corporations. So fundamentally by virtue of them being able to successfully hack us in peace time, I would say that they are a peer adversary.

COMMISSIONER FRIEDBERG: Well, I don't think anyone doubts they're a peer adversary. The question is are they ahead in meaningful ways, and if so, in what domains? But maybe that's a question we can pursue further.

MS. DeSOMBRE: Oh, yes, I'm happy to answer that later.

CHAIRMAN WONG: Thanks, Aaron.

Let's move to Commissioner Glas.

VICE CHAIR GLAS: Well, many thanks to all of you. I have two questions, and if we don't have time to cover both of them, I'll come back.

Mr. Chen, appreciated your testimony talking about and connecting it to the real threats on the Colonial Pipeline, which we all regrettably experienced. In your testimony you talk about disinformation campaigns which the U.S. has not - has also been victim to sort of disinformation campaigns. Can you talk about that in a broader context as our audience on Capitol Hill is particularly interested in sort of the narratives that are being driven and what you think the implications are?

Ms. DeSombre, appreciated your recommendations to Congress related to the China bill under current consideration. I noted in your testimony you also talked about the cyberespionage and cyber - the prevalence of this industry in China being a direct threat to intellectual property. As you know, the Trump Administration moved forward to levy tariffs associated with - to address these punitive trade practices, but it sounds like the problem is even getting worse. Can you elaborate on that a little bit more? And we can take time at the very end with the second round. See how far we can get.

So, Mr. Chen, I'll start with you.

MR. CHEN: Sure. Thank you, Commissioner. That's a great question.

I think in terms of disinformation in a broader context the Chinese sort of modus operandi here is a little bit different than some of the other actors that we may have seen, particularly Russia.

The Chinese propaganda apparatus, which is the system that would be spewing this kind of disinformation, tends to want to play up its - China's relative or comparative superiority in all sorts of things related to governance and culture and all these different aspects of society. That is a little bit different than say sort of Russian efforts in their - abroad or against the United States even where Russian operatives were simply setting out to cause as much chaos and as much division as possible.

So for the moment I think the Chinese threat is - has yet to fully manifest. They are certainly capable of I think dividing communities and sowing a ton of sort of discord and chaos and really playing both sides of that. They have not really demonstrated that capability in their operations at home because that's - a lot of this propaganda apparatus is geared towards keeping the CCP in power, and obviously practicing on how to divide a community is a thing for that.

Should they ever do so, I think we would face a particularly kind of nefarious threat, especially when layered and timed correctly with other aspects of cyber operations. So in terms of implications I think just because we haven't seen them do it now, doesn't mean that they're not fully capable of it and inflicting that upon us. So that would be a thing I would want to prepare for.

VICE CHAIR GLAS: Thank you.

Ms. DeSombre, I know you - we only have a minute-and-a-half left, but can you tackle that question?

MS. DeSOMBRE: Yes, absolutely. I'll be brief. So I think I would just point to a single set of data, which is the number of successful Chinese cyber operations that were meant for economic espionage - ended up successfully stealing American IP. And between 2015 and today, 2022, you see a dip right after the Chinese - China-U.S. Cyber Agreement, but never truly a stop. And it's only ever gone up since then.

And so arguably it's hard to even conceive that this was in result of the signing of the Xi-Obama agreement at all, and potentially even could be coincided with the strategic organization of the PLA into the SSF. So simply they had no intention of stopping. They were simply reorganizing themselves so that way they could do it better.

VICE CHAIR GLAS: Thank you. And I'll come back for round two. Thanks.

CHAIRMAN WONG: Thank you, Kim.

Let's move to Commissioner Schriver.

COMMISSIONER SCHRIVER: Morning and thank you to our witnesses for those excellent statements and presentations. Let me try to squeeze in two quick questions. The first one is a general one; second one more specific to the PLA.

First general question, Ms. DeSombre, you made a comment which I thought was interesting that the PRC is advantaged somewhat by the fact that they don't have constraints that the United States imposes on itself due to international law or agreements or commitments. Do we see any constraints at all or restraints? Is there any evidence in Chinese language, materials or anything that's been made available publicly that suggests there is leadership guidance saying “here's where the line are,” or are they completely unrestrained as far as we can tell? It's just a matter of capability that constrains them?

MS. DeSOMBRE: Thank you for that question, Commissioner Schriver. I unfortunately am not an expert in doctrine, so I leave that to my colleagues on the panel to figure out, but from an operational perspective we have not yet seen a disruptive attack on U.S. critical infrastructure. However, their cyber-attacks have been fairly consistent and they've tried numerous technical and human factors that I don't think the United States would do virtually by, like I said again, the operational tradecraft, abiding by international law, abiding by the law of armed conflict, et cetera.

And so I think you're right. I think that there hasn't been something that from an operational perspective they haven't tried yet except for a real disruptive or destructive attack on U.S. critical infrastructure.

COMMISSIONER SCHRIVER: Thank you. Yes, I think it's important to understand as we think about U.S. approaches if they're sort of unconstrained by naming and shaming and international law and norms how we really think about our own tool kit. So appreciate that answer.

On the PLA, and start with Mr. Chen and if there's time Dean, Mr. Cheng.

Mr. Chen, you made an interesting point about the reorganization and the integration of these capabilities into war fighting as being sort of untested and the unknowns. And I know that's true in our own system. When we reorganize it's ultimately for the purpose of getting better, but the process of reorganizing and implementing new structures is itself difficult and there's a learning curve, et cetera.

What would you say are the long poles in the tent for them to really leverage this new organization, the Strategic Support Force? Are we seeing them in exercises? Are we seeing them as being integrated into traditional war fighting capabilities so that we would understand that cyber would be integrated into a campaign? What's your assessment of that?

MR. CHEN: Thanks, Commissioner. That's a great question. I think my general assessment here is that they talk a lot about integrating. They understand the importance of integrating particularly cyber and sort of electromagnetic warfare into other domains of conflict. And if you sort of read PLA media there is not a lot of mention of the SSF and how they perform in exercises.

There is however some mention of sort of what one might refer to as like the back end of the SSF, so reserve units and militia units that are tasked with cyber operations, usually defensive. And so - that's at the local level. So at the military district level those folks don't tend to do well. They've listed a couple of deficiencies with these types of reserve units that are participating in exercises.

One of them is that they obviously don't have enough talent. And so there's been some exhortations to like, “hey, when you call up your reserves, please don't call them from the local propaganda department because they're very busy.”

And then the other deficiency is really that military district commanders have problems understanding how - like great, I've got this cyber reserve unit in play; what do I do with them? And so at lower levels this integration is very much not complete. And at higher levels with more exquisite kind of well-developed capabilities the Chinese don't mention that a lot.

One thing that they do mention and actually kind of pertains to the last question was that increasingly they make the comparison between strategic cyberwarfare capabilities and nuclear capabilities. And that's sort of one of the drivers behind this emphasis on centralization, right? Xi Jinping is the only one that can make this call, just as he would be the only one to make the call for a nuclear strike.

COMMISSIONER SCHRIVER: Great. Thank you.

CHAIRMAN WONG: Thank you. We'll turn to Chair - Commissioner Scissors.

COMMISSIONER SCISSORS: Thanks for the promotion.

I appreciated Bob's question earlier and I think I'm actually extending it, but I want to first object to one little thing he said on the way to a good question because it was also used by - mentioned by several of our panelists today.

The entity list is not a sanction; it's a licensing process. Or if we're going to call it a sanction, we have the weakest idea of sanctions I can possibly imagine and we shouldn't be surprised when it doesn't deter Chinese cyber action. So a sanction is you punish the other firm, not you put them - have them write some paperwork and they return to the status quo.

And you know, we are in Congress, and Congress uses the entity list as a sanction and it's mined all the time, but it's - they're wrong. So let's think about - if we mean meaningful sanctions, let's think about something more than that.

Now to - and I don't want to put words in Bob's in mouth, but to extend his question - and this is for Dean because he's heard me talk about this before so it's fair for me to impose it on him.

Civil-military fusion, applying to information warfare resources. How important are Chinese commercial IT firms? And I'm going to try to give you - to PLA capabilities. And I'll try to give you a range here from like civil-military fusion - please stop saying that word; it doesn't really mean anything - all the way to they're basically a part of the PLA with regard to information warfare. And I realize you're going to be somewhere in between because that seems to be reasonable. So if you're somewhere in between, could you identify as much as possible particular firms or particular sectors that are more closely associated with PLA capabilities?

MR. CHENG: Yes. Civil-military fusion needs to be seen in the context of Chinese mobilization efforts. Let me note here in this reorganization of the Central Military Commission, mobilization was elevated to a general directorate level, meaning this is really important, people. Pay attention. We've got somebody who bureaucratically is in charge of this now.

There is an entire parallel mobilization structure, the National Defense Mobilization Commission, which runs from the national level, Xi Jinping-equivalent, all the way down to the township level. Now what does this have to do with information warfare and cyber?

According to the Science of Military Strategy, 2013 Edition, I believe, for the first time the Chinese military openly acknowledged that there are three pieces broadly speaking to China's information warfare capabilities. First is within the PLA itself. This was pre-reorganization, but therefore the PLA SSF.

Two, non-military governmental resources and assets: Ministry of State Security, Ministry of Public Security.

And third, the broader entire civilian economic base. That means that IP addresses, that means that potentially corporate IT departments, as well as Chinese antivirus firms; and they do exist, all of these - China Telecom, the state-owned enterprise - all of these are potential sources of three things: personnel, equipment, and facilities, and by that last item I would include their networks, are potentially available in event of need.

The mobilization structure exists to absorb and pull those elements in. The Chinese writings on mobilization include discussions of limited versus national, public versus secret, localized, and very focused scientific - and in this regard here information mobilization, information resource mobilization falls under the S&T mobilization aspect.

So what I would say is that they on a day-to-day basis simply a part of the PLA? No. But upon mobilization under the broad rubric of civil-military fusion all the way down to the nitty-gritty of how do we mobilize, you have the potential at least of being able to call upon any and everyone, any and everything in the corporate, academic, state-owned enterprise realms.

COMMISSIONER SCISSORS: Can I just ask a really quick follow-up? That was an informative answer, but do you have a sector or a couple of sectors you would name off the top where you'd say look, this is where the PLA right now would go first? As an economist I'm looking at what sectors of the economy are most important in this domain. Is there anything you could characterize?

MR. CHENG: So I would say that certainly for example all of China's telecommunications. Most of it is state-owned enterprises, so that's actually not a particularly difficult ask. Huawei of course is the primary provider. It is not a state-owned enterprise, as you know, but it is a Chinese company which means that the Chinese can reach out and touch that company's capabilities and assets.

Insofar as Chinese satellites for example, it is - China Great Wall Corporation is a wholly-owned subsidiary of China Aerospace Science and Technology Corporation, which is a state-owned enterprise, and yet Great - China Great Wall is somehow seen as a - oh, it's a commercial company that simply sells satellites and satellite services. Don't read the Chinese version of the website that says oh, and we're a wholly-owned subsidiary.

CHAIRMAN WONG: Thanks, Derek.

We're going to turn to Commissioner Wessel.

COMMISSIONER WESSEL: I thank you all for being here. I have too many questions; let me see if I can focus in hopefully a second round.

It seems to me we still have a fundamental mismatch in terms of our thinking versus Chinese thinking. And I go back to the 2015 agreement between Xi and Obama where Xi indicated that they would no longer engage in espionage for economic gain when in fact economic security and national security are essentially the same thing. So it was a empty promise.

Mr. Chen, you talked about the Colonial Pipeline. As I recall, it was not the switching in pipeline that was undermined. It was their accounting system and it was their fear of not getting paid that resulted in the disruptions, not the question that the oil and gasoline, et cetera, wouldn't flow.

So going through some of the questions of my colleagues it seems we're putting security behind profits. To Derek's question about entity lists and sanctions, et cetera, we are still aiding and abetting China. The problems with Huawei were identified early in the 2000s and we're still trying to find the money to replace Huawei systems from our networks to be able to have greater security. Massive amounts of U.S. capital are supporting Chinese entities, CCP policies, including Chinese military companies where our Wall Street firms are able to assist them outside of the U.S. market.

Are we taking this problem seriously enough? Has China pre-positioned electronic assets and capabilities in our system that gives them such an advantage that until we take - put security ahead of profitability we will continue to be vulnerable?

Mr. Chen, do you want to start with that?

MR. CHEN: Sure. Yes, that's a great point, Commissioner. I think you're right. I think in some instances our nation continues to prioritize profit over security. That's been a bit of a defining feature as we've sort of shifted our relations with China overall.

I think some of this is a product of the fact that our systems are fundamentally different. So as Mr. Cheng mentioned, the Chinese government can exert considerable leverage on any company operating in China, to say nothing of the fact that many of them are actually extensions of the government as state-owned enterprises.

But the United States operates in a free market. And so the United States Government has much more limited leverage than by comparison the Chinese government might. And so there's a lot of situations where - because in this free market American companies are obliged to pursue profits for shareholder interests and that can generate externalities on the American taxpayer. And we're seeing that now. The example you mentioned, we're having trouble finding money to rip out Huawei boxes and put in more secure ones. I don't have a ready answer for that.

I would just note here that we are looking at fundamentally different systems and as much as the Chinese have said since 1978 that they would like to reform and open up and they're embracing the free market, especially since Xi Jinping has come to power that sort of narrative has been turned on its head. They are still very much a statist economy and that is the kind of counterpart we're dealing with, the kind of adversary we're dealing with.

COMMISSIONER WESSEL: Do our other witnesses have thoughts?

MS. DeSOMBRE: I can go. So I would say that I absolutely agree in that in some cases we are putting security behind profits, however I think that when we're talking about the sanctions list and the entities list, one of the risks that I would like to highlight is that we are creating in some instances, by trying to rip out our two systems from each other, a bifurcated set of economies.

And I would suggest that instead of hiding away and shutting ourselves off, we should be more open and go into some of these areas in which China is trying to construct their Digital Silk Road, for example, and to offer a viable alternative and merge our security and our profits together.

COMMISSIONER WESSEL: Thank you.

CHAIRMAN WONG: All right. Thanks, Michael.

Okay. Dean, just -

COMMISSIONER CHENG: Yes, just very quickly. I think it's notable here that IT security in any major firm other than an IT security firm is an overhead cost and therefore by definition it ranks alongside paying the janitorial services, not a high-priority product, other than unless of course you are CyberStrike or Norton Security or something like that. And that obviously has implications regarding where a company puts its money.

COMMISSIONER WESSEL: Thank you.

CHAIRMAN WONG: Great. Thanks, Mike.

Ms. DeSombre, I just want to focus in on one of your recommendations regarding devoting more resources to domestic semiconductor fabrication facilities. Is the reasoning behind that kind of a macro-level security where we don't want choke points for semiconductors, or if China ever does reach its ambition of being a leader in kind of more exquisite semiconductor fabrication that we don't want them to have that leverage over us, or is the reasoning behind that that we fear that within that hardware; if it does come from China, or elsewhere, that there's embedded in that certain vulnerabilities if we're purchasing them, or is it both?

MS. DeSOMBRE: I would argue that it is both, but far more the former than the latter. So when we're talking about some of the more advanced pieces of semiconductor equipment that are manufactured we are beholden to China in a lot of ways, not just by virtue of having a majority of these semiconductors being manufactured by TSMC in Taiwan, but also given our current state of affairs and the supply chain shortage for a lot of these chips, a lot of the chips that go through Taiwan or manufactured through Taiwan are actually going through Chinese airports in order to get to the United States.

So that's fundamentally a choke hold that the United States should try and circumvent.

The hardware side of the equation is less-well fleshed out by the industry. There were some scares a couple years ago when that Bloomberg piece came out about Chinese manufactured chips potentially having some issues, but that was not - it did not seem to hold up under scrutiny. However, it is still a sizeable risk if China and the U.S. get to the point where we are such adversaries that we could end up having Chinese-tampered chips in our own software.

CHAIRMAN WONG: Thank you. And one question for Dean. My understanding is that the United States in levying direct cyber sanctions or cyber-related sanctions, that the grand majority of these sanctions are applied to Russian, North Korean, and Iranian persons or entities. Very few of them are Chinese designees, and if they are, it's usually Chinese entities that have been doing work for WMD proliferation related to North Korea. Why is that? That's my first question.

Second, is that okay? And if not okay, what should we be doing as far as supplying our direct sanctions on bad Chinese cyber actors?

MR. CHENG: Thank you for that question. My understanding in the first place is that applying sanctions publicly means providing evidence on a legal basis going into court, which Chinese defense lawyers, who may actually be American defense lawyers retained by the Chinese, make very clear would raise questions of sources and methods. And that therefore brings to highlight yet another asymmetry, which is the separation between law enforcement and intelligence in our system where the intelligence community may well have proof positive, but is not prepared to expose sources and methods.

Another aspect here however, and this was highlighted with the release of Meng Wanzhou, the CFO of Huawei, is that we have also been not serious about even enforcing the ones where we have pretty good public evidence. The release of Ms. Meng, who was being detained by our Canadian allies, was about violation of Iran sanctions, not about cyber theft. And she was released for free.

And the message that that sent to Beijing is visible in how the Chinese welcomed her home. This was a hero's welcome. And the Chinese press ran the following tag line: The Arrest of Meng Wanzhou Was Because of the Rise of China and the Release of Meng Wanzhou was the Product of the Rise of China. It's a difficult situation when we insist on not just shooting ourselves in the foot, but reloading and emptying a second magazine.

CHAIRMAN WONG: Ms. DeSombre, in 30 seconds do you have any thoughts on that? I saw you kind of nodding along.

MS. DeSOMBRE: Oh, I agree.

(Laughter.)

CHAIRMAN WONG: Well, let's move to our second round. I know that Carolyn had mentioned she wanted a second bite of the apple here.

COMMISSIONER BARTHOLOMEW: Yes, please. Thanks very much.

Mr. Chen, you did not have a chance to respond to Commissioner Fiedler's question about escalation, but I want to elaborate on it a little bit. First, you particularly mentioned human factors and I just wonder how one manages escalation in the context of human factors, right? The Colonial Pipeline, what happened there, might look particularly different if you think about it in the context of what happened in the snowstorm and 20 people stuck for 22 hours on freeways in Virginia. So how is there management of escalation when you bring human messiness into the context? That's one question.

Then the second question perhaps for all of you is none of us have mentioned attribution at all. In a warfare context do we have the ability to determine where these attacks are coming from, who's doing them, and then how we could respond?

MR. CHEN: Yes, thanks, Commissioner. That's a great set of questions. I'll try to take a stab at that first one.

I think it is very difficult because - to manage escalation especially when it sort of enters into the human realm. And I think if we're at the point where there are human impacts, we've already moved to the highest level of the escalation ladder, right? That would be sort of - PLA writings tend to have compared this to a nuclear strike, right? So if a nuclear weapon has been detonated, we are - consider us all escalated at that point. And crisis management at that point is pretty muddy.

The Chinese have not said a lot in the sources that are available about sort of how they intend to manage the cascade of human impact that would follow a major cyber-attack, but I think some of this is potentially dangerous because the Chinese - as Chinese military doctrine is focused on winning early. And so could we rule out the possibility of such a crippling strike, cyber-attack? I don't know. I don't think that we could. And so it's - I think it's prudent to be prepared for it.

And actually the second question I'll just take a little bite at. Some of that is - you mentioned attribution. That's vital. So we would need to know who is carrying out this kind of attack on us in order to be able to retaliate. And that's the sort of foundation of deterrence, right? We need to know who hit us.

I won't go into sort of the technical details on how that might work. I know that attribution in general tends to be one of the hardest things to do in this space. So with that I'll pass it to my fellow panelists.

MS. DeSOMBRE: I'm happy to touch on the technical side of that, John.

So there's a lot of debate in academia, especially for cyber in the last 10 years, about how hard or difficult attribution may or may not be. I am going to dispel those myths. Attribution is possible. It may be difficult, but within the United States either through the public or the private sector, attributing cyber-attacks has not been an issue.

And in fact, there are times where the United States Government will engage in active defense such as burning or publishing Chinese tool sets before an operation takes place. And that's happened I think a year ago now, as well as the Biden Administration's current press release about the Russian videos that may or may not get released on the Ukraine.

And so I would say that it's a possibility. It's likely that any kind of cyber attack that originates from China - I have full faith in either the government or the private sector in their attribution capabilities.

COMMISSIONER BARTHOLOMEW: Thank you.

Dean, do you have anything to add?

MR. CHENG: I would add that I think that one of the dangers here is a potential asymmetry the other way, which is would the Chinese believe that attribution is difficult and engage in dangerous actions when in fact attribution may be much more possible than they realize, in which case you then have set up a situation where now they have overextended themselves, in a sense left themselves exposed, and now the ugly option is climbing down with domestic implications versus proceeding ahead anyway?

COMMISSIONER BARTHOLOMEW: Thank you.

CHAIRMAN WONG: Great. I have Bob down for a second round as well.

COMMISSIONER BOROCHOFF: Yes, I'll be quick. Before I ask my one single question of Ms. DeSombre, I just - I want to clarify and thank you, Derek, for what you brought up.

In the business world, there are two ways that businesses are punished: One is often referred to as the nuclear option, and that's where a business loses its license to operate. That was my understanding of the entity list. There are so few people or businesses, entities on the entity list. It may well be that the reason there are so few is because of what Commissioner Wessel commented upon, which is Americans tend to be very reticent, very cautious about removing the license to operate and making it illegal.

So clearly there is a discussion that needs to take place about security over profit, and it's possible that's what's causing the very small number of entities to be on the entity list. I don't know. I'm not an expert on that. I look forward to learning more about it.

My one question for you, Ms. DeSombre, was in your initial comment you talked about the way that the space race - this is my interpretation of what you said - the space race put security over profit. And I'd like you to elaborate. Is that your understanding? Did I understand what you said about there being a comparison between the two?

MS. DeSOMBRE: So thank you, Commissioner, for the question. When I had mentioned the space race, I'm referring again to the human factor that some of my panelists have brought up. But instead of the human factor of cyber operations as a target, I'm referring to the human factor of our own capacity building.

COMMISSIONER BOROCHOFF: Okay.

MS. DeSOMBRE: So with regards to the space race, effectively Congress passed the National Defense Education Act for the engineering community to be able to build up capacity to put a man on the moon. We're completely underfunding our cybersecurity education, under-resourcing our cybersecurity practitioners in a way that in the long term will, just to borrow another Dean-ism I suppose, shoot us in the foot.

COMMISSIONER BOROCHOFF: Thank you.

CHAIRMAN WONG: Great.

Aaron, I think you had a second round?

COMMISSIONER FRIEDBERG: Yes, thank you. I wanted just to sort of put a proposition (telephonic interference) especially to Mr. Chen. I'm getting an echo, so somebody may be un-muted.

And this is a variation on the theme of putting security over profit. It strikes me that overall, although the magnitude of this problem - and I'm focusing here particularly on the cyberespionage and economic espionage as compared to the military piece - the magnitude has grown enormously over the last several decades, but we're still operating in a kind of business-as-usual mode, which means we're running around sort of using the tools we have to try to patch an increasing number of holes in our system.

So if you think about the problem, you can defend against it, you can try to get people to - you can name and shame, you can try to establish norms that discourage people from doing things, or you can try to impose costs on them.

You can't name and shame people who don't feel shame for what they're doing. You may spend decades trying to work out norms at the U.N., but don't hold your breath. The defenses are for the most part reliant on the actions of private companies, which for various reasons are often reluctant to spend what they need to spend really to fully defend themselves. And as far as the imposition of costs, we're using a narrow range of tools that were really primarily designed for other purposes like sanctions or putting companies on the entities list.

It strikes me that if we're really going to address this problem, we're going to have to start operating in a quite different way, and that that probably involves a greater role for the government than has been true in the past and that many of us would normally be comfortable with. So for example, imposing or creating requirements for defenses that companies have to meet on the defense side, and on the offense side creating other tools, much broader for imposing costs on a wide array of Chinese entities. So that's my proposition.

And, Mr. Chen, I'd be curious to hear you respond, and if then if we have time Dean as well.

MR. CHEN: Yes, thanks, Commissioner. I'd agree with that, certainly the premises of that that you've laid out there. I think it does call for a different response.

I'd add one note here, which is sort of related to issue linkage, right? So as the U.S. Government might feel compelled to intervene more actively, I think we probably ought to be doing a better job of issue linkage, which is to say that the Chinese for instance say that the SSF needs to be centrally-commanded, held at a - authority held at the highest levels. Are we targeting Chinese leadership and holding them responsible for actions that we don't want them to take?

And so there's been a lot of discussion about entities, the entity list and sanctioning companies that are actually participating in these kinds of activities against us. I think it may be time to consider expanding the range of options up into the Chinese leadership apparatus because those are the guys that are ostensibly calling the shots. And even if they're not, they should be the ones held responsible for maligned behavior. So there are other ways to do this that are worth discussion.

COMMISSIONER FRIEDBERG: Dean, do you have any thoughts on that?

MR. CHENG: Yes, I think that one of the things to think about here is again our own accounting systems, our own investment incentives suggest that - for example, should cybersecurity, some amount of a corporate - corporation's expenditures be considered potentially tax write-offs or tax breaks?

Commissioner Scissors has pointed out that we will never out-subsidize the Chinese, nor should we try. So I don't think subsidizing things leads to a good outcome, but promoting behavior through our own system of tax write-offs, et cetera, God forbid complicating the tax code further, but this might be one of those sorts of things that would in fact incentivize companies to do the right thing simply within the current constraints.

MS. DeSOMBRE: If I could jump in, Commissioner, just briefly, I also think that the United States has not fully grasped the number of technical cost impositions that we are currently able to do and I would highly recommend especially the vulnerability equities process or preemptively burning tool kits of our adversaries in cyberspace.

CHAIRMAN WONG: Thank you. Let's turn to Commissioner Fielder.

COMMISSIONER FIEDLER: So I wanted to return to sort of conflict scenarios. The cyber domain seems to me to require command and control at the highest levels to more rapidly make decisions, whether on our side or their side. We've heard lots of testimony in our military-related hearings about Chinese military's inability to delegate down to people in various scenarios or for lower-level units to take initiative.

What happens in a conflict to accentuate the difference between how the United States operates militarily and how the Chinese operate in decision making in cyber - as it relates to the cyber domain?

MR. CHEN: I can take a stab at that. Thank you, Commissioner.

I think one of the sort of artifacts of the reorganization has been that the CMC - Xi Jinping wants to hold the SSF in the palm of his hand, and in some ways that excludes regional PLA forces that would be fighting in sort of a theater-level conflict. And so this bifurcation that I had talked about leads to a situation where you might have at the operational level Chinese decision makers not having the information they need from the SSF.

So we see that in a couple of organizational quirks where like long-range over-the-horizon reconnaissance assets actually are - have SSF officers in those units. And so you sort of have questions about like, well, if my long-range radar or like strategic cyber reconnaissance tells me a thing, that information gets passed directly to Xi Jinping and not to theater-level commanders that might need that information. So this is great for peace time control. It means that the PLA's shooters out in the operational level - they can't shoot what they can't see. And so they have to call home to Beijing every time they want to do something.

But in an actual conflict there's a big sort of - you're going to call home to Beijing every time to see what they can see? There's a big process there and it's likely to be overwhelmed. There's a lot of things that need to happen on the fly, and that applies especially for cyber operations. And so I'm not entirely convinced that they can - that they have this down pat despite all of the rhetoric and the reforms.

COMMISSIONER FIEDLER: Yes, which is why I was asking the question.

I have one other question about - Dean, we're talking about network warfare and electronic warfare. So we both have the capability, China and the United States, to degrade each other's command and control fairly quickly in a conflict, which then puts us back into a conventional domain, if you will. In other words, what happens when both sides degrade each other's command and control rapidly? What do you think happens?

MR. CHENG: So let me begin by noting that I think one of the key problems with cyberwarfare, and to your first question, is that we have this terrible habit learned from Hollywood that cyberwarfare is like artillery campaigns. I need a cyber barrage on these coordinates; get it to me right now. Clack, clack, clack, boom. Things go down.

In reality cyberwarfare is built upon weeks, months, even years of penetration, mapping, et cetera. It is not clack a couple of keys and you have an effect. Which means that preemption and early phase use of cyber is key because of the cyber domain will literally change as security measures are installed, are initiated, as passwords change, et cetera. What that means then is that whoever goes first with the key clacking is more likely to have an outsized benefit.

Once we get into the war, as you've noted, then is when you have a degraded C2, and then in that context our commanders are more likely to be flexible, less likely to be operating according to a preset battle plan, et cetera. That at least is the theory behind mission-oriented orders, et cetera.

Let me just note here however very quickly one of the two great - sorry, two very great dangers: One is that there are PLA SSF units and presumably officers at every war zone, theater, command level. This is the reorganization of the command structure. And second of all, the high level of Russian-Chinese military cooperation and recent exercises means that China is potentially learning very scary lessons from the Russians. And unlike their observations of the

United States, this is not simply watching from afar, but actively exercising with people who are doing this for real in a war.

CHAIRMAN WONG: With about six minutes left and two Commissioners in a second round of questions, I would ask those two Commissioners to perhaps back to back ask those questions, direct them at a witness, and then see how much answer we can get out of them.

So, Commissioner Glas and Commissioner Wessel?

VICE CHAIR GLAS: For the sake of time I will defer to Commissioner Wessel.

COMMISSIONER WESSEL: I thank you, Madam Vice Chair. A quick question just as we look at enabling and advancing Chinese capabilities and the profits over security issue.

Last year the China Commission endorsed a proposal that some call a reverse CFIUS but really is a way of assessing outward investments to determine whether they undermine critical supply chains, critical capabilities.

Can each of you quickly opine as to whether you think having some presidential review over those kind of investments is valuable?

Mr. Chen, do you want to start?

MR. CHEN: Sure. Thanks, Commissioner. I do think - I'm not intimately familiar with all of the details of a reverse CFIUS, but I do think that it is a worthwhile thing to explore. I think that a lot of this outbound investment has a long-range impact on China's ability to develop and field capabilities that they could then use to support their cyberwarfare posture. So I do think it's worthwhile.

COMMISSIONER WESSEL: Ms. DeSombre?

MS. DeSOMBRE: Echoing those statements I do believe that especially given some of the military-civil fusion organizations and corporations that are on the sanctions list that does directly contribute to China's military buildup there are a few cyber corporations on there. And I would suggest that if there are any U.S. outward-bound investments into those corporations that they should be stopped.

COMMISSIONER WESSEL: Dean, any thoughts quickly?

MR. CHENG: Yes, sir. I think that trying to control outward-bound investment by companies, et cetera, other than those specifically beyond those already covered by export controls gets us into some very ugly gray zones. How do you control for venture capital and things like that, especially where you're talking about technologies that we may or may not even have an idea what their impact is?

I would note however that the massive amounts of money available to TSP, to various state-level pension funds, is something that should be reviewed carefully in part because of who is at stake, large government workforces, and also because it would seem that many of the investment firms that are managing these huge, literally trillions of dollars' worth of investments may be operating for their own purposes. And that I think gets us back into an area of really sort of very clear potential impact on national security.

COMMISSIONER WESSEL: Thank you.

CHAIRMAN WONG: Well, I want to thank our witnesses for some very cogent and thought-provoking testimony. We will move to our second panel in about 10 minutes. We will take a 10-minute break and reconvene at 10:50.

(Whereupon, the above-entitled matter went off the record at 10:41 a.m. and resumed at 10:52 a.m.)

PANEL II INTRODUCTION BY COMMISSIONER CAROLYN BARTHOLOMEW

COMMISSIONER BARTHOLOMEW: Our second panel will evaluate China's goals, actors, and methods for conducting cyber espionage. First we will hear from Adam Kozy, who is an independent analyst, as well as the founder and CEO of the boutique consulting firm SinaCyber, who will discuss the Ministry of State Security's role in state-sponsored cyber espionage.

Before founding SinaCyber, Mr. Kozy worked at CrowdStrike tracking cyber espionage activities from China, North Korea, and Russia. He is the author of the forthcoming book Geeks, Spies, and Criminals: How Chinese Intelligence Is Hacking Its Way to Hegemony.

Second, we will hear from Kelli Vanderlee, a Senior Manager for Strategic Analysis at Mandiant, who will address China's cyber espionage operators' tactics, techniques, and procedures. Her work analyzes trends in cyber espionage activity, identifies risks to organizations, and assesses adversary motivations.

Prior to Mandiant, Ms. Vanderlee worked as a Strategic Communications Analyst at Leidos, Inc., and is an adjunct professor of Arabic at George Washington University.

And finally we will hear from Dakota Cary, a Research Analyst at Georgetown University's Center for Security and Emerging Technology (CSET) who will discuss how Chinese universities and telecommunications firms support state-sponsored cyber espionage.

His research focuses on China's efforts to develop cyber espionage capabilities through AI and cyber security research at Chinese universities, the Chinese military's efforts to automate discovery of software vulnerabilities, and new policies that improve China's cyber security talent pipeline.

Thank you all in advance very much for your testimony. I'd like to remind each of you to keep your remarks to seven minutes, and Mr. Kozy, we'll begin with you

OPENING STATEMENT OF ADAM KOZY, INDEPENDENT ANALYST, CEO & FOUNDER, SINACYBER

MR. KOZY: Perfect, thank you so much. Members of the Commission, thank you for having me today. I will be discussing, specifically commenting on China's cyber espionage goals and the Ministry of State Security, or MSS's, role in achieving them.

Today I'm going to use two recent Department of Justice indictments as case studies to kind of illustrate the history and breadth of cyber operations carried out by MSS contractors and why their future ability to continue these operations is of grave concern.

Finally, I will submit several recommendations on steps Congress can take to combat this threat.

In the interest of time, I'm going to pretty much breeze over how China uses cyber espionage to achieve its strategic goals, mostly due to there being readily available open source materials explaining this in greater detail, as well as my written testimony before you.

You can also see Figure 2 within your documents to see greater details on how the PRC actually tasks its intelligence agencies to collect on key technology gaps.

What really sets the MSS apart is its positioning within the PRC's intelligence apparatus and its excellent use of alternative tradecraft to accomplish its objectives. I believe a combination of six factors have led to the MSS's current dominance in conducting cyber espionage campaigns.

First, the PLA had a storied history of corrupt senior leadership, cyber operators moonlighting for extra cash and poor operational security practices, which led to several public embarrassing exposures of their operations.

This was also extremely well-timed with the PLA's cyber force reorganization under the Strategic Support Force and came at a time when tensions with the U.S. over cyber espionage were at a peak, offering a convenient off-ramp.

The MSS also has an easier time recruiting, given it does not commission officers the same way that the PLA does. And the MSS also went through an earlier graft period during the beginning of Xi Jinping's tenure.

Second, the MSS has a unique domestic and foreign intelligence collection capabilities, building on a close relationship with the Ministry of Public Security, which it uses for cover and often is collated -- co-located with those locations and afford it very unique surveillance capabilities, including the Great Firewall of China and its ability to censor and contract information.

Third, the MSS invested early on in ecosystems it could control, cyber ecosystems it could control and grow. This led to the Thirteenth Bureau, or Technical Bureau's, creation of CNITSEC in 1998, which primed it to establish relationships with Chinese private sector security firms and hoard exploits from China's vulnerability research communities.

Fourth, its ability to effectively combine human intelligence operations with cyber campaigns and synthesize big data collection for targeting purposes.

Fifth, its use of contractors affords them plausible deniability and the ability to compartmentalize its collection efforts. But this also opens the door for criminal actors to target global victims with impunity.

Sixth, the legal structures give -- within the PRC give the MSS unfettered access to Chinese firms, both domestic and overseas, and recent legislation requires all software and hardware vulnerabilities discovered by its own cyber security industry to be run through the MSS, allowing them to cherry pick high value vulnerabilities, which can be turned into exploits used in cyber espionage campaigns.

Additionally, recent bans on Chinese researchers attending foreign cyber security conferences and bug bounty events means that China has become all take and no give when it comes to global cyber security measures.

I'd like to take a step back and briefly address the two specific cases I brought up earlier. The first is the case of Wicked Panda, or APT41, and specifically the defendant Tan Dailin, or Wicked Rose, as he's known online. They are believed to be a bunch of contractors operating on behalf of the MSS and have conducted cyber espionage campaigns against over 100 global firms.

Tan is the perfect example of how the PRC was able to early on leverage its domestic patriotic hacking talent to supplement a relative lack of in-house talent among its intelligence agencies. His story also demonstrates that there appears to be a revolving door for talented intrusion operators between the PLA, the MSS, and China's foremost cyber security firms, as he would work for all three over his career.

Tan was first a central figure in the 2001 U.S. Sino hacker war. Then while attending Sichuanese universities, he formed close ties with the developer of PlugX, a very popular malware deployed by Chinese cyber actors, as well as other skilled patriotic hackers, eventually forming his own hacking group out of his dorm room.

Tan and his early associates were likely approached by the PLA's Chengdu Technical Reconnaissance Bureau to conduct some of these intrusions from at least 2005 to 2007, specifically against DoD networks. Tan was the author of the Jin Wi rootkit, which was used in several intrusions under the Titan Rain nomenclature.

This internship for the PLA likely proved to be a launching point for the careers of several Wicked Panda associates which would go on to work for Yanlong Tech, a company tasked with making China's gaming industry globally competitive.

Tan was actually arrested in 2009 by the MPS, which demonstrates that his criminal history did not actually appear to hinder his ability to later contract for the MSS, and may in fact have been an opportunity for him to serve a reduced sentence in exchange for using his technical skillset for state-directed use.

They also showed that Wicked Panda actors continued to use their for-profit criminal activities on the side of their contracting gigs on behalf of the state, even employing ransomware and crypto jacking tools on victim networks to monetize their intrusions.

Furthermore, Wicked Panda shows that the MSS is in fact able to synthesize massive amounts of personally identifiable information via big data projects, in this case run by these specific contractors, to conduct follow-on targeting of journalists and dissidents.

This has incredibly grave implications when considering the OPM and Anthem intrusions of 2015, which compromised the information of cleared government workers.

Speaking of OPM, the second case study I'd like to discuss is Turbine Panda, which is a group of contractors and MSS operators in Nanjing responsible for those intrusions, as well as long-running campaigns against the aerospace industry.

Many of you here today may soon experience the results of MSS cyber espionage campaigns if you fly to China within the next couple of years. China's first domestic airliner, the C-919, is a direct beneficiary of some of these Turbine Panda intrusion campaigns conducted against American and European firms to steal proprietary technology.

This series of indictments demonstrates how the CCP uses cyber and human collection methods in tandem to close those key technology gaps. Shortly after announcing a joint venture with many of these American and EU companies to produce the turbine engine for C -- the C-919, the MSS and its contractors began setting up cyber intrusion campaigns to steal the designs and many other foreign manufactured components.

Notably, the operations were conducted in close coordination with human operators, including Xu Yanjun, a senior MSS officer who was eventually lured to Belgium by the FBI and E.U. partners and ultimately arrested.

Xu and other senior MSS officials coordinated efforts to use a USB device to implant malware on these victim networks and afterwards tried to scrub the malware from these networks in an attempt to cover their tracks after a public CrowdStrike blog outed this cyber campaign.

This shows a high level of coordination between two separate collection efforts and demonstrates that these operations are not happening in silos but used as force multipliers to achieve the CCP's goals of global technology supremacy.

The MSS's uses -- use of contractors, many of them sourced from China's early patriotic hacking circles in criminal underground, have led -- have set a dangerous precedent where the PRC allows criminal cyber operators to conduct criminal activity for personal property with impunity.

Left unchecked and without meaningful consequences imposed, this threat has continued to grow and allow these state-affiliated criminal actors to continue these operations.

This includes the March 2021 Microsoft Exchange server intrusions by multiple MSS and PLA affiliated cyber operators, which left many attacked surfaces open for criminal actors beyond China and proves that the CCP has little regard for collateral damage despite regularly pushing an alternative to the traditional rules-based norms in cyber space.

COMMISSIONER BARTHOLOMEW: Mr. Kozy, sorry, can I ask you to wrap up? We're over time.

MR. KOZY: Sure, sure, definitely. Though it has been suggested that the CCP has lost control of these actors, this is a hard pill to swallow.

And as the advanced -- most advanced authoritarian state with unrivaled censorship abilities to control the flow of information, the CCP is absolutely able to control this behavior, and instead has chosen to turn a blind eye to it in exchange for the collection of intelligence.

Yeah, sorry, my timer did reset. So I will skip over my recommendations and allow you to read those instead.

PREPARED STATEMENT OF ADAM KOZY, INDEPENDENT ANALYST, CEO & FOUNDER, SINACYBER

February 17, 2022

Adam Kozy
CEO/Founder SinaCyber, Former FBI and CrowdStrike

Testimony before the U.S.-China Economic and Security Review Commission Hearing on
“China’s Cyber Capabilities: Warfare, Espionage, and Implications for the United States”

Introduction

Members of the commission, thank you for inviting me to appear before you today to discuss the threat posed by cyber espionage operations carried out by the People's Republic of China (PRC). I have been asked specifically to comment on China's cyber espionage goals and the Ministry of State Security's (MSS) role in achieving them. My testimony will examine the MSS's rise in cyber espionage capabilities, timelines of important evolutions in the PRC's intelligence collection strategy, similarities and separation of roles played by both the MSS and the People's Liberation Army (PLA), and the threats it poses to the United States and its allies. In particular, I will use two recent US Department of Justice indictments to illustrate the history and breadth of cyber operations carried out by MSS contractors, and why their future ability to continue these operations is of grave concern. Finally, I will submit several recommendations on steps Congress can take to combat this threat.

Rise of the MSS-Contractor Model

This testimony will illustrate how the MSS's model of using a combination of in-house talent and cyber contractors has won the CCP's favor for engaging in economic-driven cyber espionage. A combination of external factors and internal decisions made throughout the early 2000s made this model preferable to the PLA's former 3rd Department's (3PLA) historically noisier operations and past mistakes. These include:

- A long-planned PLA reorganization conveniently announced at the end of 2015 at a time when Sino-US tensions over cyber espionage were at their highest
- Additional time to combine the capabilities of the 3PLA, responsible for the military's signals intelligence (SIGINT), and the 4th Department (4PLA), responsible for the PLA's EW capabilities
- Successive public exposures of 3PLA units by US private sector cybersecurity firms
- Less corruption and moonlighting activities among the MSS due to an earlier disciplinary investigation period done during Xi Jinping's first years
- Better integration among State-owned Enterprises (SOEs) & private sector
- No military commissioning (PT training, dorms, etc.) enabling easier recruitment
- MSS 13th Bureau's (CNITSEC) integration into the vulnerability mining ecosystem, providing better exploits and tooling
- Cover & domestic surveillance capabilities provided by Ministry of Public Security (MPS)
- Superior provincial recruiting of lead figures in underground hacking groups
- Ability to run domestic cyber conferences and leverage recruitment opportunities
- Plausible deniability

What is uniquely concerning about the threat posed to the US and its allies by the MSS is the blind eye it turns on contract hackers engaging in criminal activity for personal profit in exchange for collection of intelligence priorities, and its ability to leverage China's excellent vulnerability mining ecosystem to hoard exploits for cyber operations. In addition, MSS-affiliated actors such as TURBINE PANDA/APT26 and WICKED PANDA/APT41 have engaged in increasingly brazen big data collection operations (such as OPM), which has been proven to be used by the MSS in future targeting operations. In total, these make the MSS a unique cyber adversary that in many ways has surpassed the smash-and-grab PLA intrusions of the past and created a much more dangerous environment globally when considering intrusions like the recent Microsoft Exchange Server/HAFNIUM exploitation, which opened attack surfaces to a more public audience.

This is not to discount the capabilities of the PLA's newer Strategic Support Force (SSF), which have likely recently improved by integrating both computer network exploitation (CNE) capabilities for espionage, and computer network attack (CNA) capabilities which can prepare potential targets for follow-on destructive attacks in a wartime scenario. However, there has been a marked increase in cyber espionage activity conducted by the MSS and its contractors over the past several years, suggesting its model is more favorable for conducting cyber espionage. To better understand the nuanced reasons for this change, one must examine the early origins of cyber espionage in China.

The Turning Point for Cyber Espionage in China

Though the PRC's electronic warfare (EW) capabilities date back well before 2000, the early 2000s saw a dramatic shift in the Chinese Communist Party's (CCP) view of Computer Network Operations (CNO) and its usefulness as a way to bridge key technology gaps and rapidly gain parity with advanced adversaries like the U.S. in a variety of dual-use technologies (military and private sector) outlined in the CCP's overlapping strategic plans that would otherwise be unattainable without years of research and billions spent on development. The notion that CNO could be used not just as a warfighting capability, but as a modernized extension of its long-running economic espionage campaigns would fundamentally change the PRC's intelligence collection methods over the next two decades.

This shift toward viewing CNO and "hacking" as a key component of intelligence collection was likely caused by an intersection of three major factors during the same time frame:

1. Throughout the late 1990's, PLA doctrine began emphasizing information-centric strategies to help the PRC win future "informatized" wars and developing asymmetric capabilities to disrupt more technologically advanced opponents.
2. From 1997-2001, a new subset of young, patriotic, and technologically savvy Chinese citizens began coalescing in underground hacking communities and using international site defacements as an outlet for perceived injustices against China by foreign nations.
3. From 1998-2003 CCP officials from the PRC's various security apparatuses began experimenting with directed censorship of information on the internet as a way to influence national sentiment in projects that would become the Golden Shield Project and the Great Firewall (GFW).

Within several short years, the CCP recognized that the internet posed a massive threat to the CCP's internal stability, but that if information and the talented youth using the internet for nationalistic purposes could be directed properly it would be a massive boon to establishing control over its populace while advancing China's strategic economic goals.

Dating back to 2003's Titan Rain (a cover term for a series of Chinese intrusions into US and UK government systems), the PLA's former 3rd Department (3PLA) appears to be the earliest and most ardent adopter of CNO for espionage purposes. However, over time the MSS's superior tradecraft, recruiting practices, and important role in China's thriving vulnerability ecosystem would make it the chief threat to a variety of global victims across multiple sectors. Its ascension post-2015 as the PRC's lead entity for economic espionage is likely no coincidence as the PLA began undergoing long-planned reforms which would transform its cyber warfare capabilities, which have been discussed in other panels today.

A Brief Timeline of Important Points in China's Cyber Espionage Evolution

- 1996 - Internet is made available to Chinese homes
- 1997 - Foundation of The Green Army, China's first patriotic hacking group
- 1998 - Chinese authorities begin experimenting with censorship and timing
    - Cult of the Dead Cow releases "Back Orifice Program" and Trojan use increases in China
    - Indonesia Riots and turn toward defacements
- 1999 - Taiwan/Belgrade Embassy Bombings and the birth of Red Hackers malicious intent
    - Green Army goes commercial - Shanghai group becomes NSFOCUS
- 2001 - US/China hacker war over Hainan/EP3 Incident
- 2003 - Microsoft hands source code to the MSS 13th Bureau (CNITSEC), and known contractors Topsec and Venustech
    - Extensive hiring of patriotic hacking groups by PLA, MSS, and private firms
- 2003-2006 - Titan Rain intrusions against US and UK defense networks.
- 2005-2010 - CNE campaigns explode (ShadyRat, GhostNet, HiddenLynx, Aurora, etc.)
- 2008 - Beijing Olympics strengthens MSS standing and alliances between private sector contractors
- 2008-2010 - Intrusions against Tibetan activists and other "Five Poisons" shows MSS involvement
- 2010-2012 - TURBINE PANDA actors (MSS Nanjing contractors) prep C919 campaign
- 2012 - Xi Jinping becomes CCP General Secretary and initiates anti-corruption campaigns, deposing several high-ranking MSS officials
- 2013 - Mandiant releases APT1 report exposing 3PLA 2nd Bureau's Unit 61398 operations since 2006
- 2014 - CrowdStrike exposes PUTTER PANDA, 3PLA 12th Bureau Unit 61486

- 2015 - Xi announces PLA reorganization and creation of PLASSF
    - Intrusions into US Office of Personnel Management (OPM) deemed a massive intelligence boon to MSS (later tied to TURBINE PANDA actors)
- 2016 - Wooyun.org, China's main vulnerability reporting site since 2010, goes dark
- 2017 - FBI arrest of Sakula developer and MSS Officer Xu Yanjun in relation to TURBINE PANDA operations. MSS quietly restricts CN vulnerability researchers from attending overseas conferences
- 2017-Present - An anonymous group called IntrusionTruth begins doxxing MSS-affiliated contractors including GOTHIC PANDA/APT3, STONE PANDA/APT10, AURORA PANDA/APT17, KRYPTONITE PANDA/APT40, and more
- 2018 - Tianfu Cup and several other domestic cybersecurity conferences show significant government backing and controlled vulnerability mining ecosystem
- 2020 - WICKED PANDA/APT41 indictment exposes contractors criminal activity and shows individual involvement in cyber operations can date back to 2001
- 2021 - HAFNIUM intrusions showed exploit was shared rapidly among PLA and MSS-affiliated cyber operators and reckless disregard for criminal distribution

Background on the MSS

Creation and Authority

The MSS was created in 1983 by combining the remnants of the CCP's Investigation Department with the Ministry of Public Security (MPS) components of intelligence and counterintelligence to form a ministry that more wholly focused on gathering foreign intelligence. The fact that it was partially formed from the MPS and its first minister was a former vice minister of the MPS meant that the MSS initially had a hard time finding its identity, often having to compete with the MPS for both separate operational and policy space within the higher echelons of CCP decision-making bodies.

However, the MSS's close ties to the MPS would become increasingly beneficial in the early 2000s, affording both convenient cover for MSS offices, which were often co-located with MPS offices (see Figure 1), as well as providing key insight into both the PRC's censorship apparatuses (GFW) and software review processes. The latter would later allow the MSS's Chinese National Vulnerability Database (CNNVD) to have early access to key vulnerabilities that now make up the exploits used in cyber operations today.

The MSS was believed to have strengthened its position regarding foreign policy decision-making and intelligence under former MSS Minister Geng Huichang (耿惠昌) during the run-up to the 2008 Beijing Olympics and after handling riots in Tibet and Xinjiang, which followed shortly after the games.[1] The Ministry saw a budget increase and an expansion of capabilities,

[1] "New Foreign Policy Actors in China", *Stockholm International Peace Research Institute*, September 2010, http://books.sipri.org/files/PP/SIPRIPP26.pdf

which likely included cyber divisions as beneficiaries, as evidenced by a sharp increase of cyber campaigns directed against dissidents and other “Five Poisons”.[2]

However, a series of defections, perceived intelligence failures, and several high level officials removed over graft during Xi Jinping’s anti-corruption campaigns in 2012 provided institutional setbacks to its ambitions. Geng (now the Deputy Director of the Subcommittee for Hong Kong, Macao, Taiwan and Overseas Chinese) was believed to have been spared by Xi due to his role in uncovering deposed Politburo member Zhou Yongkang’s planned military coup to oppose Xi’s appointment as General Secretary. Geng’s replacement in 2015, Chen Wenqing (陈文清), served in both the MPS and MSS before becoming the deputy director of the Central Commission for Discipline Inspection (CCDI), the watchdog responsible for many of the inspections and arrests that took down previous MSS officials. Chen’s prior career and subsequent appointment as MSS Minister likely represented renewed trust in the MSS by Xi who had already stacked loyalists into key positions among the CCP’s highest echelons. Chen is also believed to have taken the helm right as the PLA began its reforms and its cyber espionage portfolio was likely handed over to the MSS, giving him tremendous control over the rise in cyber intrusions into western systems carried out by the MSS and its contractors.

The MSS derives its authority from the CCP’s State Council (see Figure 2) and compounding legislation in 2014, 2015, and 2017, including China’s National Intelligence Law (国家情报法) made clear requirements that all Chinese citizens and companies (operating in China or Chinese companies abroad) must collaborate with the MSS in gathering intelligence. In addition, all Chinese government departments are required to support its intelligence operations when asked. This provides the MSS with the ability to leverage universities, think tanks, foreign affairs departments, government sponsored overseas educational programs, military liaison programs, friendship and student associations, etc. for operational cover as well as to use them as recruitment platforms. This policy also provides the MSS access to many foreign government officials, scientists, academics, and students.[3,4]

For further reading on the MSS’s history and key personalities I highly recommend “Chinese Communist Espionage: An Intelligence Primer” by Peter Mattis and Matt Brazil. For further reading on China’s whole-of-society approach to espionage and examples of specific espionage cases I recommend “Chinese Espionage: Operations and Tactics” by Nicholas Eftimiades.

How the MSS Sources Technical Capabilities

Like the PLA, which sourced much of its early intrusion capabilities from its burgeoning, tech-savvy patriotic hacker cadres, the MSS is not thought to have had well-developed in-house

[2] The Five Poisons are typically categorized as perceived threats to the CCP’s rule of China and include: Uyghur dissidents, Tibetan dissidents, Falun Gong members, Chinese democracy movements, and advocates for Taiwanese independence

[3] “Chinese Espionage: Operations and Tactics”, Nicholas Eftimiades, *Virtruvian Press*, 2020

[4] National Intelligence Law of the People’s Republic of China (Adopted at the 28th Standing Committee of the 12th National People’s Congress on June 27, 2017.

cyber capabilities in the early 2000s, and sought to recruit from outside sources. The PLA coordinated with SOEs like the China Electronics Technology Group (CETC) and its multitude of subsidiaries (Westone, for example[5]) to throw capture-the-flag competitions at top Chinese universities to recruit hacking talent early on, and by all accounts was relatively successful in this approach (see Tan Dailin in the sections below). An exact timeline on the MSS recruitment of its cyber talent is much harder to pinpoint, but likely began around the same time as the PLA's due to a growing interest in developing its own technical capabilities.

The MSS's true secret weapon turned out to be it's Technical Bureau/13th Bureau, which formed the China Information Technical Security Evaluation Center (CNITSEC/中国信息安全测评中心) in 1998. While ostensibly acting as the government arm entrusted with software and code review, the intelligence agency was able to capitalize and use its access to interface with nearly every single domestic cybersecurity company pursuing government contracts and know first-hand which Chinese technical researchers were discovering top-tier vulnerabilities that could be used in cyber intrusion operations (see Figure 3). If not already familiar with them via CNITSEC, the MSS would come to work closely with many of the Chinese cybersecurity companies that had begun to snap up the early generations of patriotic hackers during the 2008 Beijing Olympics. This included:

- NSFOCUS - the commercial branch of The Green Army, the original Chinese hacking collective
- Topsec - recruited Honker Union of China founder Lin Yong (林勇/Lion)
- Venustech - hired a significant amount of former Xfocus and 0x557 members
- Qihoo 360 - employed legacy figures Yuan Renguang (袁仁广/yuange) and Pan Jianfeng (潘剑锋/pjf)

In addition to having access to a pipeline of China's early hacking talent, CNITSEC's true value would come from providing the MSS with an easy way to cherry-pick high value vulnerabilities directly from the source, which could be turned into exploits for cyber espionage campaigns. CNITSEC was likely doing this as early as 2003 when it was given Microsoft's source code as part of a security agreement between Microsoft and the Chinese government for usage on its networks.[6] This was then renewed again in 2010 with Wu Shizhong (吴世忠) as CNITSEC's director, who was also dual-hatted as the MSS 13th Bureau Director according to state documents from 2009-2013.[7,8] CNITSEC is also in charge of reviewing software for government

[5] https://www.intelligenceonline.com/corporate-intelligence/2020/06/24/westone-top-pla-cybersecurity-and-encryption-supplier

[6] https://news.microsoft.com/2003/09/26/china-information-technology-security-certification-center-source-code-review-lab-opened/a

[7] https://web.archive.org/web/20220208054411/https://www.cert.org.cn:8443/publish/main/49/2012/20120330183806295838762/20120330183806295838762_.html

[8] https://www.crowdstrike.com/blog/two-birds-one-stone-panda/

use, in compliance with the national Cybersecurity Law. In June 2017, Wang Jun, chief engineer of CNITSEC discussed the Microsoft-CETC joint venture and the need for suspension of Chinese government use of Windows 10 Chinese Government Edition until it is "secure and controllable".[9]

Open source analysis in 2017 revealed that CNITSEC and the subordinate CNNVD were likely purposely delaying reporting on specific vulnerabilities allowing operational windows for their usage in cyber operations.[10] Just a short time later, in confirmation, KRYPTONITE PANDA/APT40, a known contractor for MSS Hainan[11] was found to have used high-value vulnerability CVE-2018-0802 as a 0day exploit, a month before it was publicly reported as being discovered by Chinese firm Qihoo 360.[12]

Legitimate security companies are known to receive advance notice of vulnerabilities from Western firms such as Microsoft's Active Protection Partners (MAPP) program, whereby the firms are notified up to a week in advance of upcoming security updates. Several Chinese firms privy to these agreements are believed to have actively abused them in the past, knowing that the initial update merely patches the simple proof-of-concept exploit, leaving a window of opportunity often lasting several weeks for alternative exploitation methods while the vendor continues to roll out security updates to address all vectors.

It is suspected that abuse of this system may have led to a rapid proliferation of proof-of-concept code first turned into an exploit by the HAFNIUM group in January 2021 during the widespread Microsoft Exchange Server intrusions. The original HAFNIUM group was quickly joined by multiple APTs that had access to the exploit, with some likely having access prior to Microsoft's patch release. This hints at an internal domestic vulnerability sharing network as the groups with access included both those with suspected ties to the MSS as well as PLA:

- Tick/STALKER PANDA, a group with suspected ties to the former 3PLA's 4th Bureau (Unit 61419)
- LuckyMouse/EMISSARY PANDA, a group with suspected MSS Shanghai ties
- WICKED PANDA/APT41, a group with known ties to MSS Sichuan contractors
- Tonto Team/KARMA PANDA, a group with suspected ties to the former 3PLA's Shenyang TRB (Unit 65016)

MSS operators are also known to source tools and datasets from underground marketplaces. This has previously included purchasing both datasets that could be used for further intrusion operations or potential human intelligence (HUMINT) operations, as well as malware sales from known cyber criminal vendors. This may account for the variety of tools seen in use by MSS

[9] https://www.uscc.gov/sites/default/files/USCC-Webster-Written-FINALSUBMIT.pdf

[10] https://www.recordedfuture.com/chinese-mss-vulnerability-influence/

[11] https://intrusiontruth.wordpress.com/2020/01/16/apt40-is-run-by-the-hainan-department-of-the-chinese-ministry-of-state-security/

[12] https://www.crowdstrike.com/blog/two-birds-one-stone-panda/

operators and explain why many of them are more advanced than tools typically seen in the domestic Chinese underground marketplaces.

In an example of typical MSS operations, an intrusion into a European target saw MSS officers pay contractors to conduct network exploitation on victim systems. Though the origin of the contractors was unknown, they used tools associated with the Russian underground, conducting lateral movement across the victim systems before turning direct intrusion access over to MSS officers. The objectives of the MSS were unclear in this case, however, the access would allow for easy exfiltration or potential future strategic web compromise activity.

MSS & PLA: Competition vs. Collaboration

Prior evidence suggested that MSS and PLA operations were somewhat in competition for resources as well as for valuable collection on identified targets. Previously, it was believed there was a lack of coordination between APT operations groups and there are plenty of examples in private sector reporting of multiple China-backed adversaries concurrently collecting the same information on the same network with different operators and tooling. However, it is likely this coordination is improving with time and greater control of the PLASSF's cyber actions due to the reorganization.

There have also been observed instances of the MSS stealing potential recruits from the former 3PLA. A candidate who had already been approached by PLA recruiters was enticed to the MSS due to an easier recruitment process, better pay/benefits, and more freedom as non enlisted, which typically meant physical training (PT) for cyber operators unused to it and living in military dorms. MSS recruitment strategies will be discussed further in the next section.

It appears unlikely in the current environment that MSS cyber operations would be used to prep the battlefield for PLA network attacks in a wartime footing. This is largely due to the MSS's role as primary foreign intelligence collector, a role it would likely default to during wartime scenarios, and its use of criminal contractors, which are relatively uneven in their capabilities and methods for conducting CNE. A more likely scenario is that the MSS's various network access via their contractors would be handed over to the PLASSF's CNA units for follow on actions based on MSS recommendations about target value. This would essentially be handing its malware controllers over to the military to centralize its possible attack surfaces. As the PLASSF combines the former 3PLA's SIGINT capabilities and the 4PLA's EW methods, it is likely already conducting intelligence vs. attack value analysis internally to inform its cyber units on whether a target should be collected on or maintain a foothold on its network for future CNA use.

The PLASSF's 311 Base has inherited multiple separate units' prior roles in conducting psychological warfare operations, making it unlikely the MSS would conduct cyber operations for this purpose. However, another likely scenario is that the MSS instructs its various contractors to engage in patriotic hacking of lower tier targets to avoid conflicting with military operations and to cause chaos and confusion. This would be likely a fairly simple task given the history of many of its contractors and their patriotic roots.

Recruitment

Contractors act as both a force multiplier and alternative tradecraft for the MSS. Although open source tools provide the bare essentials needed to meet their collection requirements, contractors greatly augment their technical capabilities and plausible deniability. The MSS appears to extensively favor the use of contractors because it allows for operations to be easily terminated, adds an extra layer of operational security (OPSEC) between the victim and intelligence officers, offers a variety of technical responses to fulfill collection requirements, creates plausible deniability in the event attacks are reversed, and can provide additional technical expertise that may not exist in-house.

Contractors are approached in a variety of ways, sometimes maintaining distance and providing only direction and requirements. Other times partnerships may be formalized via CNITSEC and government contracts. It is assessed that during the Beijing 2008 Olympics, the MSS hired several contractors under the pretext of conducting security evaluations and pentesting. These hackers-for-hire were based regionally and were told to use any means necessary to compromise targets. It is unclear whether any of these contractors were then kept on retainer for future operations after the relationship was established. However, the MSS has since been observed continuing the use of contractors in multiple operations, making it more likely that established agreeable working relationships with specific contractors were formed and those contractors were solicited multiple times.

Recruitment also appears heavily sourced from long-standing patriotic hackers and in many cases blackhat cyber criminals hacking domestically for profit. New laws during the late 2000s gave new powers to the MPS and MSS to pursue cyber criminals domestically, and it is believed that many of these same individuals came under legal scrutiny or were arrested. It is suspected several were released in exchange for rendering their skills to the state for cyber espionage purposes, and subsequently allowed to continue their criminal activities as long as they targeted victims outside China. See the “Evolution” section below for an example of this.

Various domestic Chinese hacking conferences from 2008 onward demonstrated that there seemed to be an almost revolving door between China’s early patriotic hacker groups, the PLA, MSS affiliated entities like CNITSEC, and various private sector companies later proven to have worked for China’s intelligence services. Security conferences like XPwn2017, a Beijing conference sponsored by Baidu and legacy patriotic hacking team Xfocus, partnered with CNNVD, Venustech, Alibaba, Pangu Team (China’s top iOS jailbreaking team), and Knownsec (another security company founded by legacy Chinese hackers).[13] Its main consultants featured (see Figure 4):

[13] http://xpwn.xfocus.net/

- HUANG Xin (黄鑫) aka *Glacier* of Xfocus, —the author of China's first domestic remote access tool (RAT) and listed as the Chief Technology Officer (CTO) of Big World (大成天下)
- ZHOU Jingping (周景平) aka *Superhei* of Ph4nt0m Security Team—Chief Security Officer (CSO) of Knownsec
- LIU Hongyun (刘鸿运)—Deputy Chief Engineer of CNITSEC
- ZHU Qianghang (朱钱杭) aka *Pineapple* of Venustech Active Defense Lab
- WEI Qiang (魏强), aka *Funnywei* of Xfocus who has taught cyber operations for the PLA Information Engineering University
- HAO Yongle (郝永乐) of the CNNVD Operations Management Center

Conferences like XPwn and Tianfu Cup are known fertile recruitment grounds for the MSS and even the PLA as it provides ample opportunity to meet with established hacking teams, skilled individual operators, and university students. There will be a separate panel following this one that discusses some of the universities the MSS and PLA use as recruiting grounds.

Contractors are likely provided ample financial compensation for their efforts, though China likely struggles from the same private sector "brain drain" effect given China's top tech firms have significantly higher salaries and freedom. However, the MSS has an advantage of being able to co-opt talent if they wish, especially if an individual's cyber activities conducted during their youth fall under criminal activity.

Prior to 2017, skilled vulnerability researchers at BAT and Qihoo 360 were able to double up on prize money by reporting it domestically and then winning competitions like Pwn2Own abroad to receive prize money from western security vendors. While Chinese dominance in these competitions was notable to western researchers, it still provided top security vendors with access into the kinds of vulnerabilities China was producing. The post-2017 arrangement damages this process and gives even more vulnerability hoarding power to the MSS. As a result, the MSS and specifically CNITSEC likely needed to increase their prices as part of the 2017 restriction on Chinese vulnerability researchers reporting to foreign vendors before reporting to the MSS. In addition, it is believed that many of these security researchers or MSS contractors were barred from leaving China after 2017 and the arrest of the Sakula developer following his attendance at a US security conference.

It is unclear the exact type of "immunity" contractors that also hack for profit are given if they conduct operations on behalf of the MSS. Immunity is a loaded term in China, where senior t retired CCP officials once thought immune to purges were made low again under Xi Jinping's rule to prevent outsized influence over current politics. Immunity in this case is much more likely to represent the MSS and MPS turning a blind eye to these criminal activities rather than providing lifelong immunity. This makes the relationship between blackhat contractors and the MSS a tenuous one, based mostly on those criminals conducting their activities outside of China to prevent a conflict of interest where the MSS and MPS need to protect Chinese citizens from their own operators. This is likely why there is a rise of tactics like ransomware and crypto-jacking against foreign targets from several Chinese actors.

Collection Priorities for PRC Intelligence & Subsequent Tasking

There are numerous fantastic resources that are publicly available and show how China's multitude of concurrent plans including the 863 & 973 Plans, Five Year Plans, Made in China 2025 (MIC2025), Space Science & Technology in China: A Roadmap to 2050, and more, which all create an overlapping tapestry of key technology gaps. Some of the highlights of China's priorities from recent plans include:

- **Alternative Energy** - Solar, Wind Turbines, Hybrid/electric cars
- **Biotechnology** - Biomanufacturing, Biopharmaceuticals, Genetically modified organisms, Infectious disease treatment, Cutting-edge vaccines and drugs
- **Defense -** Aerospace & Aeronautical Systems, Armaments, Marine Systems, Radar, Optics, Space infrastructure and exploration technology
- **High-end Manufacturing** - Chemical Manufacturing, Advanced robotics, Aircraft engines, High-performance composite materials, Integrated circuit manufacturing equipment and assembly technology
- **Technology** - Artificial intelligence, Big data analysis, High-end computer chips, Network equipment, Quantum computing and communications, Rare-earth materials

These technology gaps ultimately get broken down into more specific intelligence requirements that the PRC's intelligence agencies are then tasked with collecting. For collection, the MSS and PLA likely share common parent in the form of the State Administration of Science, Technology and Industry for National Defense (SASTIND/国家国防科技工业局). See Figure 2 for an organizational chart. Within SASTIND there are likely two departments responsible for developing and tasking technology related intelligence requirements, and for collecting intelligence against those requirements.[14]

- The Comprehensive Planning Department, which tasks collection to the MSS and most likely, the PLA, Joint Intelligence Bureau.
- The International Cooperation Department, which has its own independent collection capability. Members of this department travel with PRC scientists to collect information against specific requirements.

After tasking from SASTIND, it is unclear how the MSS or PLA divvy up requirements or whether they compete on objectives (competition between the two has thus far only been observed publicly on an operational basis).

One key factor sets PRC intelligence gathering apart, which is that it takes a whole-of-society approach to collection. Prior anecdotes about "grains of sand" aside, the MSS is able to

[14] Chinese Espionage: Operations and Tactics", Nicholas Eftimiades, *Virtruvian Press*, 2020

influence Chinese companies, overseas students, professors, scientists, and the overseas Chinese diaspora to assist in intelligence gathering efforts, and has been shown to leverage all of them as both cover and collection agent. The PRC's National Security Law compels assistance when required, and the MSS, like its domestic partner the MPS, has been known to pressure family members residing in China to force actions of those abroad.

This is a force multiplier when combining the MSS's ability to conduct human intelligence (HUMINT) and cyber operations in concert. That ability will be discussed in the "HUMINT + Cyber" section.

Evolution: Chinese Patriotic Hacker → PLA → MSS → Private

This early evolution of how the PRC leveraged its early patriotic hacking groups to supplement its lack of in-house talent is best viewed through the lens of one individual who has been present throughout this entire process: Tan Dailin (谭戴林) aka WickedRose. A September 2020 US DoJ indictment against several members of the WICKED PANDA/APT41 featured Tan and several co-conspirators who had conducted over 100 documented intrusions into global companies over the course of a decade.[15] My own research around this indictment and actor led me to discover the untold story of how Tan evolved from an angsty patriotic hacker at university, to the leader of a group of contract hackers for hire for the PLA, an MSS contractor, and eventually a savvy cybersecurity entrepreneur (see Figure 5).

Tan was a central figure in the early 2000s Chengdu patriotic hacking scene and a notable member of the Evil Octal Security Team. While attending Sichuan-area universities, he formed ties with Zhou Jibing (赵纪斌) aka WHG, the developer of PlugX[16], a remote access tool (RAT) that would later be favored by a majority of Chinese APT groups from 2012-2016[17]. Tan's skills as a developer and intrusion operator led to him founding the Network Crack Program Hacker (NCPH) group out of his dorm room while at the Sichuan Institute of Science and Engineering/Sichuan University of Science and Technology (SCIT/四川理工学院). Tan and Zhao worked to develop the NCPH rootkit, which was also known as GinWui. The variant GinWui.A is believed to have been an early precursor to PlugX, which was later licensed out to multiple APT groups for use in offensive campaigns against western systems. This suggests both a common supply chain entity providing these tools across PLA and MSS lines, and that Zhao was likely paid to continue to develop and refine his malicious code into first PlugX and later the evolved Clambling RAT over several years and cycles of development.

[15] https://www.justice.gov/opa/pr/seven-international-cyber-defendants-including-apt41-actors-charged-connection-computer

[16] https://cybersecurity.att.com/blogs/labs-research/the-connection-between-the-plugx-chinese-gang-and-the-latest-internet-explo

[17] https://www.blackhat.com/docs/asia-14/materials/Haruyama/Asia-14-Haruyama-I-Know-You-Want-Me-Unplugging-PlugX.pdf

Tan applied to graduate school at Sichuan University in 2005. It was during his time there that Tan is believed to have been approached by the PLA, which found him via his blog and his attempted intrusions into Japanese systems. In September 2005, he was encouraged to participate in a Network Attack/Defense Competition where he and his team won first place.[18] Tan was found by the Chengdu Military Militia Information Sub-Unit—a unit that likely served as recruitment spotters for the former 3PLA Chengdu Military Region (MR) 1st Technical Reconnaissance Bureau (TRB) Unit 78006, which was later implicated in the Titan Rain attacks against the U.S. government.[19]

Following the competition in October 2005, Tan and his team of former NCPH colleagues participated in an intensive 16-hour-a-day, month-long training period with the PLA designed to simulate attacks, design hacking tools, and develop training courses for network infiltration strategies. It is assessed that these efforts greatly improved PLA cyber operations at the time.

In the spring of 2006, Tan continued to refine the Ginwui rootkit before dropping out of school on 30 April 2006 to pursue state-directed intrusion operations full time. From May through September 2006, Tan and the NCPH crew likely conducted CNE operations directed against the U.S. DOD on behalf of the PLA. The intrusions at the time were unprecedented and are some of the first examples of the PLA (and by extension the CCP) paying the salaries of hackers for hire to conduct CNE against the U.S.[20]

From the timing of Tan's blog posts during these intrusions, it is clear the PLA provided lodging and salaries to several young Chinese hackers as part of this campaign. Included among those mentioned as "colleagues" on Tan's posts was *Blackfox*, the alias of fellow indicted WICKED PANDA member Jiang Lizhi (see Figure 6).[21] In 2007, Jiang would go on to work for offensive cyber PLA contractor Yanlong Tech, a technology firm regularly targeting the gaming industry—which is assessed to be activity roughly analogous to early Winnti Group operations against multiple Asian and western gaming firms. It is unclear whether Tan and Jiang had met prior to this hacking "internship" with the PLA, but it is likely this served as a common thread for their future endeavors together as well as the reason Yanlong did early work for the Chengdu MR TRB. Tan would join Yanlong reportedly only in 2011, but Jiang stayed until 2014 when he left to start Chengdu 404, the other contracting entity outlined in the 2020 DoJ indictment.
Details from Tan's personal blog show that he also disliked his time at Sichuan University and was merely there to get his degree, much preferring his "internship" colleagues and time spent hacking. Tan's own former university in Zigong listed him among accomplished students for winning first place in the first national computer network offensive/defensive competition and earning the "first-class merit award" from the PLA Chengdu MR. Other records show he competed in the Chengdu Westone Cup and took second place in 2006. Westone is a

[18] https://www.hsgac.senate.gov//imo/media/doc/042809Paller.pdf?attempt=2

[19] https://web.archive.org/web/20120822123730/http://www.time.com/time/magazine/article/0,9171,1692063-2,00.html

[20] Dunham, Ken, and Jim Melnick. "Wicked Rose" and the NCPH Hacking Group. fserror.com/pdf/WickedRose_andNCPH.doc

[21] https://web.archive.org/web/20060712163357/http://www.mghacker.com:80/default.asp?cateID=1

subsidiary of the China Electronics Technology Group Corporation's (CETC) Network Information Security Company and of the CETC 30th Research Institute in Sichuan. CETC is a known state-owned enterprise (SOE) and benefactor and potential driver of Chinese CNE and intellectual property theft; the organization has conducted classified work on behalf of the PLA and MSS.

In April 2009, several Chinese forums reported that Tan was arrested by the Ministry of Public Security (MPS) after he reportedly conducted Distributed Denial of Service (DDoS) attacks and blackmailed users of other popular hacking forums such as Hackbase, the magazine HackerXFiles, and 3800hk. Members of these groups are believed to have turned him into the authorities. He faced 7.5 years in jail, however it is unclear whether he actually served any of the time.[22]

Given the DoJ indictment information that he contracted for the MSS more recently, one potential theory is that due to his prior military contracting service, the MSS made him a plea deal to continue hack-for-hire intrusion activity in exchange for commuting his sentence. Tan is suspected to have reappeared in 2011 when he worked for Yanlong Tech using the alias *Blackwolf*, reuniting with his former associates *Blackfox* and *EvilC0de*. The firm appeared to have strong ties to the gaming community and due to prior five year plans outlining the CCP's desire to become a major global force, it is believed many of the team members used their experience working with kernel-level vulnerabilities modding games to conduct intrusion operations and target Asian and western gaming firms to steal technology and monetize in-game currency.

It is unclear why Tan left after barely a year at Yanlong, but he wasted no time getting back to his criminal roots by setting up a fake antivirus firm named Anvisoft.[23] Although the firm purported to offer a security product, given Tan's concurrent activities, it is likely this was a front company for other activities and that Tan began contracting for the MSS around this time.

Tan's activities after 2012 are less readily accessible despite his fame. This is potentially due to his online presence being scrubbed by the MSS. Registrant data for emails tied to Tan suggest he was still active as a MSS contractor and consistently registering domains from 2012 to 2019—though none that were immediately traceable to WICKED PANDA/APT41 activity. This is potentially indicative of him using third parties for domain registration given his own notoriety by that point.
Legal records show that from a period from June 2010 to at least April 2020, Tan was busy registering several private technology firms with various focuses, serving as a legal representative, technology director, investor, and CEO at several firms. Tan was still in Chengdu during this period as evidenced by both the firms he registered and also the technology patents filed under his name.

[22] https://web.archive.org/web/20160506182604/http://www.thedarkvisitor.com/2009/04/withered-roselaw-donecome-and-got-him/

[23] https://krebsonsecurity.com/2012/11/infamous-hacker-heading-chinese-antivirus-firm/#comments

Tan’s path follows many famous legacy Chinese hackers who served as contractors or educators for various state-backed entities in the late 2000s before becoming entrepreneurs in China’s burgeoning cybersecurity scene throughout the 2010s. As demonstrated in countless other companies claiming to do only whitehat security work on behalf of the Chinese state, many of the upper echelon of China’s cybersecurity companies have close ties to the CCP and conduct offensive operations as well as providing defense. Some of these firms, such as Threatbook and Qihoo 360, have established themselves as defensive cybersecurity organizations, but they likely also engage in offensive intrusion activities and/or vulnerability research on behalf of the CCP. Former Qihoo 360 executive Tan Xiaosheng (谭晓生) served as a director at one of Tan’s own firms and has been previously implicated along with Qihoo for his ties to the MSS 13th Bureau/CNITSEC.

Also of note in these indictments against WICKED PANDA/APT41 was their collection of data during their intrusion campaigns which fed into a big data repository tool Tan’s co-conspirators called SonarX. These actors were particularly skilled at extracting personally identifiable information (PII) during their intrusions and finding a way to monetize it via this platform. Furthermore, the case showed that not only are breaches like these collecting the data, but that the data sets are being organized and used for follow-on targeting of dissidents, journalists, and religious figures. This proves the MSS is likely capable of using data gleaned from other breaches such as 2015’s OPM breach to create targeting packages for both future cyber and HUMINT operations.

MSS Use of HUMINT and Cyber Operations in Tandem

Another recent DoJ/FBI case that brilliantly shows how the MSS operates is a series of indictments tied to a set of cyber operators named TURBINE PANDA/APT26. This actor and its campaigns stand out for several reasons:

- The case resulted in the first US arrest and extradition (in partnership with EU-based authorities and allies) of a high-ranking MSS intelligence officer.
- It demonstrated the MSS’s ability to use HUMINT operations and insider threats in tandem with cyber espionage campaigns to great effect (See Figure 7)
- MSS’s HUMINT and cyber operators frequently communicated and even attempted to cover one another’s tracks, demonstrating a high degree of coordination.
- MSS cyber operators were likely made up of a mixture of in-house talent and outside contractors, many of which have traceable backgrounds to various Chinese patriotic hacking groups.
- TURBINE PANDA’s multi-year cyber campaign systematically targeted various aerospace firms that made up the supply chain for foreign-sourced parts for China’s C919 airliner.

- TURBINE PANDA operators also played a role in conducting the OPM intrusion, likely as part of the MSS's big data collection efforts to map US cleared government employees.
- The timescale for these operations happened in quick succession; Chinese aerospace firms had barely inked joint ventures with western firms before operational prep began.
- The totality of identifying key technology gaps, cyber campaigns, HUMINT operations, malware development/usage, and eventual arrests offered a rare glimpse into the full Chinese intelligence cycle from tasking to collection, analysis, and eventually a state-backed beneficiary.
- The aftermath showed an immediate reaction from the MSS from 2017 onward, which banned many security researchers from traveling to overseas conferences and codified CNITSEC's ability to harvest domestic vulnerability research for use in exploits. If anything this likely increased the potency of MSS cyber capabilities.

A major focus of the CCP in the late 2000s was a Chinese-built commercial aircraft designed to compete with the duopoly of western aerospace and keep pace with China's exponentially growing middle class and their travel needs. That aircraft would become the C919—an aircraft roughly half the cost of its competitors, and which completed its first maiden flight in 2017 after years of delays due to design flaws. But the C919 can hardly be seen as a complete domestic triumph as it is reliant on a plethora of foreign-manufactured components (see Figure 8 for an incomplete list). Likely in an effort to bridge those gaps, TURBINE PANDA conducted cyber intrusions from a period of roughly 2010 to 2015 against a variety of companies that make up the C919's supply chain.

Specifically, in December 2009, the state-owned enterprise (SOE) Commercial Aircraft Corporation of China (COMAC/中国商用飞机有限责任公司) announced it had chosen CFM International's (a joint venture between U.S.-based GE Aviation and French aerospace firm Safran, formerly Snecma) LEAP-X engine to provide a custom variant engine, the LEAP-1C, for the then-newly announced C919. The deal was reportedly signed in Beijing during a visit by then-French Prime Minister François Fillon.

Despite the early deal with CFM, both COMAC and fellow SOE the Aviation Industry Corporation of China (AVIC/中国 航空工业集团公司) were believed to be tasked by China's State-owned Assets Supervision and Administration Commission of the State Council (SASAC) with building an "indigenously created" turbofan engine that was comparable to the LEAP-X. In August 2016, both COMAC and AVIC became the main shareholders of the Aero Engine Corporation of China (AECC/中国航空发动机集团), which produced the CJ-1000AX engine. The CJ-1000AX bears multiple similarities to the LEAP-1C, including its dimensions and turbofan blades.

The AECC conducted its first test in May 2018, having overcome significant difficulties in their first mockups. Though it is difficult to assess that the CJ-1000AX is a direct copy of the LEAP-X without direct access to technical engineering specifications, it is highly likely that its makers benefited significantly from the cyber espionage efforts of the MSS, knocking several years (and potentially billions of dollars) off of its development time.

From August 2017 until October 2018, the DoJ released several separate, but related indictments against Sakula developer Yu Pingan[24], JSSD Intelligence Officer Xu Yanjun[25], GE Employee and insider Zheng Xiaoqing[26], U.S. Army Reservist and assessor Ji Chaoqun[27], and 10 JSSD-affiliated cyber operators in the Zhang et. al. indictment[28]. What makes these DoJ cases so fascinating is that, when looked at as a whole, they illustrate the broad, but coordinated efforts the Jiangsu State Security Department (JSSD) in Nanjing took to collect information from its aerospace targets. In particular, the operations connected to a TURBINE PANDA showed both traditional human-intelligence (HUMINT) operators and its cyber operators working in parallel to pilfer the secrets of several international aerospace firms and even the data from OPM.

It is believed that cyber targeting of aerospace firms by TURBINE PANDA cyber operators began in January 2010, almost immediately after the LEAP-X engine was chosen for the C919. The Zhang indictment describes initial preparatory action using doppelganger sites to conduct strategic web compromises (SWC) in combination with DNS hijacking to compromise various aerospace firms using two China-based APT favorite pieces of malware, PlugX and Winnti, and malware assessed to be unique to the group dubbed Sakula.

The same ZHANG indictment indicates that these operations were overseen by CHAI Meng (柴萌), who likely managed the JSSD's cyber operators as a pseudo Cyber Section Chief. Reporting to CHAI was the cyber operator team lead, LIU Chunliang (刘春亮/sxpdlc1r/Fangshou), who appeared to establish and maintain much of the infrastructure used in the attacks on various aerospace targets as well as organize the intrusions conducted by the operators Zhang Zhanggui (张长贵/leanovr/leaonr), Gao Hongkun (高洪 坤/Mer4en7y), Zhuang Xiaowei (庄臬伟/jpxxav), Ma Zhiqi (马志琪/Le Ma), and Li Xiao (李潇/zhuan86). Many of these individuals are assessed to have storied histories in legacy underground hacking circles within China dating back to at least 2004. Notably, Liu also appeared to broker the use of Sakula from its developer Yu, as well as the malware IsSpace (associated with SAMURAI PANDA) from its developer Zhuang. Liu and Yu's conversations about Sakula would be a critical factor in tying all of this disparate activity together as Sakula was believed to be unique to the JSSD operators and could be used to tie several aerospace intrusion operations into a single, long-running campaign as well as the OPM intrusions.

[24] https://regmedia.co.uk/2017/08/24/yu.pdf
[25] https://www.justice.gov/opa/press-release/file/1099881/download
[26] https://www.justice.gov/opa/pr/new-york-man-charged-theft-trade-secrets
[27] https://www.justice.gov/opa/press-release/file/1096411/download
[28] https://www.justice.gov/opa/press-release/file/1106491/download

Simultaneously, there was a HUMINT element to the JSSD's espionage operations against aerospace targets. Xu Yanjun, was identified in his indictment as the Deputy Division Director of the Sixth Bureau of the JSSD in charge of Insider Threats. Xu affiliated himself with two cover organizations—Jiangsu Science and Technology Association (JAST) and the Nanjing Science & Technology Association (NAST)— when interacting with potential targets. Xu also was reported as frequently associating with the Nanjing University of Aeronautics and Astronomics (NUAA), a significant national defense university controlled by China's Ministry of Industry and Information Technology (MIIT), that interfaces directly with many of China's top defense firms and state-owned enterprises. It is likely no coincidence that NUAA is a regular collaborator with state-owned enterprises (SOEs) COMAC and AVIC, the main shareholders of AECC, which went on to produce the LEAP-X inspired CJ1000-AX turbine engine for the C919.

Over the course of several years, Xu would recruit both an insider at LEAP-X manufacturer General Electric (GE), Zheng Xiaoqing, and a Chinese-born Army reservist, Ji Chaoqun (季超群). Zheng's background appears to have made him uniquely qualified to accurately assess turbine engine schematics, and it was clear from his indictment that he had received coaching on which sensitive information on GE's turbine technology to access and how to use steganography in an attempt to exfiltrate the information. Ji, who entered the U.S. on an F-1 student visa to study electrical engineering in Chicago, was approached by Xu (initially undercover as an NUAA professor) in December 2013 and eventually recruited to provide assessments on other high-value individuals in the aerospace industry for potential recruitment by the MSS. Ji's position in the U.S. Army Reserve program known as Military Accessions Vital to the National Interest (MAVNI) provided a perfect cover for Ji's assessment activities, as the program focuses on potential recruitment of foreign citizens with skills pertinent to national interest and legally residing in the U.S. Had it been successful, JI would have been handing Xu other foreign-born recruitment candidates as they were about to enter U.S. military service on potentially sensitive projects.

Exposure

As the frequency of MSS operations increased and attention shifted from the PLA during its reorganization, a mixture of anonymous reporting from a group called IntrusionTruth, private sector reporting, and DoJ indictments have shed more light on the MSS's cyber operations. However, most notably, these repeated exposures do not appear to be actively hindering continued activity from MSS contractors, which have only gotten more brazen in their recent activities.

Beginning in May 2017, the first public exposure of MSS-affiliated entities came from an anonymous group known as IntrusionTruth in the form of blogs and a twitter account dropping (sometimes dubiously sourced) series of posts detailing personal details of MSS cyber contractors and the breadcrumbs they'd left behind during their prior intrusion efforts. Over the course of several years they would out individuals tied to groups known in the private sector as

GOTHIC PANDA/APT3, STONE PANDA/APT10, AURORA PANDA/APT17, KRYPTONITE PANDA/APT40, and other lesser known entities. These were roughly tied to provincial and national level MSS bureaus and CNITSEC offices in Guangdong, Tianjin, Jinan, and Hainan respectively. Though sometimes presented haphazardly in blog posts, multiple private sector firms' work including CrowdStrike, Mandiant, and RecordedFuture appeared to frequently corroborate IntrusionTruth's releases. In addition, several released DoJ indictments followed these mysterious releases, further corroborating that the US government knows about many of these actors and their backgrounds.

I will refrain from commenting much further on IntrusionTruth as anonymity is key to their continued successful operations. The MSS has previously proven it has no issues publicly executing spies or those assisting foreign powers, and their very existence is likely perceived as a threat to the CCP.[29] However, I do believe good work is being done here and it is breaking down some of the existing barriers between private sector cyber intelligence and the federal sector, which ultimately leads to more future collaboration.

Integral work is currently being done by all the mentioned parties to identify these threats and prevent them from harming US interests. However, more work is needed to assist these efforts with funding and new policies centered around collective defense, active defense/offense, and education of our partners, allies, and our workforces.

Recommendations

The CCP has managed to absorb new technology and strategy the U.S. has pioneered (the Internet, EW usage in the Gulf War, Cult of the Dead Cow's use of Trojans, Microsoft's source code, destructive cyberweapons, etc.) and turn it into an asymmetric advantage. In a way, rampant Chinese cyber espionage is a monster of our own creation, but it is one that can at least be curbed through carefully considered policy adjustments.

One thing is painfully clear: the strategy of "Name & Shame" does not work, and the CCP's constantly regurgitated response asking for proof and the US complying is akin to handing China a report card on their intelligence gathering capabilities. Robust, two-way policies for sharing of threat actor information across the private and federal sector, as well as between international intelligence partners can still be incredibly useful. But naming and shaming in hopes of embarrassing China into changing its behavior is not the effective deterrent or panacea it was perhaps naively hoped to be under rule of Xi Jinping.

My recommendations, while numerous, look to combat China's whole-of-society approach to gathering intelligence with our own multi-faceted active defense approach. It draws upon

[29] "Chinese Communist Espionage: An Intelligence Primer", Introduction, pg. 1, Peter Mattis and Matthew Brazil, Naval Institute Press 2019

frustrations myself and many other hard-working patriots in both the federal and private sector have experienced when trying to combat this threat for well over a decade. This involves a strategy of hardening defenses, providing *meaningful* consequences that impose costs to APT groups, and education of our partners and domestic assets.

Harden Defense

- Invest in better software solutions and data centers to un-silo and share data between domestic agencies and commercial businesses. Some collaboration is happening between CISA and information sharing and analysis centers (ISACs), but it is disparate, usually depends on interpersonal relationships, and data is fragmented from company to company (i.e. hard to utilize effectively for collective defense). This needs to go beyond CISA and should involve several government agencies and counterintelligence stakeholders.

- Re-examine intelligence classification methods for data sharing purposes. As demonstrated in several of the aforementioned DoJ cases, much of the data concerning Chinese intrusions are “overclassified”, which unnecessarily gate keeps relevant parties and hampers collective defense. Sources and methods should remain classified, but most cyber tactics, techniques, and procedures (TTPs) are predominantly discoverable using open source techniques and should be treated as such. Open source centers work and should be more accessible to the private sector.

- Increase intelligence sharing on Chinese cyber espionage with allied international countries to reduce attack surfaces and increase collective defense. The US need not act as gatekeepers of Chinese counterintelligence when a multitude of nations and industries suffer from the same affliction. Encourage two-way sharing of Indicators of Compromise (IOCs) and counterintelligence reports. Improve inter-agency task forces to share internationally, and educate partners on removing bureaucracy from the multitude of cyber departments and stakeholders that currently exist. Publicly promote united stances with partners against China’s cyber espionage activities and more recently destructive actions (HAFNIUM).

- Establish defensive partnership programs via government and private sector cybersecurity firms with Asian allies (Taiwan, Japan, South Korea, Philippines, Vietnam) to hunt, remove Chinese adversaries from their networks, and improve overall defensive posture. Frankly, this should have already started for increasingly critical technology companies such as TSMC and other partners in the semiconductor supply chain.

- Re-shape public and private policies around disclosure of hacks. As both a former FBI and private sector cybersecurity employee I’ve seen a breakdown between the balance of commercial firms trying to prevent stocks from plunging by disclosing an intrusion and counterintelligence efforts getting the timely information they need for national security purposes. Incentivize reporting of intrusions via trusted commercial cybersecurity partners or FBI/DHS and establish meaningful consequences for firms that sweep intrusions under the rug or attempt to cover them up. Reporting should be mandatory for commercial firms receiving government money, especially defense contracts.

- More defensive options for federal (FBI, DHS) and approved private sector entities to remove attack surfaces and take down (and recover copies of) malicious C2 infrastructure. Increased sharing between federal/private stakeholders to include hosting providers and domain providers. Expand existing sharing relationships to include raw data in addition to technical indicators of malicious activity.

Active Defense/Offense

- More offensive options on a sliding scale for federal (DOD/NSA, CIA) entities to impose cost on known APT groups. Currently, there are no actions happening (or at least publicly known) that have dissuaded Chinese APTs from engaging in cyber espionage. The CCP has done cost/benefit analysis and concluded it is currently too beneficial to its strategic plans to stop these activities or to care about being implicated. In many cases, these individual actors or firms are well-known to US intelligence agencies; we should not be as hesitant to let our own professionals covertly degrade their ability to conduct future operations especially when there is a body of evidence of historical criminal or destructive actions. Tan Dailin/*WickedRose* would easily fall into this category as a two decade repeat offender.

- Add Chinese universities, companies, and conferences providing support to APTs or a proven cyber talent pipeline for the MSS/PLA to the US Commerce Department's Entity List. Consider revoking visas for professors and students from Chinese universities in special cyber and technology programs that are known to receive funding/support from MSS/PLA or have been implicated in prior espionage cases.

- Conduct economic action to include sanctions against known CNITSEC contractors and entities actively supporting Chinese cyber espionage, surveillance of minority groups, and vulnerability miners that fail to report to affected western companies.

- Deputize and create standards and procedures around private cybersecurity companies' ability to assist in deception and denial techniques on behalf of their customers. Think less "letters of marque" and more the model set by the NSA's Accredited Cyber Incident Response Services vendors.

- Draft public policies that protect valuable domestic security researchers from external attacks by foreign APT groups and make targeting them a punishable offense by law. Establish meaningful consequences for foreign intelligence services that seek to harm, intimidate, or disrupt the work of US domestic security researchers. The recent incident involving an anonymous researcher P4x shutting down North Korea's internet in retaliation to personal attacks and a lack of government support comes to mind.[30]

- Work with international law enforcement partners to apprehend and degrade MSS contractor's overseas accomplices or seize laundered funds. This hits select entities in their wallets and makes it more difficult to for them to profit off criminal activity on the side of their MSS operations.

Educate

- Reform the DoJ's "China Initiative" to include more educational resources about MSS/PLA recruitment techniques and the consequences of spying. Students studying abroad are frequent targets of these efforts, but there are little efforts made to educate students from abroad on the potential consequences. Solicit input from Chinese-Americans and trained linguists to make educational videos about PRC intelligence recruitment and pressure techniques, and safe steps to report it to university authorities and the DoJ. Require US universities to establish safe reporting spaces free of reprisal or public ridicule, as there are several cases of Chinese students reporting "unpatriotic" activities to the MSS while abroad, damaging trust in Chinese student associations. These efforts should take maximum effort to not discriminate against Chinese students and professors or impede normal educational exchanges.

- Sponsor "diplomatic track" cyber competitions that promote further sharing between Chinese and western capture-the-flag/cybersecurity groups to reestablish the hacker spirit of healthy competition. Anyone who's attended DEFCON or any less commercial cybersecurity conference will be able to tell you that for the most talented of cyber researchers, they attend to share knowledge and bend technology to their will, free of any patriotic loyalty. Attendees are immune from threat of arrest or prosecution, which encourages their best to attend these events and contribute to cross-country information exchanges and dialogue.

- Coordinate alternate bug bounty programs with western stakeholders (Google, Microsoft, Apple, Meta) to encourage Chinese researchers to responsibly disclose vulnerabilities. Allow Chinese-focused payment methods (Alipay, WeChat/Weixin Pay) with a holding mechanism that pays out only after a designated time period where patching can take place and CNITSEC's ability to cherry-pick vulnerabilities can pass. This encourages more Log4j style disclosures[31] from Chinese tech firms where PRC intelligence is shut out from utilizing high value 0days.

[30] https://www.wired.com/story/north-korea-hacker-internet-outage/

[31] In 2021, an Alibaba employee first reported the now infamous Log4j vulnerability to Apache, bypassing CCP government policies of reporting to CNITSEC first. Why the Alibaba researcher did not report the vulnerability to the government first is unclear, but the company lost a government contract as a result

- Continue to improve, invest in, and boost domestic US cybersecurity talent programs to fill the shortage of qualified professionals. Allocate funding for hiring qualified private sector experts as government consultants and improving federal/private partnership opportunities. Relax drug testing and federal application policies for cyber positions given the rapidly changing legal landscape for marijuana and psilocybin medical use across many states in the US. Former FBI Director Robert Mueller advocated this approach in 2010 anticipating the need to bring on more qualified cyber professionals in the future, and noting how many excellent applicants were turned away based on outdated drug policies.

Appendix and Figures

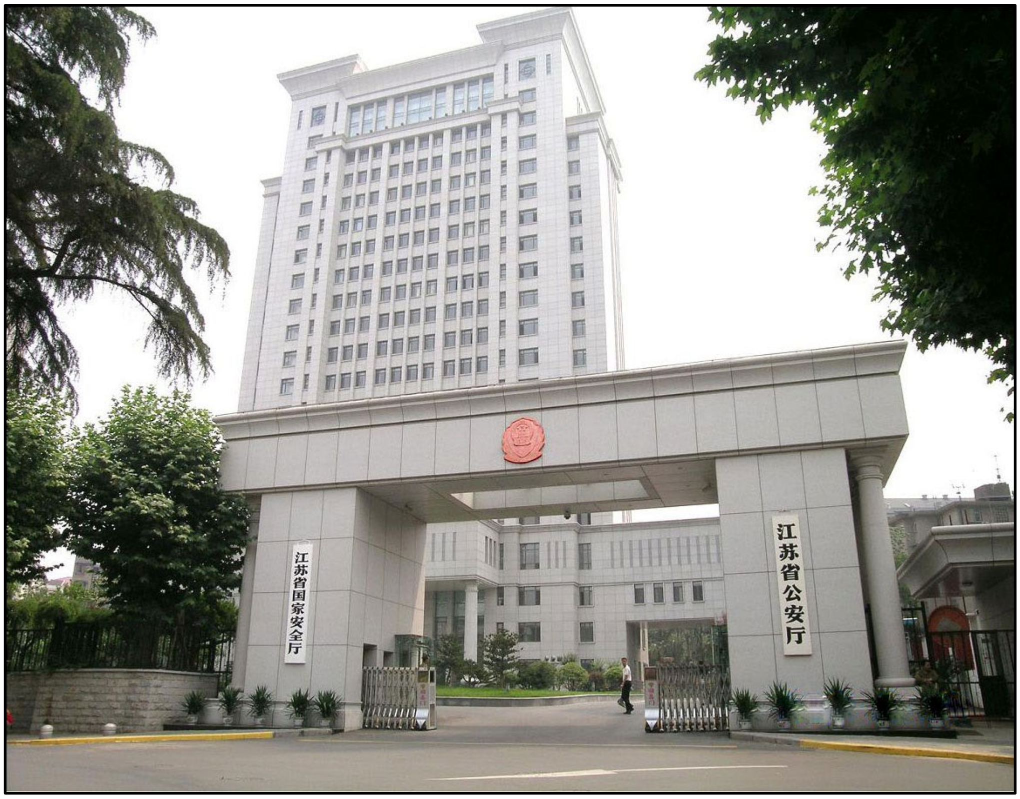


Figure 1. An image showing the MSS often shares buildings with and uses the MPS for cover. This is one of at least two locations cyber contractors known as TURBINE PANDA/APT26 were believed to operate out of on behalf of the MSS Jiangsu Department in Nanjing.

and the employee was likely reprimanded, making researchers hesitant to skip over the government again in the future.

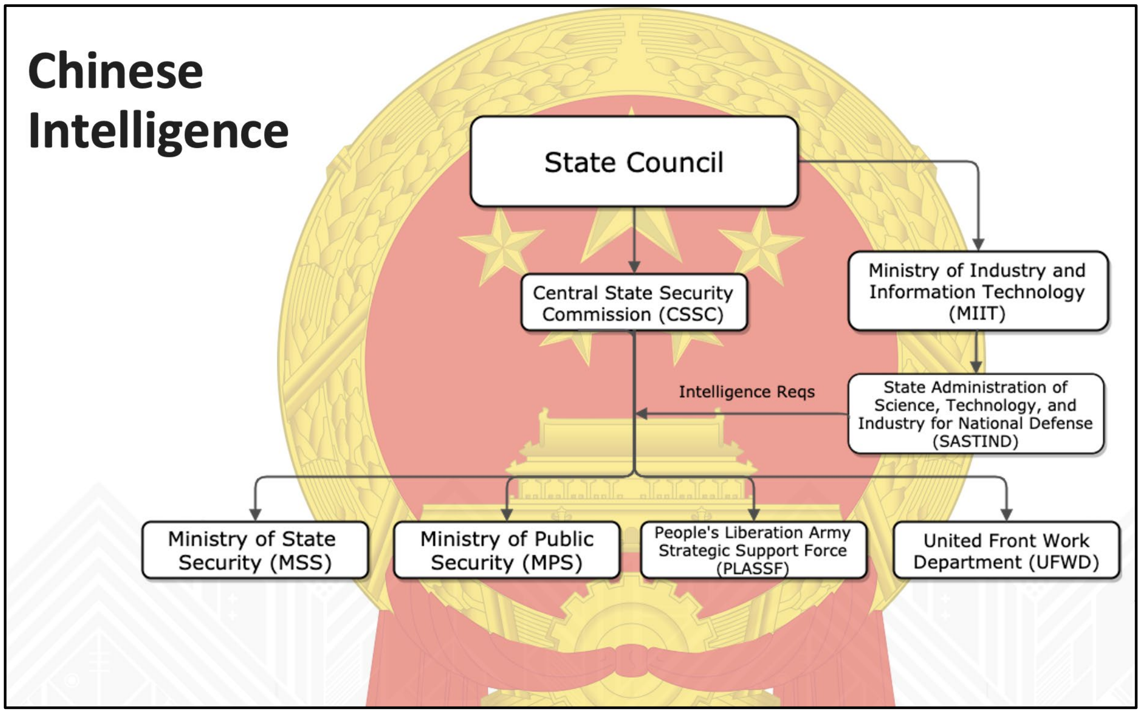
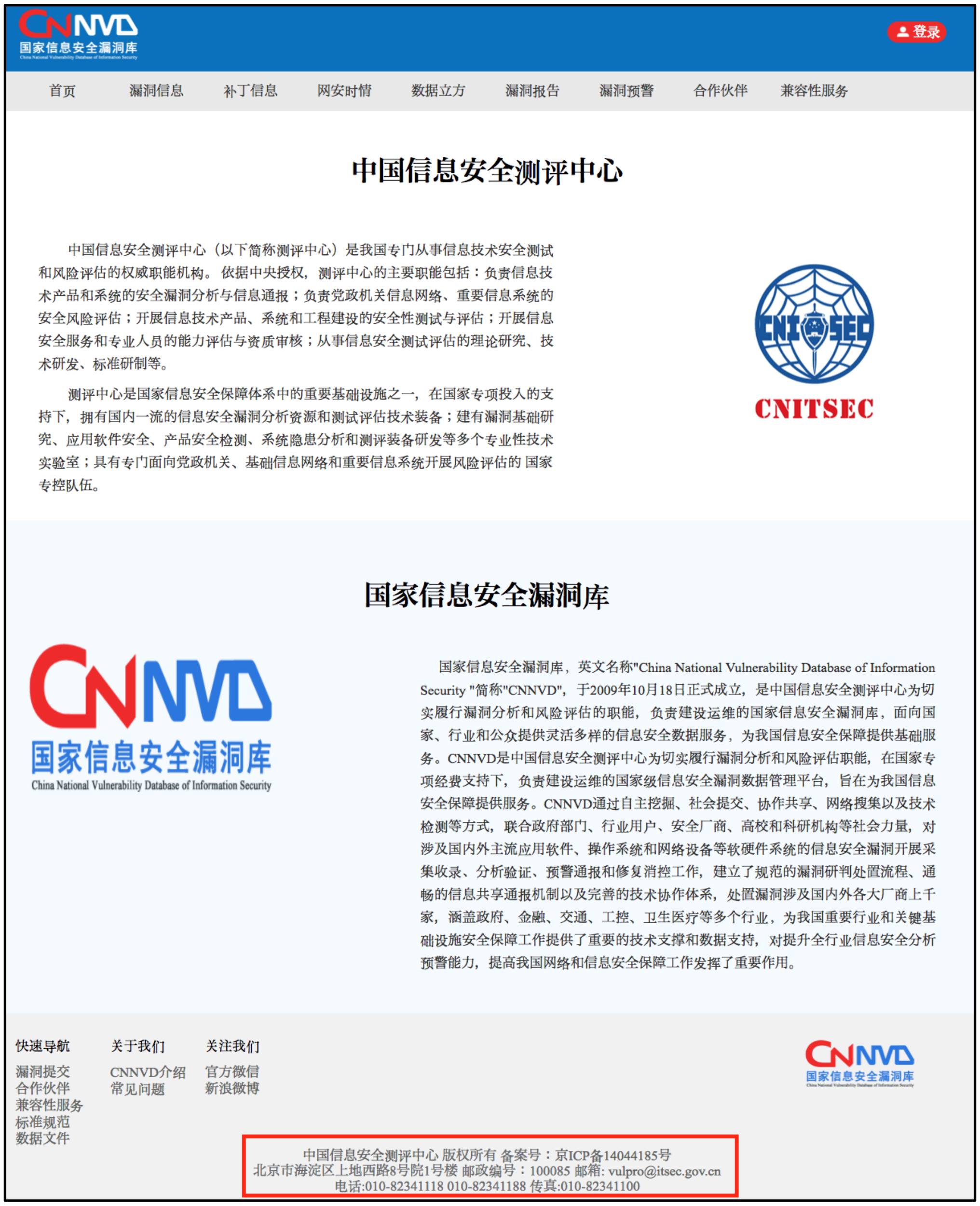

Chinese Intelligence
State Council
Central State Security Commission (CSSC)
Ministry of Industry and Information Technology (MIIT)
Intelligence Reqs
State Administration of Science, Technology, and Industry for National Defense (SASTIND)
Ministry of State Security (MSS)
Ministry of Public Security (MPS)
People's Liberation Army Strategic Support Force (PLASSF)
United Front Work Department (UFWD)

Figure 2. An organizational chart showing where the MSS likely derives its authority and intelligence requirements from.



中国信息安全测评中心

中国信息安全测评中心（以下简称测评中心）是我国专门从事信息技术安全测试和风险评估的权威职能机构。依据中央授权，测评中心的主要职能包括：负责信息技术产品和系统的安全漏洞分析与信息通报；负责党政机关信息网络、重要信息系统的安全风险评估；开展信息技术产品、系统和工程建设的安全性测试与评估；开展信息安全服务和专业人员的能力评估与资质审核；从事信息安全测试评估的理论研究、技术研发、标准研制等。

测评中心是国家信息安全保障体系中的重要基础设施之一，在国家专项投入的支持下，拥有国内一流的信息安全漏洞分析资源和测试评估技术装备；建有漏洞基础研究、应用软件安全、产品安全检测、系统隐患分析和测评装备研发等多个专业性技术实验室；具有专门面向党政机关、基础信息网络和重要信息系统开展风险评估的 国家专控队伍。

国家信息安全漏洞库

CNNVD
国家信息安全漏洞库
China National Vulnerability Database of Information Security

国家信息安全漏洞库，英文名称"China National Vulnerability Database of Information Security "简称"CNNVD"，于2009年10月18日正式成立，是中国信息安全测评中心为切实履行漏洞分析和风险评估的职能，负责建设运维的国家信息安全漏洞库，面向国家、行业和公众提供灵活多样的信息安全数据服务，为我国信息安全保障提供基础服务。CNNVD是中国信息安全测评中心为切实履行漏洞分析和风险评估职能，在国家专项经费支持下，负责建设运维的国家级信息安全漏洞数据管理平台，旨在为我国信息安全保障提供服务。CNNVD通过自主挖掘、社会提交、协作共享、网络搜集以及技术检测等方式，联合政府部门、行业用户、安全厂商、高校和科研机构等社会力量，对涉及国内外主流应用软件、操作系统和网络设备等软硬件系统的信息安全漏洞开展采集收录、分析验证、预警通报和修复消控工作，建立了规范的漏洞研判处置流程、通畅的信息共享通报机制以及完善的技术协作体系，处置漏洞涉及国内外各大厂商上千家，涵盖政府、金融、交通、工控、卫生医疗等多个行业，为我国重要行业和关键基础设施安全保障工作提供了重要的技术支撑和数据支持，对提升全行业信息安全分析预警能力，提高我国网络和信息安全保障工作发挥了重要作用。

中国信息安全测评中心 版权所有 备案号：京ICP备14044185号
北京市海淀区上地西路8号院1号楼 邮政编号：100085 邮箱: vulpro@itsec.gov.cn
电话:010-82341118 010-82341188 传真:010-82341100

Figure 3. An image from CNNVD’s (the PRC’s vulnerability clearing house) site showing the MSS 13th Bureau CNITSEC’s oversight of CNNVD, and a shared location in Zhongguancun Park in Beijing.

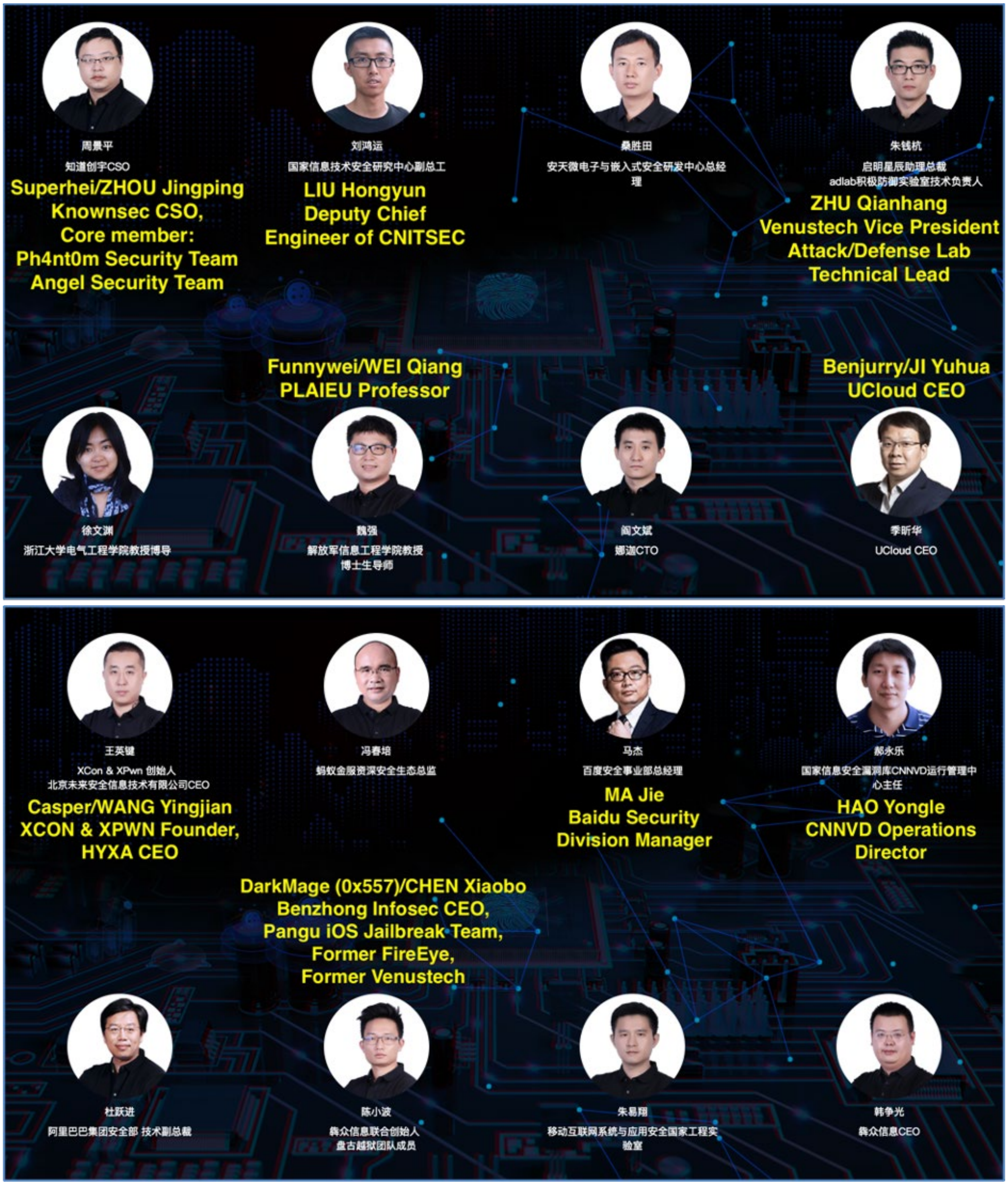
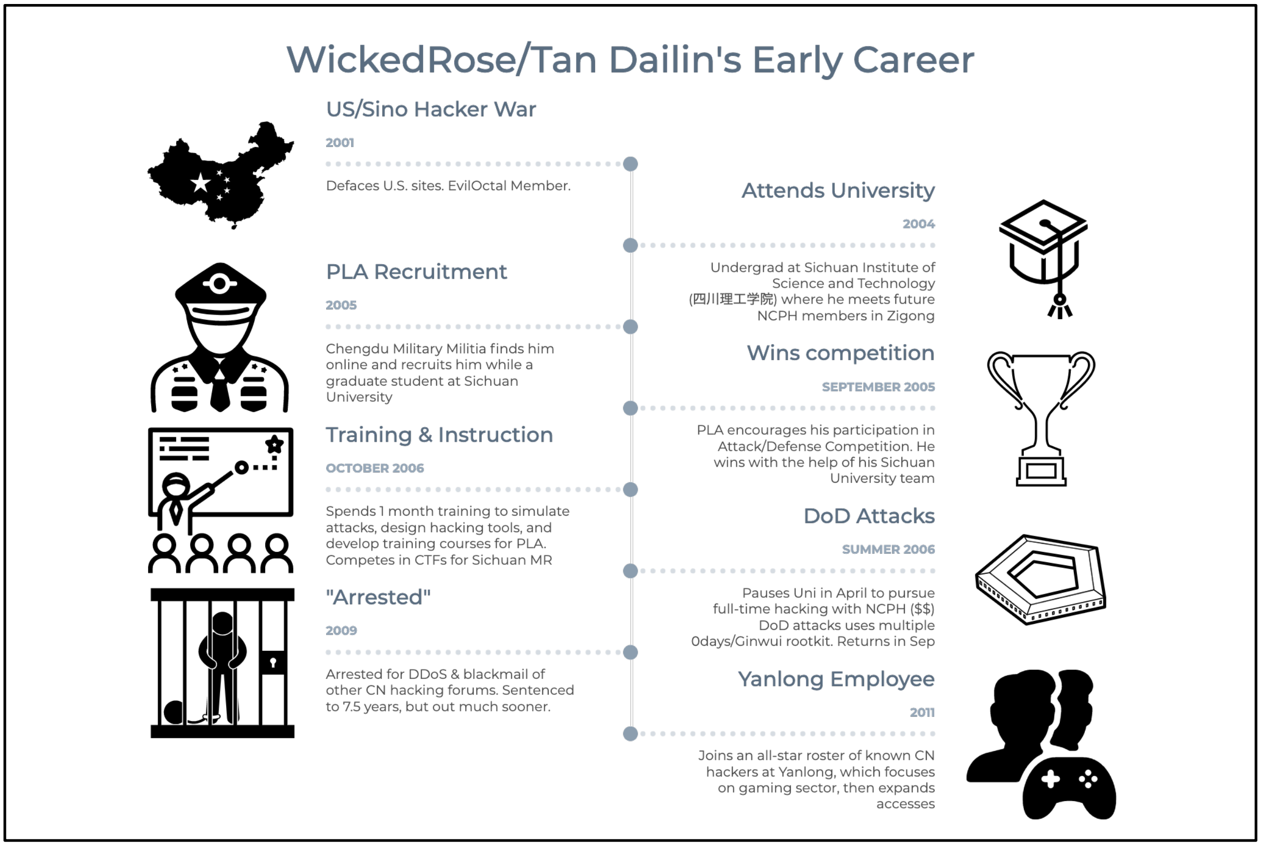


Figure 4. XPWN's Advisory Board Reads Like a Xfocus and MSS Contractor Yearbook



WickedRose/Tan Dailin's Early Career

US/Sino Hacker War

2001

Defaces U.S. sites. EvilOctal Member.

Attends University

2004

Undergrad at Sichuan Institute of Science and Technology (四川理工学院) where he meets future NCPH members in Zigong

PLA Recruitment

2005

Chengdu Military Militia finds him online and recruits him while a graduate student at Sichuan University

Wins competition

SEPTEMBER 2005

PLA encourages his participation in Attack/Defense Competition. He wins with the help of his Sichuan University team

Training & Instruction

OCTOBER 2006

Spends 1 month training to simulate attacks, design hacking tools, and develop training courses for PLA. Competes in CTFs for Sichuan MR

DoD Attacks

SUMMER 2006

Pauses Uni in April to pursue full-time hacking with NCPH ($$) DoD attacks uses multiple 0days/Ginwui rootkit. Returns in Sep

"Arrested"

2009

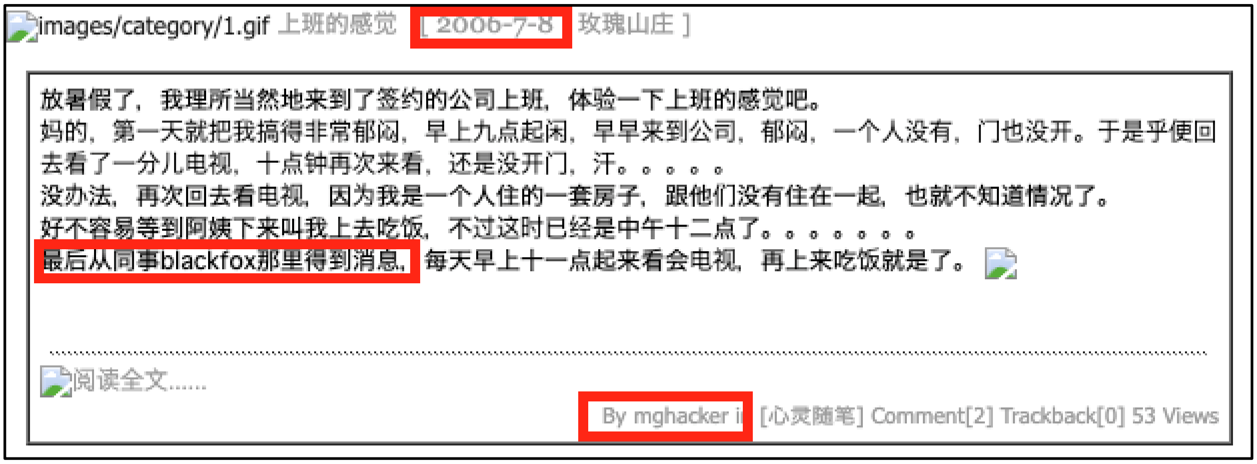
Arrested for DDoS & blackmail of other CN hacking forums. Sentenced to 7.5 years, but out much sooner.

Yanlong Employee

2011

Joins an all-star roster of known CN hackers at Yanlong, which focuses on gaming sector, then expands accesses

Figure 5. A timeline of Tan Dailin/WickedRose's early career and evolution from patriotic hacker to PLA operator and trainer, criminal operator, gaming firms, MSS contractor, and eventually cybersecurity firm owner.



images/category/1.gif 上班的感觉 [2006-7-8 玫瑰山庄]

放暑假了，我理所当然地来到了签约的公司上班，体验一下上班的感觉吧。
妈的，第一天就把我搞得非常郁闷，早上九点起闲，早早来到公司，郁闷，一个人没有，门也没开。于是乎便回去看了一分儿电视，十点钟再次来看，还是没开门，汗。。。。。
没办法，再次回去看电视，因为我是一个人住的一套房子，跟他们没有住在一起，也就不知道情况了。
好不容易等到阿姨下来叫我上去吃饭，不过这时已经是中午十二点了。。。。。。。
最后从同事blackfox那里得到消息，每天早上十一点起来看会电视，再上来吃饭就是了。

阅读全文......

By mghacker i [心灵随笔] Comment[2] Trackback[0] 53 Views

Figure 6. Archive of Tan's Personal Blog from 2006 Shows Blackfox was Likely Also Working for the PLA's Chengdu MR at the Same Time

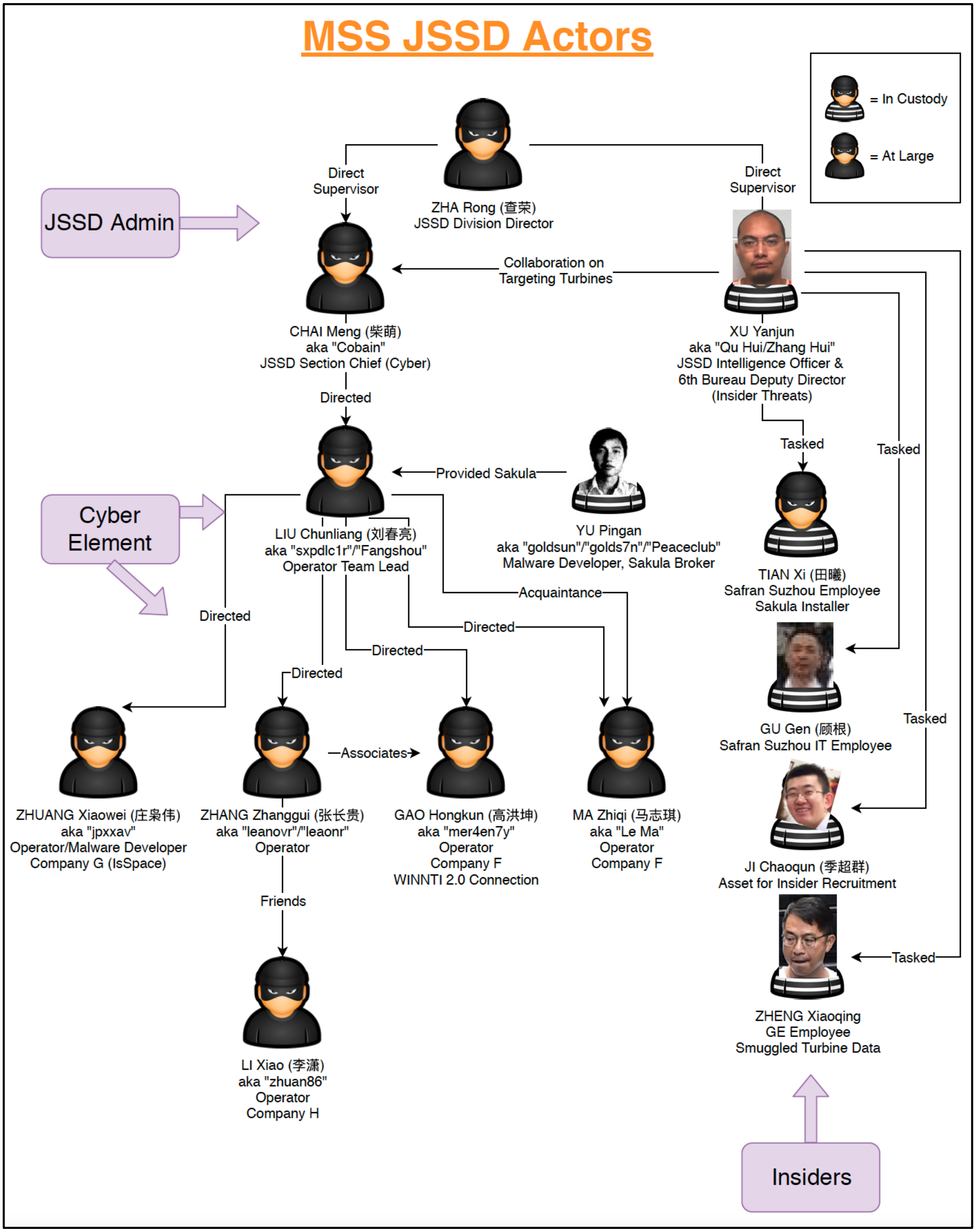


Figure 7. A mapping of how MSS cyber operators known as TURBINE PANDA and MSS HUMINT operators worked in tandem to pilfer aerospace secrets over a multi-year campaign.

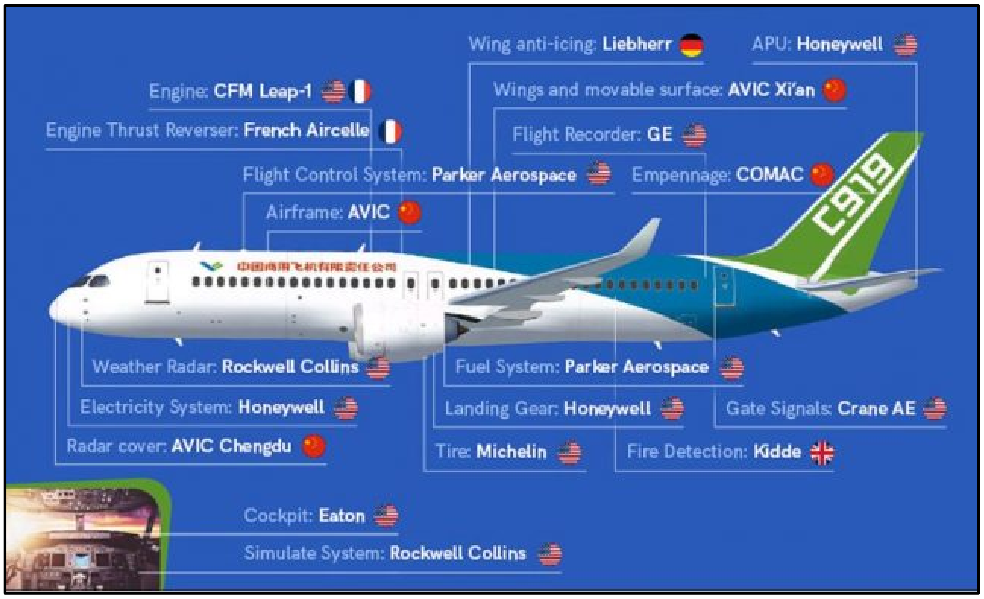

Wing anti-icing: Liebherr
APU: Honeywell
Engine: CFM Leap-1
Wings and movable surface: AVIC Xi'an
Engine Thrust Reverser: French Aircelle
Flight Recorder: GE
Flight Control System: Parker Aerospace
Empennage: COMAC
Airframe: AVIC
C919
中国商用飞机有限责任公司
Weather Radar: Rockwell Collins
Fuel System: Parker Aerospace
Electricity System: Honeywell
Landing Gear: Honeywell
Gate Signals: Crane AE
Radar cover: AVIC Chengdu
Tire: Michelin
Fire Detection: Kidde
Cockpit: Eaton
Simulate System: Rockwell Collins

Figure 8. An aviation enthusiast site's breakdown of the C919 airliner's foreign components[32]

Industry Names (CrowdStrike, Mandiant, Microsoft, Other)	**Affiliation**	**Unit/Location**
COMMENT PANDA APT1 FLUORINE	Former 3PLA 1st Bureau	Unit 61398 - Shanghai
PUTTER PANDA APT2 SULFUR	Former 3PLA 12th Bureau	Unit 61486 - Shanghai
OVERRIDE PANDA APT30 Naikon	Former PLA Chengdu 2nd TRB	Unit 78020 - Kunming
GOTHIC PANDA APT3 BORON UPS, Buckeye	MSS Contractors (Boyusec)	Guangzhou, Guangdong
TURBINE PANDA APT 26 TECHNETIUM Bronze Express	MSS Contractors	Nanjing, Jiangsu

[32] Originally retrieved from: https://www.aerotime.aero/aerotime.team/447-made-in-china-why-c919-can-hardly-be-calledchinese

STONE PANDA APT10 POTASSIUM CloudHopper, MenuPass	MSS Contractors (Huaying Haitai, Laoying Baichen)	Tianjin
AURORA PANDA APT17 HELIUM HiddenLynx, Sportsfan, DeputyDog	MSS Contractors (Real SOI, etc.)	Jinan, Shandong
KRYPTONITE PANDA APT40 GADOLINIUM Bronze Mohawk	MSS Contractors (Hainan Xiandun Technology)	Haikou, Hainan
WICKED PANDA APT41 BARIUM	MSS Contractors (Chengdu 404)	Chengdu, Sichuan

Appendix 1. A partial rosetta stone for Chinese APT groups that have been publicly outed to date.[33]

[33] Much more comprehensive rosetta stones exist in the private sector and at the classified level, however, I have attempted to protect proprietary data where possible and only used ones that have had public outings and multiple corroborations for the purposes of this testimony. Further sourcing available upon request.

OPENING STATEMENT OF KELLI VANDERLEE, SENIOR MANAGER, STRATEGIC ANALYSIS, MANDIANT THREAT INTELLIGENCE

COMMISSIONER BARTHOLOMEW: Great, thank you very much, we look forward to the questions. Ms. Vanderlee.

MS. VANDERLEE: Hi, can you guys hear me all right? Great. Thank you to the USCC for their invitation to contribute to this important hearing.

For more than 15 years, Mandiant has been conducting investigations and collecting evidence about malicious cyber threat activity, including operations that we attribute to China. Based on this evidence and careful analysis, we've built an understanding of many individual Chinese cyber threat groups, as well as the broader trends shaping these activities.

So looking at Chinese cyber espionage tactics, techniques, and procedures, threat clusters attributed to China exhibit a range of skills and employ tactics common to many threat groups. Following a significant military and intelligence restructuring, we believe that the technical tradecraft used by Chinese cyber espionage groups has become stealthier and more agile.

I'd like to focus specifically on three tactics: vulnerability exploitation, third-party compromise, and software supply chain compromise, because these three exemplify both the scale and the strategic evolution and use of tactics for maximizing efficiency and impact of operations.

So beginning with vulnerability exploitation. A vulnerability is a software flaw that malicious actors can exploit for a variety of purposes. Zero day vulnerabilities are those that were exploited before the vendor was aware there was a problem, before consumers knew, and before there was a fix available.

Vulnerability exploitation can be a quite powerful tactic because once threat actors know a particular software flaw exists, they can target any internet-accessible device running that software, either in targeted or mass campaigns.

So the proxy log-on campaign from earlier, early in 2021 is a perfect example of this. In that time period, we documented at least five different activity sets that we attribute to China using the zero day vulnerabilities in Microsoft Exchange servers to gain access to targeted networks.

While three of the groups appear to carefully select their targets before exploitation, two conducted widespread scanning and compromised tens of thousands of servers and virtually every vertical on region. The broad impact of this activity prompted unprecedented international response.

In July 2021, governments and intergovernmental organizations in North America, Europe, and Asia issued coordinated statements condemning this exploitation campaign as well as other Chinese cyber espionage activity.

The second tactic I'd like to talk about is third-party compromise. Third-party compromise is a multistage operation. One of the most commonly cited examples of this is APT10 targeting managed service providers in order to gain access to the clients of those organizations.

With this tactic, a single compromise can facilitate attackers' access to multiple potential targets, and victims may be less likely to detect and have fewer options to prevent an intrusion that abuses a trusted channel, such as that between a service provider and a client.

However, I'd like to discuss a bit of a less traditional example. During a 2019 APT41 incident at a telecommunications company, Mandiant identified malware sitting on servers that were responsible for routing SMS messages.

This malware was designed to work with two lists. One was a keyword list of words that were of interest to China, and the other list was of specified phone numbers and device IDs. So they had preselected users of interest and topics of interest.

And when an SMS message was sent across that telecom's network, if the sender or receiver matched the device list and if the content matched the keyword list, they would collect that message for the threat actors to later come and get. We called this malware MESSAGETAP.

This example demonstrates Chinese efforts to move upstream and collect data closer to the global telecommunications backbone. Instead of targeting individual devices, they're collecting the information at the telecom, many degrees removed from the end user, which means that there is no evidence or no sign on the targeted device or the affected device that any messages were intercepted.

The third tactic I'd like to discuss is software supply chain compromise. And this is when attackers implant malicious code within legitimate programs or updates. In 2019 and 2020, we saw evidence of at least four examples of Chinese software supply chain compromises that involved software that was recommended or in some cases required by government authorities.

Three of these cases involved Chinese government software and appear to be intended to collect intelligence about foreign businesses operating in China as well as Chinese citizens.

So looking at these tactical shifts towards being more stealthy, more agile, more efficient and other observations, Mandiant suggests that Chinese cyber espionage activity has demonstrated higher tolerance for risk and is less constrained by norms and diplomatic pressures. We can see that in indictments.

While indictments of actors such as the APT1 and APT3 appeared to result in these groups ceasing operations, more recent indictments of groups like APT10 and APT41 appear to have only resulted in pauses in activity.

We can also look at IP theft. Two recent U.S. indictments suggest that Chinese cyber espionage groups continued to conduct commercial IP theft as -- in one case as early as one month after the agreement was signed.

After the agreement, Mandiant continued to observe Chinese cyber espionage groups steal military and dual use IP. We also saw Chinese state-sponsored actors regularly target organizations where commercial IP theft is a plausible objective, like technology, engineering, construction, transportation, biotech.

However, we do not have a case where the available evidence is sufficient to confirm that this type of data was targeted, staged, and left the network since the agreement was signed.

So what do we do about Chinese cyber espionage? Very briefly, we can support private sector defense and resiliency. And this has been said in the last panel, this has been said in the 2015 panel about this topic. But things like incident reporting and information sharing are valuable.

Other creative actions, such as using a search warrant to remove web shells that Chinese cyber espionage actors have installed on private sector servers during the proxy log-on campaign may also be something worth exploring.

And I believe, very quickly, also an example that came out of the proxy log-on campaign and may be worth repeating is leaning more on international partners to issue coordinated statements, as well as encouraging our allies to report when they are observing Chinese cyber espionage activity in their country.

And when they are also sharing details about this activity, it may raise the cost for China for conducting this activity and decrease plausible deniability because the United States is not the only country going public with these types of statements.

Thank you for your time.

PREPARED STATEMENT OF KELLI VANDERLEE, SENIOR MANAGER, STRATEGIC ANALYSIS, MANDIANT THREAT INTELLIGENCE

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

PANEL II: CHINA'S GOALS AND CAPABILITIES FOR CYBER ESPIONAGE

China's Capabilities for State-Sponsored Cyber Espionage

KELLI VANDERLEE

SENIOR MANAGER, STRATEGIC ANALYSIS

MANDIANT THREAT INTELLIGENCE

FEB. 17. 2022

Executive Summary

- Following China's military and intelligence restructuring, Mandiant Threat Intelligence believes the technical tradecraft used by Chinese cyber espionage groups since 2016 has steadily evolved to become stealthier and more agile, while taking measures to complicate attribution.
- Chinese cyber espionage operators' use of vulnerability exploitation, third party compromise, and software supply chain compromise exemplify both the scale of Chinese state-sponsored threat activity and the strategic evolution in use of tactics to maximize efficiency and impact.
- In 2020 and 2021, we believe Chinese cyber espionage activity has demonstrated a higher tolerance for risk and is less constrained by norms or diplomatic pressures.

Chinese Cyber Espionage Distinguished by Interests and Scale

Threat clusters attributed to China exhibit a range of skill levels and employ tactics, techniques, and procedures (TTPs) common to many cyber threat groups.[i] Following China's military and intelligence restructuring, we believe the technical tradecraft used by Chinese cyber espionage groups since 2016 has steadily evolved to become stealthier and more agile, while taking measures to complicate attribution. For example, using software supply chain and third-party compromises to collect data makes detecting and preventing intrusions more difficult for victims.

Chinese cyber espionage malware use appears to have evolved to operate on a wider variety of operating systems, focus on modular code families, and increasingly incorporate malware only executed in memory. Actors also leverage a combination of publicly and non-publicly available tools to accomplish operations. We believe that Chinese threat groups have become increasingly likely to use publicly available malware and other widely used tactics, particularly in early stages of a compromise, in an effort to blend in with other threat activity.

The primary elements that distinguish Chinese cyber espionage activity from that of groups we track linked to other states are national interest and scale. Beijing has specific and unique intelligence collection requirements that are unlikely to overlap with other nations, for example in Hong Kong, Tibet, and the Uyghur community. In terms of scale, Chinese cyber threat activity is simply bigger. Based on Mandiant observations, there are more Chinese state-linked threat groups conducting more compromises, exploiting more zero-days than other nations – and this remains true even after the volume of Chinese cyber threat activity we observed declined by at least half from 2013 to 2016.[ii,iii]

Initial Infection Vectors: A Journey of a Thousand Miles Begins with a Single Step

Chinese cyber espionage actors use a variety of initial access vectors to gain a foothold in targeted environments including email phishing and other social engineering, strategic web compromise, and SQL injection. While not unique to Chinese groups, Chinese activity sets have used several tactics with distinction. For the purposes of this testimony, I would like to focus on Chinese cyber espionage operators' use of vulnerability exploitation, third-party compromise, and software supply chain compromise, as these reflect both the scale, and the strategic evolution in use of tactics to maximize the efficiency and impact of Chinese cyber espionage.

Vulnerability Exploitation

Malicious actors exploit flaws or vulnerabilities in software for a variety of purposes ranging from obtaining information about a targeted device that should not have been accessible, to causing a device to stop working, to convincing a targeted device to run attacker commands. Many of the vulnerabilities we see threat actors exploit are vulnerabilities that vendors have disclosed and patched. These are sometimes called n-day vulnerabilities. Zero-day vulnerabilities are vulnerabilities that were exploited before the vendor was aware of the issue to release a patch, and before consumers had the option to update their software and fix the problem.

Chinese cyber espionage actors have made effective use of both n-day and zero-day vulnerabilities in 2020 and 2021.[iv] Significantly, in Mandiant analysis of zero-day exploitation from 2012 to mid-2021, of the vulnerabilities we were able to attribute, Chinese state-linked groups exploited more than any other nation.[v]

APT41 Exploits Multiple N-Day Vulnerabilities in Early 2020

In early 2020, Mandiant observed APT41[1] conduct a large-scale campaign leveraging vulnerabilities in enterprise networking and endpoint management devices from Citrix, Cisco, and Zoho, that affected more than 75 Mandiant customers.[vi] These organizations spanned 20 nations including the United States, and a variety of sectors, from aerospace and defense, to pharmaceuticals, to energy and utilities.

Despite the wide aperture of the campaign, we found evidence that the activity was targeted. For example, observed attempts to exploit Cisco devices were only sent to Cisco devices, suggesting that the attackers had identified a list of internet accessible devices before commencing operations. APT41 is one of the most prolific Chinese cyber espionage groups that we track, and this campaign further underscores the apparent high operational tempo and wide collection requirements for APT41.[vii]

Multiple Chinese Activity Sets Exploit Microsoft Exchange “ProxyLogon” Vulnerabilities

From January to March 2021, we documented many threat groups using the so called “ProxyLogon” zero-day vulnerabilities to gain access to targeted networks, including at least five activity sets we attribute to China.[viii] While three of these clusters appeared to carefully select their targets before an attempted exploitation of these vulnerabilities, others conducted widespread scanning and compromised tens of thousands of servers in virtually every vertical and region.

The progressive adoption of the same exploit code among Chinese espionage groups prior to the release of a public patch potentially indicates the existence of a shared development and logistics infrastructure and possibly a centralized coordinating entity. Mandiant research dating back to 2013 has likewise suggested a logistical support function supporting Chinese cyber espionage groups.[ix]

The widespread impact of this activity prompted an unprecedented international response: in July 2021, governments and intergovernmental organizations in North America, Europe, and Asia issued coordinated statements condemning the ProxyLogon exploitation activity as well as other cyber espionage directed by the Chinese government.[x,xi,xii]

Pulse Secure VPN Zero-day Exploitation

Mandiant investigated multiple intrusions in the defense, government, high-tech, transportation, and financial sectors in the U.S. and Europe that occurred between August 2020 and March 2021. We suspect these incidents began with exploitation of several vulnerabilities in Pulse Secure VPNs, including one zero-day. We attribute this activity to two Chinese activity clusters, one of which we suspect of having ties to APT5. Associated with this activity, we are tracking at least 16 malware families specifically designed to manipulate Pulse Secure devices.[xiii]

Both activity sets associated with this campaign took steps to preserve operational security and stymie forensic investigations, such as clearing logs, cleaning up evidence of data staged for exfiltration, and

[1] Mandiant defines APT groups as activity clusters we believe to be state sponsored and primarily focused on espionage.

changing file timestamps. The actors demonstrated detailed knowledge of the targeted appliances and victim networks.

Third Party Compromise

Third-party compromise exploits the inherent trust that users and administrators place in relationships with other legitimate businesses, as well as genuine products and services that enter their organization through expected avenues. Malicious actors frequently target professional service providers, such as lawyers or accountants, and technology service providers, such as managed IT, managed service providers (MSPs), or cloud infrastructure providers to gain access to client data and networks. Third-party compromises afford tactical and operational advantages to attackers compared to direct targeting: a single compromise can facilitate access to multiple potential targets, and victims may be less likely to detect, and have fewer options to prevent, an intrusion that abuses a trusted channel.

APT10 MSP Compromises

In April 2017, PricewaterhouseCoopers (PwC) reported on APT10 activity targeting MSPs to conduct third-party compromises against additional victims in "Operation Cloud Hopper."[xiv] According to PwC, APT10 initially compromised MSPs, then used this access to infect downstream customers by exploiting the trusted access to systems required for the MSP to conduct its services. Data stolen from these customers was then often compressed and sent back to the MSP for eventual exfiltration.

This is consistent with Mandiant observations.[xv] For example, we investigated cases in which APT10 accessed victims through MSPs in North America and Europe. A notable infection involved a SOGU backdoor that was set to communicate with its command and control (C&C) server through a server belonging to the victim's MSP, likely indicating a foothold on the MSP's network. The tactic also masks malicious C&C and exfiltration traffic and make it appear innocuous.

A U.S. indictment, unsealed in December 2018, and other open-source reporting further corroborates APT10’s use of MSP third-party compromise to gain access to additional victims, including telecommunications companies.[xvi,xvii]

APT41 and MESSAGETAP

During a 2019 incident response investigation at a telecommunications network provider, Mandiant identified a malware family dubbed MESSAGETAP that we attribute to APT41.[xviii] Specifically, MESSAGETAP was discovered within a cluster of Linux servers responsible for routing Short Message Service (SMS) messages to an intended recipient or storing them until the recipient has come online.

MESSAGETAP is designed to work with configuration files providing parameters for collection: keywords of geopolitical interest to China, as well as international mobile subscriber identities (IMSI) and phone numbers identifying specific devices for potential monitoring, see Figure 1. If SMS content sent or received by one of the identified devices also matched the keyword list, the contents of the message would be saved for later collection by the threat actors. Sanitized examples of keywords include the names of political leaders, military and intelligence organizations, and political movements at odds with the Chinese government.

The deployment of MESSAGETAP at a telecom demonstrates Chinese strategic intelligence collection efforts to move "upstream," collecting information closer to the backbone of global communications. Instead of targeting individual devices for SMS data, the detected APT41 campaign captures such information at the telecom, many degrees removed from the end user. This type of compromise would leave no forensic evidence on targeted users’ devices or other signs that the messages had been intercepted.

Software Supply Chain Compromise

A specialized subset of third-party compromise, supply chain compromise, occurs when attackers gain unauthorized access to legitimate infrastructure or tools and implant malicious code to be delivered by the legitimate vendor or repository via the same trusted distribution methods that users would normally use to obtain the legitimate hardware, software, open-source package, or updates.

In Mandiant analysis of software supply chain compromise incidents from 2013 to 2020, of the incidents we were able to attribute to state sponsored actors, Chinese threat groups conducted nearly double the number of Russian and North Korean-attributed incidents combined.

APT41 is well known for several large-scale software supply chain compromises targeting video games as well as common enterprise software, such as the 2018 campaign affecting the ASUS live update utility, dubbed Operation ShadowHammer by Kaspersky.[xix] Open-source reporting suggests that more than 50,000 systems installed the malicious update.[xx] See Figure 2 for information about APT41 software supply chain compromises.

In 2019 and 2020, we observed evidence of at least four examples of suspected Chinese software supply chain compromises which involved trojanizing or including suspicious functionalities in software provided, and in some cases, required by government authorities. Three of these cases involved Chinese government software and appear to have been intended to gather intelligence on foreign businesses operating in China as well as Chinese citizens.[xxi, xxii, xxiii] One instance affected a Vietnamese government digital signature verification software.[xxiv]

Chinese Military and Intelligence Restructuring Informs MSS and PLA Cyber Threat Activity

Since taking power in 2012, Xi Jinping has sought to consolidate domestic power and maintain China's regional hegemony through political and military modernization.[xxv] Mandiant Threat Intelligence believes the restructuring of China's military and civilian intelligence agencies significantly impacted cyber espionage operations in terms of active actors, tempo of operations, and observed TTPs, particularly from 2014 to 2016 when several substantial changes were enacted, see Figure 3.[xxvi]

Mandiant recently conducted a focused study of Chinese cyber threat activity from 2017 to 2020 and found that observed cyber threat activity appears to be consolidating into patterns reflective of the new structure and operational mandates of the People's Liberation Army (PLA) and the Ministry of State Security (MSS).

Building on this research, we suggest that MSS activity can be differentiated from that of the PLA based on geographic scope and alignment of operations and victims to each organization's mission mandate. While threat groups we believe to be affiliated with PLA Theater Commands, such as Tonto Team and TEMP.Overboard, appear to focus operations on regions within the areas of responsibility of their respective Theater Commands, MSS-affiliated groups, such as APT41, APT5, and APT10, discussed above, demonstrate a much broader geographic scope. We also believe that MSS groups are more likely to target the United States and regions outside of China's direct sphere of influence, such as Europe, Latin America and the Caribbean, and North America. This geographic spread likely reflects MSS responsibilities to conduct domestic counterintelligence, non-military foreign intelligence, and support aspects of political security.[xxvii]

Indictments, Sanctions, Diplomatic Agreements No Longer Significantly Constrain Cyber Espionage

Mandiant Threat Intelligence believes Chinese cyber espionage activity has demonstrated a higher tolerance for risk and is less constrained by norms or diplomatic pressures than previously characterized, mirroring bolder rhetoric and policy in other arenas.

Public Exposure and Indictments of Cyber Threat Operators

Evidence suggests that public exposure and indictments of Chinese cyber espionage operators has become less effective at deterring threat activity over time.

Public exposure and indictments of APT1 and APT3 in 2014 and 2017, appeared to result in those groups ceasing operations.[xxviii,xxix,xxx] In contrast, while we did not observe new APT10 activity for approximately two years after the 2018 indictment, the group has since resumed threat activity.[xxxi] Similarly, following the indictments against APT41 operators and affiliates announced in September 2020, we noted only a lull in activity with resumed operations observed by summer 2021.[xxxii]

Diplomatic Agreement to Cease Commercial-Application IP Theft

Indictments released in 2020 and 2021 further indicate that Chinese threat groups continued to steal commercial application intellectual property (IP) after the September 2015 agreement between Presidents Obama and Xi was established.[xxxiii]

Following the early 2021 ProxyLogon exploitation campaign, the U.S. Department of Justice (DOJ) unsealed an indictment against members of APT40, alleging that the indicted individuals worked for front company Hainan Xiandun established and directed by the Hainan Province MSS branch.[xxxiv] One of the most significant accusations in the indictment, Act 52, indicates that APT40 stole commercial application intellectual property (IP) in October 2015, one month after the Obama-Xi agreement was forged. In December 2018, Mandiant independently identified APT40 headquarters in Hainan via technical analysis of an operation targeting Cambodian elections.[xxxv,xxxvi]

Similarly, in July 2020, the DOJ filed an indictment against two Chinese nationals accused of conducting cyber threat activity for personal financial gain as well as “with the acquiescence” and assistance of officers assigned to the Guangdong branch of the MSS.[xxxvii] The defendants allegedly demonstrated an interest in COVID-19 vaccines as well as IP from high-tech, defense, manufacturing, pharmaceutical, healthcare research, construction and engineering, energy, and media and entertainment sectors throughout the globe. This activity may also constitute a violation of the Obama-Xi agreement, though the actors’ status as freelancers could complicate that argument. Mandiant has been tracking this cluster of threat activity since 2012 as UNC302,[2] although we have evidence these actors have been active since at least 2009.

Following the Obama-Xi agreement, Mandiant continued to observe Chinese cyber espionage groups steal military and dual-use IP, for example during the Pulse Secure vulnerability exploitation campaign described above. We also see Chinese state sponsored actors regularly target organizations where commercial IP theft is a plausible objective, including intrusions at universities as well as entities in the technology, construction and engineering, transportation, and biotechnology sectors. In some cases, we discovered evidence of data staging, but often the available forensic artifacts are insufficient to confidently identify the nature of files of interest or whether data left a compromised environment. As noted above, many Chinese cyber espionage actors have demonstrated greater attention to operational security in recent years and have taken steps to cover their tracks, such as clearing logs.

Direct theft via cyber means is only one avenue for acquiring desired intellectual property, and we have also noted evidence of Chinese state initiatives supporting forced technology transfer, insider threat, talent recruitment, and acquisitions, partnerships, and joint ventures.[xxxviii] Open sources indicate Chinese interest in acquiring IP from key sectors persists, though the means used to obtain it have not always involved cyber threat activity. For example, a DOJ indictment suggests that from 2010 to 2015, APT26 conducted cyber threat activity against several companies to acquire IP related to commercial aircraft engines. A separate indictment alleges that from 2016 to 2018, an insider at a U.S. aerospace company conspired with a Chinese national to steal proprietary technology related to aviation and turbine technologies.[xxxix] The indictment further alleges that the Chinese Government provided financial support and facilitated the creation of research

[2] Mandiant creates UNC or “uncategorized” groups to track newly discovered clusters of activity and artifacts. As we collect additional related evidence over time, we expand our understanding of an UNC group.

agreements between Chinese turbine parts manufacturing companies set up by the indicted individuals and Chinese state-owned institutions working to develop turbine technologies.[xl]

Technology to Tradecraft: How Emerging Technologies Support Chinese Espionage

Mandiant Threat Intelligence assesses that innovative technologies such as 5G, quantum computing, and artificial intelligence (AI) will provide new and improved means for Chinese intelligence to capture, transfer, decrypt, and process data. With the vast amount of data already collected through Chinese cyber operations, more processing power and faster data transfer will help to turn this stolen data into actionable intelligence for future espionage activity. Significantly, the Chinese Government has also called out 5G, quantum computing, and AI as particular areas of focus for investment and development.[xli] See Figure 4.

5G

5G improves the performance, capacity, reliability, and speed of the network and decreases latency compared to 4G and other previous generations of networks, likely facilitating data collection and processing power. Vulnerabilities or backdoors can potentially be built into Chinese 5G products and allow state-sponsored espionage actors to eavesdrop, steal information, and conduct network exploitation. Malicious functionalities do not need to be included from the beginning and can feasibly be introduced by a software update.

There is some precedent for this type of activity. In November 2016, open sources, citing an internal report by the U.S. Joint Chiefs of Staff Directorate for Intelligence (J2), claimed that Boyusec, which Mandiant and the U.S. government linked to Chinese espionage actors APT3, was collaborating with Huawei to install backdoored security products onto computer and telephone equipment manufactured in China.[xlii,xliii,xliv]

Quantum Computing

Quantum computing will have significant implications for the threat landscape and cyber espionage capabilities, primarily due to quantum key distribution, its effect on cryptographic systems, and the growth in processing power. Using quantum key distribution guarantees that the data encrypted by quantum keys are transferred securely. Quantum computers can defeat many public-key cryptographic algorithms. The increased computation power of quantum computers can theoretically be used in large data analytics and optimization problems, helping China to analyze troves of data faster.

Artificial Intelligence

The Chinese State Council plans to make the nation an AI superpower by 2030 by investing in this emerging technology at home and abroad.[xlv] The country has already begun leveraging AI-based tools for surveillance and law enforcement purposes, as well as influence operations.[xlvi, ,] We assess with moderate confidence that Chinese intelligence services will use machine learning applications to help identify potential individuals for recruitment and social engineering.

Machine Learning

Machine learning is a subfield of AI that trains on data to build models to process large amounts of data in shorter periods of time. In machine learning, models learn from previous calculations and adapt to new environments to perform trend analysis, make predictions, examine behaviors, and perform other actions that illuminate relationships in the dataset. For Chinese intelligence, this technology could facilitate categorization and processing of the millions of records stolen in breaches so that it becomes actionable.

Shifting the Cost-Benefit Equation

Mandiant Threat Intelligence suggests that Chinese cyber espionage activity in 2020 and 2021 has demonstrated a higher tolerance for risk and is less constrained by norms or diplomatic pressures, mirroring bolder rhetoric and policy in other arenas.[xlix] This includes limited signs that China may be willing to engage in disruptive and destructive cyber attacks.[l,li,lii] The activity trend indicates that despite a variety of U.S. efforts to signal and enforce its perspective on Chinese cyber threat operations, Chinese policymakers view the rewards for continuing this activity as outweighing the risks of persisting in this activity.

Support Private Sector Defense and Resiliency

One significant avenue to respond to the challenge of Chinese cyber espionage against the private sector could be to explore ways to support private sector cyber defensive measures and resiliency in the event of a compromise. There are a number of forms this could take, for example:

- Incident reporting: Incentivizing private sector victims to report incidents to government authorities would help the government to collect additional evidence about Chinese cyber threat activity and better understand the scope, objectives, and techniques of these operations.
- Information Sharing: In 2021, the U.S. government noticeably increased efforts to issue public advisories about active campaigns, including details such as exploited vulnerabilities and mitigation recommendations. The government has also increased socializing best practices, for example, with public announcements about deadlines for when Federal agencies are required to patch certain exploited vulnerabilities. These announcements can inform organizations' planning around when and how they should react or take proactive steps to improve cyber security.

Other creative actions, such as using a search warrant to remove webshells that Chinese cyber espionage actors had installed on private sector servers during the ProxyLogon campaign, may also support private sector defense and resiliency.[liii,liv]

Discourage Cyber Crime, Disruptive and Destructive Attacks

If the United States and its allies seek to reduce the frequency and impact of foreign state-sponsored cyber threat activity, a beneficial foundational step would likely be to have clear definitions separating cyber espionage from cybercrime and acts of war, and to reinforce these definitions in international bodies and treaties until they become recognized and enforceable norms. Significantly, China and other nations are also actively pursuing norm-setting.[lv]

Encourage Partnership

Chinese cyber espionage activity affects not only the United States, but also many allies and partners across the globe. It is possible that coordinated announcements to condemn significant threat activity as well as encouraging other nations to release information about active campaigns could increase the cost of conducting this activity for China and reduce plausible deniability. International law enforcement cooperation may also help the U.S. and its international partners to gather data about active Chinese cyber espionage campaigns, and potentially identify ways to interrupt them.

It may also be worthwhile to explore potential avenues for the U.S. and its allies and partners to find common ground with China on cyber issues, for example on ransomware.[lvi]

Acknowledgements

Thank you to Mandiant colleagues including but not limited to: Scott Henderson, Emily Cranston, Sarah Jones, Dan Perez, Fred Plan, Nalani Fraser, Michelle Cantos, Parnian Najafi.

Appendix

Figure 1: Overview Diagram of MESSAGETAP

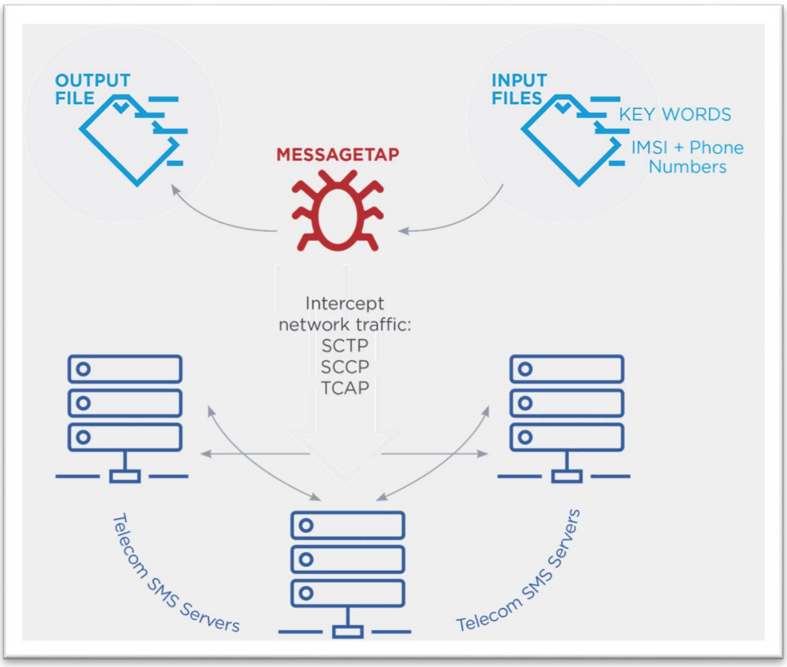


Figure 2: APT41 Supply Chain Compromises

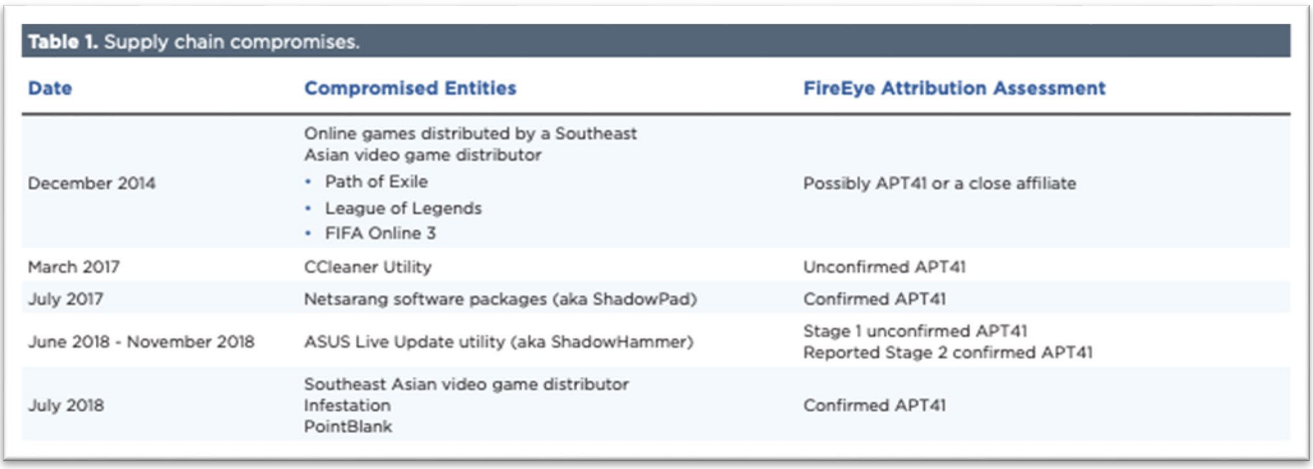


Table 1. Supply chain compromises.

Date	Compromised Entities	FireEye Attribution Assessment
December 2014	Online games distributed by a Southeast Asian video game distributor • Path of Exile • League of Legends • FIFA Online 3	Possibly APT41 or a close affiliate
March 2017	CCleaner Utility	Unconfirmed APT41
July 2017	Netsarang software packages (aka ShadowPad)	Confirmed APT41
June 2018 - November 2018	ASUS Live Update utility (aka ShadowHammer)	Stage 1 unconfirmed APT41 Reported Stage 2 confirmed APT41
July 2018	Southeast Asian video game distributor Infestation PointBlank	Confirmed APT41

Back to the Table of Contents

Figure 3: Active Network Compromises by China Based Groups

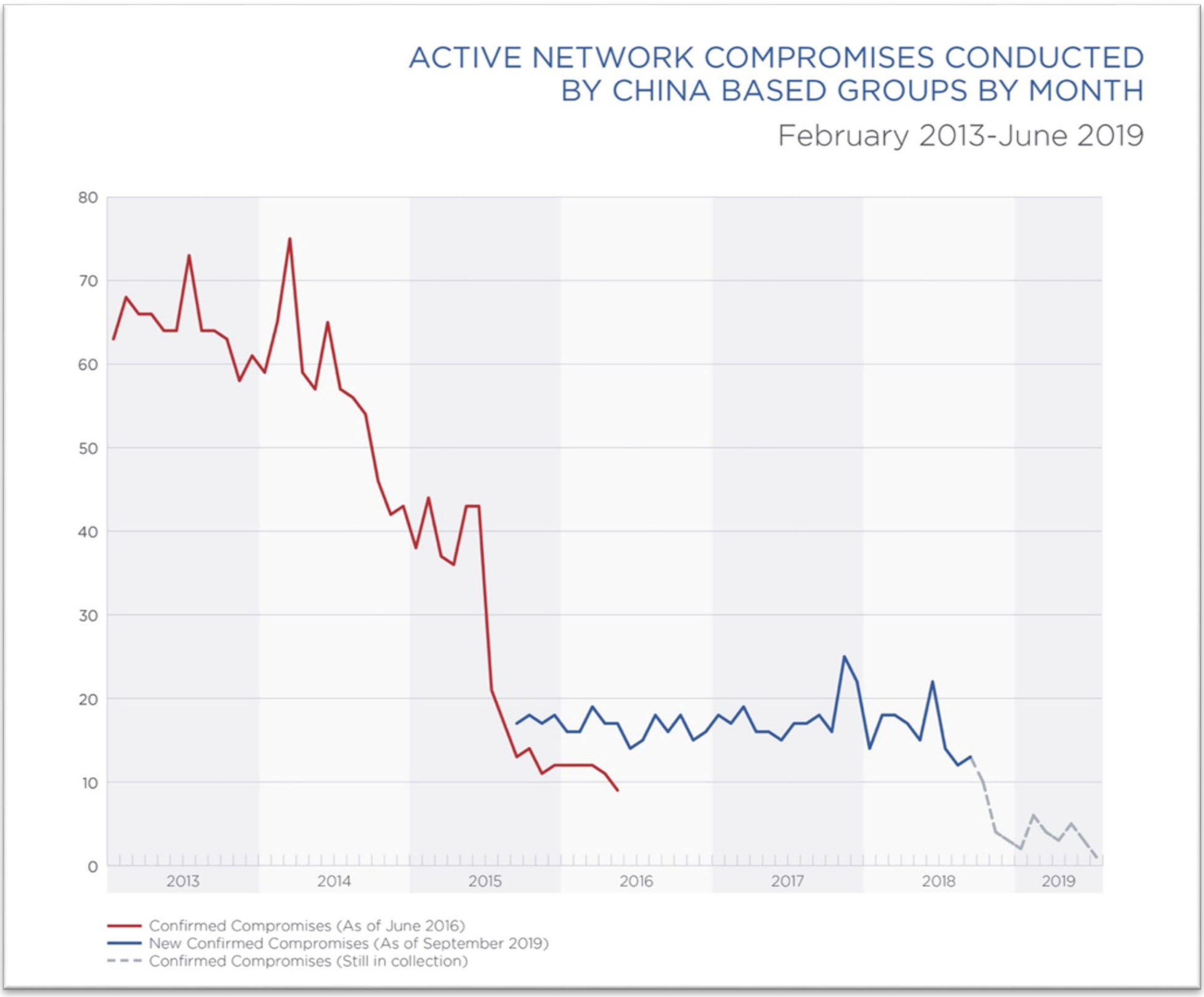
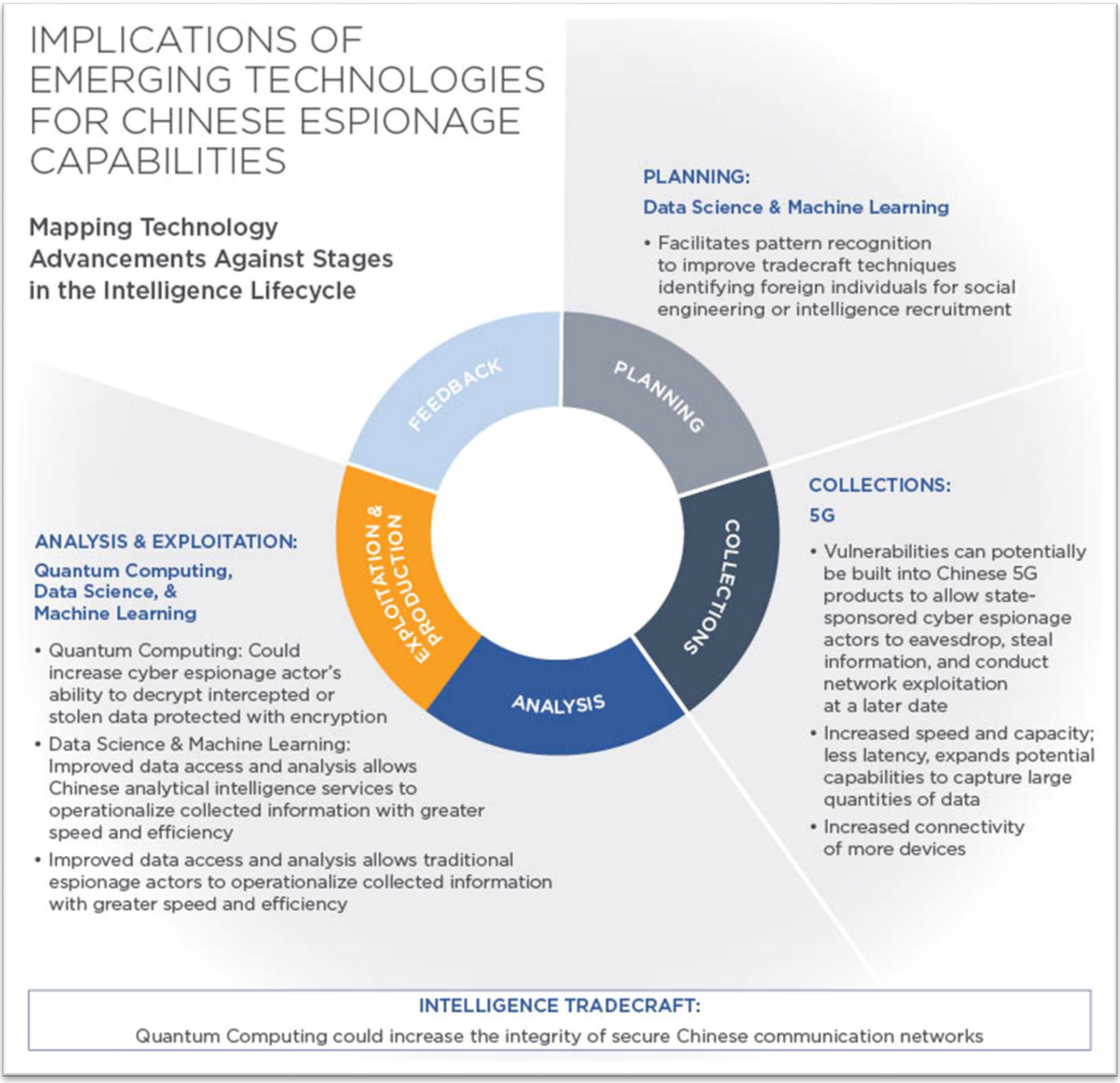


Figure 4: Use Cases for Emerging Technologies Mapped to the Intelligence Lifecycle



IMPLICATIONS OF EMERGING TECHNOLOGIES FOR CHINESE ESPIONAGE CAPABILITIES

Mapping Technology Advancements Against Stages in the Intelligence Lifecycle

PLANNING:

Data Science & Machine Learning

- Facilitates pattern recognition to improve tradecraft techniques identifying foreign individuals for social engineering or intelligence recruitment

COLLECTIONS:

5G

- Vulnerabilities can potentially be built into Chinese 5G products to allow state-sponsored cyber espionage actors to eavesdrop, steal information, and conduct network exploitation at a later date
- Increased speed and capacity; less latency, expands potential capabilities to capture large quantities of data
- Increased connectivity of more devices

ANALYSIS & EXPLOITATION:

Quantum Computing, Data Science, & Machine Learning

- Quantum Computing: Could increase cyber espionage actor's ability to decrypt intercepted or stolen data protected with encryption
- Data Science & Machine Learning: Improved data access and analysis allows Chinese analytical intelligence services to operationalize collected information with greater speed and efficiency
- Improved data access and analysis allows traditional espionage actors to operationalize collected information with greater speed and efficiency

INTELLIGENCE TRADECRAFT:

Quantum Computing could increase the integrity of secure Chinese communication networks

[i] "Chinese State-Sponsored Cyber Operations: Observed TTPs," Cybersecurity & Infrastructure Security Agency, July 19, 2021, https://media.defense.gov/2021/Jul/19/2002805003/-1/-1/1/CSA_CHINESE_STATE-SPONSORED_CYBER_TTPS.PDF

[ii] "Redline Drawn: China Recalculates its Use of Cyber Espionage," Mandiant, June 2016, https://www.mandiant.com/resources/red-line-drawn-china-recalculates-its-use-of-cyber-espionage

[iii] Nalani Fraser and Kelli Vanderlee, "Achievement Unlocked: Chinese Cyber Espionage Evolves to Support Higher Level Missions," FireEye Cyber Defense Summit, October 10, 2019, https://www.fireeye.com/content/dam/fireeye-www/summit/cds-2019/presentations/cds19-executive-s08-achievement-unlocked.pdf

[iv] "Chinese State-Sponsored Actors Exploit Publicly Known Vulnerabilities," National Security Agency, October 20, 2020, https://media.defense.gov/2020/Oct/20/2002519884/-1/-1/0/CSA_CHINESE_EXPLOIT_VULNERABILITIES_UOO179811.PDF

[v] Kathleen Metrick, Parnian Najafi, and Jared Semrau, "Zero-Day Exploitation Increasingly Demonstrates Access to Money, Rather than Skill – Intelligence for Vulnerability Management, Part One," Mandiant, April 6, 2020, https://www.mandiant.com/resources/zero-day-exploitation-demonstrates-access-to-money-not-skill

[vi] Christopher Glyer, Dan Perez, Sarah Jones, Steve Miller, "This Is Not a Test: APT41 Initiates Global Intrusion Campaign Using Multiple Exploits," Mandiant, March 25, 2020, https://www.mandiant.com/resources/apt41-initiates-global-intrusion-campaign-using-multiple-exploits

[vii] Nalani Fraser, Fred Plan, Jacqueline O'Leary, Vincent Cannon, Raymond Leong, Dan Perez, and Chi-En Shen, "APT41 (Double Dragon): A Dual Espionage and Cyber Crime Operation", Mandiant, August 7. 2019, https://www.mandiant.com/resources/apt41-dual-espionage-and-cyber-crime-operation

[viii] Matt Bromiley, Chris Digiamo, Andrew Thompson, Robert Wallace, "Detection and Response to Exploitation of Microsoft Exchange Zero-Day Vulnerabilities," Mandiant, March 4, 2021, https://www.mandiant.com/resources/detection-response-to-exploitation-of-microsoft-exchange-zero-day-vulnerabilities

[ix] Ned Moran and James T. Bennett, "Supply Chain Analysis,: From Quartermaster to Sunshop," Mandiant, November 2013, https://www.mandiant.com/resources/supply-chain-analysis-from-quartermaster-to-sunshop

[x] "The United States, Joined by Allies and Partners, Attributes Malicious Cyber Activity and Irresponsible State Behavior to the People's Republic of China," White House Press Statement, July 19, 2021, https://www.whitehouse.gov/briefing-room/statements-releases/2021/07/19/the-united-states-joined-by-allies-and-partners-attributes-malicious-cyber-activity-and-irresponsible-state-behavior-to-the-peoples-republic-of-china/

[xi] "UK and allies hold Chinese state responsible for a pervasive pattern of hacking," UK National Cyber Security Centre, July 19, 2021, https://www.gov.uk/government/news/uk-and-allies-hold-chinese-state-responsible-for-a-pervasive-pattern-of-hacking

[xii] "China: Declaration by the High Representative on behalf of the European Union urging Chinese authorities to take action against malicious cyber activities undertaken from its territory," Council of the European Union, July 19, 2021, https://www.consilium.europa.eu/en/press/press-releases/2021/07/19/declaration-by-the-high-representative-on-behalf-of-the-eu-urging-china-to-take-action-against-malicious-cyber-activities-undertaken-from-its-territory/

[xiii] Dan Perez, Sarah Jones, Greg Wood, Stephen Eckels, Emiel Haeghebaert, "Re-Checking Your Pulse: Updates on Chinese APT Actors Compromising Pulse Secure VPN Devices," Mandiant, May 27, 2021, https://www.mandiant.com/resources/updates-on-chinese-apt-compromising-pulse-secure-vpn-devices

[xiv] "Operation Cloud Hopper," Pricewaterhouse Coopers, April 2017, https://www.pwc.co.uk/cyber-security/pdf/pwc-uk-operation-cloud-hopper-report-april-2017.pdf

[xv] "APT10 (MenuPass Group): New Tools, Global Campaign Latest Manifestation of Longstanding Threat," Mandiant, April 6, 2017, https://www.mandiant.com/resources/apt10-menupass-group

[xvi] "Two Chinese Hackers Associated With the Ministry of State Security Charged with Global Computer Intrusion Campaigns Targeting Intellectual Property and Confidential Business Information," U.S. Department of Justice, December 20, 2018, https://www.justice.gov/opa/pr/two-chinese-hackers-associated-ministry-state-security-charged-global-computer-intrusion

[xvii] Jack Stubbs, Joseph Menn, and Christopher Bing, "Inside the West's failed fight against China's 'Cloud Hopper' hackers," June 26, 2019, https://www.reuters.com/investigates/special-report/china-cyber-cloudhopper/

[xviii] Raymond Leong, Dan Perez, and Tyler Dean, "MESSAGETAP: Who's Reading Your Text Messages?" Mandiant, October 31, 2019, https://www.mandiant.com/resources/messagetap-who-is-reading-your-text-messages

[xix] "Operation ShadowHammer: a high-profile supply chain attack," Kaspersky, April 23, 2019, https://securelist.com/operation-shadowhammer-a-high-profile-supply-chain-attack/90380/

[xx] "ShadowHammer: Malicious updates for ASUS laptops," Kaspersky, March 25, 2019, https://www.kaspersky.com/blog/shadow-hammer-teaser/26149/

[xxi] Catalin Cimpanu, "FBI warns US companies about backdoors in Chinese tax software," *ZDNet*, July 24, 2020, https://www.zdnet.com/article/fbi-warns-us-companies-about-backdoors-in-chinese-tax-software/

[xxii] Lily Hay Newman, "Facebook Moves Against 'Evil Eye' Hackers Targeting Uyghurs," *Wired*, March 24, 2021, https://www.wired.com/story/facebook-moves-against-evil-eye-hacking-group-targeting-uyghurs/

[xxiii] "China's Study the Great Nation app 'enables spying via back door'," *BBC News*, October 14, 2019, https://www.bbc.com/news/technology-50042379

[xxiv] Ignacio Sanmillan and Matthieu Faou, "Operation SignSight: Supply-chain attack against a certification authority in Southeast Asia," ESET, December 17, 2020, https://www.welivesecurity.com/2020/12/17/operation-signsight-supply-chain-attack-southeast-asia/

[xxv] Timothy R. Heath, "The Consolidation of Political Power in China Under Xi Jinping: Implications for the PLA and Domestic Security Forces," Rand, April 11, 2019, https://www.rand.org/content/dam/rand/pubs/testimonies/CT500/CT503/RAND_CT503.pdf

[xxvi] Cristiana Brafman Kittner and Benjamin Read, "Red Line Redrawn: China APTs Resurface," FireEye Cyber Defense Summit, October 2018, https://www.fireeye.com/content/dam/fireeye-www/summit/cds-2018/presentations/cds18-executive-s05-redline-redrawn.pdf

[xxvii] "China's Intelligence Services and Espionage Operations," Hearing Before the U.S.-China Economic And Security Review Commission, June 9, 2016, https://www.uscc.gov/sites/default/files/transcripts/June%2009%2C%202016%20Hearing%20Transcript.pdf

[xxviii] "U.S. Charges Five Chinese Military Hackers for Cyber Espionage Against U.S. Corporations and a Labor Organization for Commercial Advantage," U.S. Department of Justice, May 19, 2014, https://www.justice.gov/opa/pr/us-charges-five-chinese-military-hackers-cyber-espionage-against-us-corporations-and-labor

[xxix] Dan McWhorter, "APT1: Exposing One of China's Cyber Espionage Units," Mandiant, February 18, 2013, https://www.mandiant.com/resources/apt1-exposing-one-of-chinas-cyber-espionage-units

[xxx] "U.S. Charges Three Chinese Hackers Who Work at Internet Security Firm for Hacking Three Corporations for Commercial Advantage," U.S. Department of Justice, November 27, 2017, https://www.justice.gov/opa/pr/us-charges-three-chinese-hackers-who-work-internet-security-firm-hacking-three-corporations

[xxxi] "Two Chinese Hackers Associated With the Ministry of State Security Charged with Global Computer Intrusion Campaigns Targeting Intellectual Property and Confidential Business Information," U.S. Department

of Justice, December 20, 2018, https://www.justice.gov/opa/pr/two-chinese-hackers-associated-ministry-state-security-charged-global-computer-intrusion

[xxxii] "Seven International Cyber Defendants, Including "Apt41" Actors, Charged In Connection With Computer Intrusion Campaigns Against More Than 100 Victims Globally," U.S. Department of Justice, September 16, 2020, https://www.justice.gov/opa/pr/seven-international-cyber-defendants-including-apt41-actors-charged-connection-computer

[xxxiii] "FACT SHEET: President Xi Jinping's State Visit to the United States" White House Press Statement, September 25, 2015, https://obamawhitehouse.archives.gov/the-press-office/2015/09/25/fact-sheet-president-xi-jinpings-state-visit-united-states

[xxxiv] "Four Chinese Nationals Working with the Ministry of State Security Charged with Global Computer Intrusion Campaign Targeting Intellectual Property and Confidential Business Information, Including Infectious Disease Research," U.S. Department of Justice, July 19, 2021, https://www.justice.gov/opa/pr/four-chinese-nationals-working-ministry-state-security-charged-global-computer-intrusion

[xxxv] Fred Plan, Nalani Fraser, Jacqueline O'Leary, Vincent Cannon, Benjamin Read, "APT40: Examining a China-Nexus Espionage Actor," Mandiant, March 4, 2019, https://www.mandiant.com/resources/apt40-examining-a-china-nexus-espionage-actor

[xxxvi] Scott Henderson, Steve Miller, Dan Perez, Marcin Siedlarz, Ben Wilson, Ben Read, "Chinese Espionage Group TEMP.Periscope Targets Cambodia Ahead of July 2018 Elections and Reveals Broad Operations Globally," Mandiant, July 10, 2018, https://www.mandiant.com/resources/chinese-espionage-group-targets-cambodia-ahead-of-elections

[xxxvii] "Two Chinese Hackers Working with the Ministry of State Security Charged with Global Computer Intrusion Campaign Targeting Intellectual Property and Confidential Business Information, Including COVID-19 Research," U.S. Department of Justice, July 21, 2020, https://www.justice.gov/opa/press-release/file/1295981/download

[xxxviii] Sean O'Connor, "Howo Chinese Companis Facilitate Technology Transfer from the United States," May 6, 2019, U.S.-China Economic and Security Review Commission, https://www.uscc.gov/sites/default/files/Research/How%20Chinese%20Companies%20Facilitate%20Tech%20Transfer%20from%20the%20US.pdf

[xxxix] "Chinese Intelligence Officers and Their Recruited Hackers and Insiders Conspired to Steal Sensitive Commercial Aviation and Technological Data for Years," U.S. Department of Justice, October 30, 2018, https://www.justice.gov/opa/pr/chinese-intelligence-officers-and-their-recruited-hackers-and-insiders-conspired-steal

[xl] "Former GE Engineer and Chinese Businessman Charged with Economic Espionage and Theft of GE's Trade Secrets," U.S. Department of Justice, April 23, 2019, https://www.justice.gov/opa/pr/former-ge-engineer-and-chinese-businessman-charged-economic-espionage-and-theft-ge-s-trade

[xli] Rogier Creemers, Hunter Dorwart, Kevin Neville, Kendra Schaefer, Johanna Costigan, and Graham Webster, "Translation: 14th Five-Year Plan for National Informatization – Dec. 2021" DigiChina Project, Stanford University, January 24, 2022, https://digichina.stanford.edu/work/translation-14th-five-year-plan-for-national-informatization-dec-2021

[xlii] Bill Gertz, "Pentagon Links Chinese Cyber Security Firm to Beijing Spy Service" *The Washington Free Beacon*, November 29, 2016, https://freebeacon.com/national-security/pentagon-links-chinese-cyber-security-firm-beijing-spy-service/

[xliii] Nalani Fraser and Kelli Vanderlee, "Achievement Unlocked: Chinese Cyber Espionage Evolves to Support Higher Level Missions," FireEye Cyber Defense Summit, October 10, 2019, https://www.fireeye.com/content/dam/fireeye-www/summit/cds-2019/presentations/cds19-executive-s08-achievement-unlocked.pdf

[xliv] "U.S. Charges Three Chinese Hackers Who Work at Internet Security Firm for Hacking Three Corporations for Commercial Advantage," U.S. Department of Justice, November 27, 2017, https://www.justice.gov/opa/pr/us-charges-three-chinese-hackers-who-work-internet-security-firm-hacking-three-corporations

[xlv] Paul Mozur, "Beijing Wants A.I. to Be Made in China by 2030," *New York Times*, July 20, 2017, https://www.nytimes.com/2017/07/20/business/china-artificial-intelligence.html

[xlvi] Lily Kuo, "Chinese surveillance company tracking 2.5m Xinjiang residents," *The Guardian*, February 18, 2019, https://www.theguardian.com/world/2019/feb/18/chinese-surveillance-company-tracking-25m-xinjiang-residents

[xlvii] Amy B. Wang, "A suspect tried to blend in with 60,000 concertgoers. China's facial-recognition cameras caught him." *The Washington Post*, April 13, 2018, https://www.washingtonpost.com/news/worldviews/wp/2018/04/13/china-crime-facial-recognition-cameras-catch-suspect-at-concert-with-60000-people/

[xlviii] Philip Tully and Lee Foster, "Repurposing Neural Networks to Generate Synthetic Media for Information Operations," Mandiant, August 5, 2020, https://www.mandiant.com/resources/repurposing-neural-networks-to-generate-synthetic-media-for-information-operations

[xlix] Zhiqun Zhu, "Interpreting China's 'Wolf-Warrior Diplomacy'," *The Diplomat*, May 15, 2020, https://thediplomat.com/2020/05/interpreting-chinas-wolf-warrior-diplomacy/

[l] Georgi Gotev, "Belgium suffers major cyberattack," *Euractiv*, May 5, 2021, https://www.euractiv.com/section/politics/short_news/belgium-suffers-major-cyber-attack/

[li] Charlie Osborne, "Taiwan's major oil refineries struck by malware, causing chaos at gas stations," The Daily Swig, May 6, 2020, https://portswigger.net/daily-swig/taiwans-major-oil-refineries-struck-by-malware-causing-chaos-at-gas-stations

[lii] "Description of the investigation into the ransomware attack on important domestic enterprises [國內重要企業遭勒索軟體攻擊事件調查說明]," Taiwan Ministry of Justice, May 15, 2020, https://www.mjib.gov.tw/news/Details/1/607

[liii] "Justice Department announces court-authorized effort to disrupt exploitation of Microsoft Exchange Server vulnerabilities," U.S. Department of Justice, April 13, 2021, https://www.justice.gov/usao-sdtx/pr/justice-department-announces-court-authorized-effort-disrupt-exploitation-microsoft

[liv] "Motion to Partially Unseal Search Warrant and Related Documents and [Proposed] Order," U.S. Department of Justice, April 13, 2021, https://www.justice.gov/opa/press-release/file/1386631/download

[lv] Allison Peters, "Russia and China Are Trying to Set the U.N.'s Rules on Cybercrime," Foreign Policy, September 16, 2019, https://foreignpolicy.com/2019/09/16/russia-and-china-are-trying-to-set-the-u-n-s-rules-on-cybercrime/

[lvi] Daniel Gordon, "With Friends Like Xi's: China's Ransomware Headache," Seriously Risky Business, January 12, 2022, https://srslyriskybiz.substack.com/p/srsly-risky-biz-thursday-january-39c

OPENING STATEMENT OF DAKOTA CARY, RESEARCH ANALYST, CENTER FOR SECURITY AND EMERGING TECHNOLOGY (CSET), GEORGETOWN UNIVERSITY

COMMISSIONER BARTHOLOMEW: Thank you very much. Mr. Cary.

MR. CARY: I'd like to start by thanking the Commission for extending an invitation to testify today on China's cyber capabilities. Thank you to its members and its staff for interest in this important topic and convening three great panels.

China's cyber capabilities are expanding. Talent cultivation and research are critical to the development of those capabilities, and Chinese universities support both.

Since 2015, China has standardized its cyber security curriculum for university degree programs. It's launched a program to certify some schools as world class cyber security schools. It has built a national cyber security center in Wuhan. And it continues to work with universities on capabilities research.

Over the next decade, China's cyber capabilities are poised to blossom as these universities graduate more well-educated graduates and research continues.

The United States, to adequately address and respond to this development of China's cyber capabilities and the role its universities play in this development, it's first important to understand the relationship between the Chinese Government and these institutions.

My written testimony responds to the series of questions posed by the Commission, and I'm happy to clarify or expand upon those answers during Q&A.

I'll start by first painting a broad picture of the relationship between Chinese state hacking teams and universities. From there I'll discuss the ties between universities and ongoing research, and then touch upon some options for policymakers to consider.

Chinese universities and their relationships with state hacking teams exist on a spectrum. At the least threatening end from a U.S. securities perspective, universities serve in their typical education capacity, giving students the skills they need to be successful cyber security professionals, which in turn develops a national talent base.

At the opposite end of the spectrum, schools like Shanghai Jiao Tong University help conduct operations for the Chinese military. In between are a number of universities that help cultivate talent, support research, and enter into joint research labs or conduct research funded by the PLA or the Chinese security services.

The complete distribution of universities across this spectrum from purely educational to active participants in military hacking campaigns is unclear. However, most schools likely fall under the traditional and accepted educational role, with fewer maintaining close operational ties to the security services.

The PLA and the Chinese security services both use universities to research offensive cyber capabilities. Avenues for collaboration on research include joint research facilities, provincial government research facilities, and competitions that attract attention from large swaths of society. The entire scope of collaboration is detailed in my written testimony.

And what about risk to U.S. institutions on collaborating on cyber security research with these institutions? The United States may benefit more from this collaboration than China does. Cyber defense is a team sport. Researchers who find and disclose software vulnerabilities can secure all users of that particular system. A new technique to identify malware will help everyone defend from attack. In short, the more sharing of defensive research, the better.

As for the development of offensive techniques, Chinese institutions likely lead United States universities because the U.S. Government does not work with U.S. institutions to conduct this research.

Although the U.S. Government does do research with some schools that are titled centers of academic excellence in cyber research, there is by no means a pipeline for offensive research from universities in the United States to the U.S. Government.

Instead, the relationship between China's security services and some of its universities offers a window into its research and its operational pipeline.

The United States should consider listing some universities in China on the Department of Commerce's entity list. Listing these schools will not prevent their work on cyber capabilities, nor will it change the relationship with the Chinese Government. But their capabilities will not slow in development either.

But, by listing these universities on this list, policymakers can prevent other forms of research at these institutions from accessing United States talent or high-end technology necessary to conduct other research.

I want to emphasize that these actions will not change China's hacking capabilities, slow their development, or fundamentally change the relationship with the Chinese Government. But such actions could have knock-on effects on other areas of research.

In the course of my study of Chinese hacking teams, its universities, and its education system, it's clear to me that China has learned many lessons from the United States. Chinese university cyber security degree programs are based on standards created by NIST's National Initiative for Cyber Security Education.

Its awards for excellence in cyber security education are based on the joint National Security Administration-Department of Homeland Security Program to certify some universities in the United States as centers of academic excellence in cyber defense, cyber operations, and cyber research.

China's robot hacking games, referenced in my written testimony, are based on DARPA's 2016 cyber grand challenge. China has hosted more than a dozen rounds of competitions for this capability. In contrast, the United States has not hosted any since 2016.

Time and again, China has studied the U.S. system, copied its best attributes, and in many cases expanded upon its scope and reach. Policymakers should be flattered. We are moving in the right direction.

But the market for cyber security jobs in the United States indicates we are not graduating enough students with relevant degrees. The resulting increase in wages for cyber security professionals as demand goes unmet will attract students to this profession.

But policymakers can do more to encourage the interest in the field at the high school level. Supporting existing programs and expanding the opportunity for more students is the quickest path to success.

Policymakers should look to work with high schools and universities to ensure access to quality computer science education and host public competitions and events that draw attention and interest to the field.

Ongoing research by my colleagues at CSET preliminarily indicates that just over one percent of high school students in the United States are enrolled in AP computer science, with even fewer participating in competitions. Progress at the high school level is starting to take root, however.

From 2018 to 2021, the proportion of high schools offering computer science courses leapt from 35% to over 50%. Twenty-three states even require high schools to offer computer science classes. In the coming months CSET will provide policymakers analysis and recommendations to support such programs.

In the face of an inadequate solution to separate China's universities and its government, policymakers should instead focus on infusing the United States' cyber security pipeline with vigor, attracting qualified candidates from abroad, and supporting ongoing cyber security education initiatives domestically.

Xi Jinping is often quoted with saying that cyber security is ultimately a competition for talent. He's not wrong.

Thank you.

PREPARED STATEMENT OF DAKOTA CARY, RESEARCH ANALYST, CENTER FOR SECURITY AND EMERGING TECHNOLOGY (CSET), GEORGETOWN UNIVERSITY

Back to the Table of Contents

Testimony before the U.S.-China Economic and Security Review Commission on “China’s Cyber Capabilities: Warfare, Espionage and Implications for the United States”

February 17, 2022

Dakota Cary
Research Analyst, Center for Security and Emerging Technology

I would like to thank Chairman Wong and VICE CHAIR Glas for extending an invitation to testify today on China's cyber capabilities. Thank you to the commission members and staff for taking an interest in this important topic and convening three great panels.

China's cyber capabilities are expanding. Talent cultivation and research are critical to that expansion, and China's universities support both. Since 2015, China has standardized its cybersecurity curriculum for university degree programs, launched a program to certify qualifying schools as World-Class Cybersecurity Schools, built a National Cybersecurity Center in Wuhan, and continued work with universities on capabilities research. Over the next decade, China's cyber capabilities are poised to blossom as universities graduate more well-educated cybersecurity degree holders and as research progresses. For the United States to adequately respond to the development of China's cyber talent pipeline and the role its universities play in a capabilities development, it's important to first understand the relationship between the Chinese government and some universities. My written testimony responds to a series of questions posed by the Commission for this hearing, and I am happy to clarify or expand upon my answers during Q&A.

1. **What is known about Chinese universities' cooperation with the Chinese military and intelligence services to carry state-sponsored cyberespionage operations? Why, and in what ways, do Chinese universities facilitate state-sponsored espionage? Please provide specific examples in your answer.**

Chinese universities and their relationship with state hacking teams exist on a spectrum of activities.[1]

At the least-threatening end, from a U.S. security perspective, universities serve in their typical education capacity—giving students the skills they need to be successful cybersecurity professionals, which in turn, develops a national talent base. At the opposite end of the spectrum, schools like Shanghai Jiao Tong University help conduct operations for the Chinese military. In between are a number of universities that help cultivate talent, support research, or enter into joint research partnerships or operate laboratories with, or funded by, the Chinese military and security services.

At the talent-focused end of the spectrum are Zhejiang University and Harbin Institute of Technology. First identified as places of recruitment for Chinese hacking teams by the cybersecurity company FireEye's groundbreaking Advanced Persistent Threat 1 (APT1) report in 2013, these two universities are still graduating students prepared for government service. Talent development at both schools looks different, but they aim for the same output—highly qualified cybersecurity professionals. Zhejiang University students can take classes on writing intelligence reports, alongside classes like how to attack and defend AI systems. Harbin Institute of Technology offers similar courses aimed at getting students recruited by the state. Legacy webpages show many graduates of HIT's cybersecurity school from 2008 to 2014 went to work for the PLA's 54th Research Institute, formerly part of the General Staff

[1] Dakota Cary, "Academics, AI, and APTs: How Six Advanced Persistent Threat-Connected Chinese Universities are Advancing AI Research," (Center for Security and Emerging Technology: March 2021). DOI: 10.51593/2020CA010

Department’s 4th Department (Electronic Warfare), an organization folded into the PLA Strategic Support Force in 2015. The U.S. Department of Justice indicted four members of the 54th Research Institute in 2020 for the hacking of Equifax in 2017.

One step closer to supporting state hacking operations, schools like Xidian University, Hainan University and Southeast University mix education, hands-on practice, and career placement in interesting and innovative ways that help the security services.

Xidian University works to get its graduate students hands-on experience with a provincial bureau of the Ministry of State Security. The university had a relationship with the Third Department of the PLA General Staff Department before it was reorganized into the Network Systems Department in 2015. Xidian University operates a jointly-administered graduate degree program with the Guangdong Bureau of the China Information Technology Security and Evaluation Center (or Guangdong ITSEC). This bureau of the MSS managed a contracted team that was so prolific in hacking that it earned an APT designation, APT3, from FireEye. Xidian University awards degrees and handles admissions; Guangdong ITSEC facilitates hands-on education and pairs graduate students with MSS employees serving as mentors. Together, Guangdong ITSEC employees and Xidian University graduate students pursue research projects that meet the “actual needs” (实际求) of Guangdong ITSEC—essentially, solving technical problems to enable the MSS’s work. The graduate degree program is a clear-cut example of a university and a provincial MSS bureau collaborating to enhance students’ education and encourage students to work for state hacking teams.

Hainan University similarly involved students with the security services, albeit less formally than at Xidian University. A Hainan-based MSS officer and professor at Hainan University were indicted by the U.S. Department of Justice in 2020 for their cyber espionage operations to support the Chinese intelligence services. Starting as early as 2013, the professor allegedly recruited students from on-campus hacking competitions and offered bounties to students and colleagues to procure software vulnerabilities that facilitated hacking operations. One of the professor’s shell companies was even registered to the university library’s address.

At Southeast University in 2015, a professor similarly hosted a hacking competition for students.[2] Unlike normal capture-the-flag competitions where participants hack other teams for points, the professor offered students a real-world opportunity to earn points and gain prestige by attempting to access the network of a U.S. Department of Defense contractor. Technical indicators linked the professor, the infrastructure for the attempted hack of the company, and the competition. An alternative, but equally troubling explanation for the collection of evidence is that the professor was assisting an operation from his university equipment, alongside the contracted company, Beijing TopSec.

[2] Dakota Cary, "Academics, AI, and APTs: How Six Advanced Persistent Threat-Connected Chinese Universities are Advancing AI Research," (Center for Security and Emerging Technology: March 2021). DOI: 10.51593/2020CA010

Besides this one competition, Southeast University has an enduring relationship with the security services. Southeast University also jointly operates Purple Mountain Lab with the PLA Strategic Support Force, where researchers work together on "important strategic requirements", computer operating systems, and interdisciplinary cybersecurity research.[3] Apart from Purple Mountain Lab, a previous report by the USCC found Southeast University to be a recipient of PLA and MSS funding to support the development of China's cyber capabilities. Although the university's ties to the hacking competition and DOD contractor are intriguing, the most consequential aspect of Southeast University's relationship to the state is its enduring research program.

The deepest entanglement between university faculty and the security services is with schools like Shanghai Jiaotong University (SJTU)—where staff both support operations and conduct research to enhance cyber capabilities. The university's cybersecurity degree program is located on a PLA information engineering base in Shanghai. From 2010 to 2014, evidence emerged,

first from leaks to The New York Times, then through additional reporting by Reuters, that SJTU was engaged in cyber operations against the United States. In that period, some university computers and email addresses were tied to hacking campaigns carried out by the PLA. Although technical indicators tying the university to military hacking campaigns have apparently faded, the university almost certainly still supports operations.[4]

SJTU's Cyberspace Security Science and Technology Research Institute, home to the Network Confrontation and Information System Security Testing program, conducts research that enables cyber operations. Within this program, SJTU claims to work on "network and information system testing and evaluation, security testing for intelligent connected networks, APT attack testing and defense, and key cyber range technology."[5] In their own words, this is a bold admission of their own APT work and their perceived value to the PLA's cyber capabilities. Shanghai Jiao Tong University embodies China's military-civil fusion approach; tuition pays for professors' salaries and the military gets new capabilities as a result of their work.

The complete distribution of universities across the spectrum, from purely educational institutions to active participants in APT activity, is unclear; however, most schools likely fall under typical talent training, with fewer schools maintaining close operational and research ties to the security services.

2. **How do Chinese universities' research efforts support the PLA's development of offensive cyber capabilities? Please provide specific examples in your answer.**

[3] *Ibid.*

[4] *Ibid*.

[5] *Ibid.*

The PLA and Chinese intelligence services both make use of university research on offensive cyber capabilities. Avenues for collaboration on research include joint research facilities, research grants from the PLA and MSS, research cooperation with provincial governments, and competitions that attract attention from a wide swath of society.

In some instances, as with Southeast University or Shanghai Jiao Tong University, schools openly operate joint research facilities with the PLA. Under these circumstances, the lab-to-field pipeline is clear and direct. Similarly, China's National Cybersecurity Center in Wuhan is home to two universities—Wuhan University and Huazhong University of Science and Technology—and hosts two laboratories that likely facilitate government research.[6] The Offense-Defense Lab and the Combined Cybersecurity Research Institute both stand out as candidates for collaboration with the security services. The 13th bureau of the MSS, which has managed some hacking campaigns in the past, has an office at the Combined Cybersecurity Research Institute. The institute combines university academics with private-sector researchers to work on strategic capabilities.

Funding from the PLA or the MSS also secures access to offensive cyber capabilities from universities. In a previous USCC-commissioned report from 2012, Northrop Grumman researchers demonstrated that a number of schools received money from specific programs designed to enhance China's offensive cyber capabilities. Today, such programs likely continue.

Some schools are working with provincial governments to conduct research into cyber capabilities. Zhejiang University, a school I've mentioned for its high-quality education and is a known favorite for recruiting hacking talent, is working with the Zhejiang Provincial government to operate Zhejiang Labs.[7] Zhejiang Labs is conducting research on AI's application to cybersecurity and key cyber range technologies. Huazhong University of Science and Technology, which I've mentioned in context of the National Cybersecurity Center, is also a partner of Zhejiang Labs. The National University of Defense Technology (NUDT), a PLA university, is represented on an oversight board for the laboratory. This relationship typifies more general access to technology development conducted outside the military and in coordination with other government bodies and universities.

Finally, China has copied parts of the United States' innovation strategy to incentivize research at universities that can produce sought-after capabilities. DARPA hosted a Cyber Grand Challenge in 2016 to spur innovation in automated software vulnerability discovery, patching, and exploitation technology.[8] These tools offer both offensive and defensive capabilities that promise to increase the scale and pace of software vulnerability discovery—a key component of

[6] Dakota Cary, "China's National Cybersecurity Center" (Center for Security and Emerging Technology, July 2021). https://doi.org/10.51593/2020CA016

[7] Dakota Cary, "Down Range" (Center for Security and Emerging Technology, forthcoming).

[8] Dakota Cary, "Robot Hacking Games" (Center for Security and Emerging Technology, September 2021). https://doi.org/10.51593/2021CA005

cyber operations, and cybersecurity generally. China has emulated that competition system and since 2017 has hosted at least a dozen rounds of competitions to develop the technology.

Just two years after the People's Liberation Army's National University of Defense Technology won the first competition in 2017, the military started managing competitions of its own to concentrate resources on the development of tools to automate the vulnerabilities lifecycle. By last year, a laboratory run by the PLA Equipment Development Department hosted its first such competition. These management and oversight roles situate the PLA in an ideal position to evaluate and attract the best tools and talent. The 13th Bureau of the MSS has also hosted some of these competitions, which, when supported by enough funding, can spur technological innovation and investment. This competition structure is the most open form of research for cyber capabilities, as it allows the military (or any government agency) to draw on research from universities and the private sector.

3. **How do Chinese universities help the Chinese military and intelligence services identify and recruit talented cybersecurity professionals? Please provide specific examples in your answer.**

China's mechanisms for identifying and recruiting talent are typical for governments. There is some evidence that typical job promotion events, like career fairs or alumni engagement events, serve to promote jobs in the military or intelligence services at most universities.

Some schools shoulder additional responsibility for talent cultivation and recruitment, however. Xinhua News, China's state-run news agency, reported in 2017 that the PLA Strategic Support Force, which includes the department responsible for hacking operations—along with those responsible for space missions and operations support, signed an agreement with nine entities "to train high-end talents for new combat forces." According to Xinhua, "The universities will coordinate in recommending high-level talents in emerging S&T disciplines for priority consideration for recruitment by the [Strategic Support Force]; the SSF will designate key personnel for cultivation to go to research institutes and key laboratories for academic exchanges and further training; jointly, they will organize international and domestic competitions to find and select talents with special expertise, the best of whom will be recruited by the SSF."[9]

The full agreement between the PLA and these nine institutions is not public, so the program's particulars are unclear. Six of the entities participating are universities and three are defense industry enterprises.

University Partners of the PLA Strategic Support Force

- University of Science and Technology of China
- Shanghai Jiao Tong University

[9] "Strategic Support Force to Cooperate with Nine Local Organizations to Cultivate High-End Talents for New Combat Forces," 李国利 and 宗兆盾, Xinhua News Agency (New China News Agency; 新华社), July 12, 2017. https://perma.cc/PM8L-3WU4

- Xi'an Jiaotong University
- Beijing Institute of Technology
- Nanjing University
- Harbin Institute of Technology

Partnering Defense State-Owned Enterprises

- China Aerospace Science and Technology Corporation [CASC]
- China Aerospace Science and Industry Corporation [CASIC]
- China Electronics Technology Group Corporation [CETC]

4. **Is there significant cooperation occurring between U.S. universities and Chinese universities linked to state-sponsored cyberespionage? If so, does this cooperation create risks for the United States in general and for these U.S. universities in particular? Please address whether current export controls and sanctions lists are adequate to mitigate these risks in your answer.**

Each university mentioned here, and their relationship with U.S. institutions, is different. Some institutions, like Zhejiang University, are world-renowned for their cybersecurity education program. The university attracts the best minds of cryptography studies from around the world and its graduates are highly-prized, fiercely intelligent individuals that the United States should welcome. Conversely, institutions like Shanghai Jiaotong University have relatively little international collaboration and more important operational roles. Sanctioning schools that have helped on past cyber operations might feel like a worthwhile policy initiative, but I contend it is not.

The tools needed to conduct hacking campaigns are ubiquitous. All that most operators need is a computer, an internet connection, and training. Even if these institutions were subject to export controls, it's unlikely such policies would matter much to China's cyber capabilities. Beyond the cyber domain, such policies have merit. Advanced research often requires advanced tools, so a listing on the Department of Commerce's Entity List is still appropriate. But policymakers should not expect it to slow the development of China's cyber capabilities.

U.S. institutions that collaborate with these Chinese institutions are not at any greater risk of intelligence collection than other institutions because of their relationship. This is to say that, as in the United States, PRC policymaker intelligence requirements drive the collection and analysis cycle of operations. If a university is researching a technology that the CCP has determined to be of value, Chinese hacking teams will try to collect it, regardless of whether the school collaborates with Chinese institutions.

But what about scientific collaboration on cybersecurity research with these institutions? Again, the United States may benefit more from this collaboration than China does. Cyber defense is a team sport. Researchers who find and disclose software vulnerabilities responsibly can help secure all users of that system. A new technique for identifying malware will help everyone else defend from attack. In short, the more sharing of defensive research the better. As for the development of offensive techniques, Chinese institutions likely lead U.S. universities because the U.S. government does not work with universities to conduct offensive research for cyber operations. Although the U.S. government does designate some schools as Centers of Academic Excellence in cyber research, there is by no means a pipeline of offensive research from U.S. universities to the U.S. government. Instead, the relationship between China's security services and some of its universities offers a window into its research and operational priorities.

5. **What is known about how Chinese technology companies' cooperation with the Chinese military and intelligence services to carry out state-sponsored cyberespionage operations? Do Chinese technology companies located within China assist in tasks such as identifying adversary vulnerabilities, developing exploits, or acquiring and processing data collected through cyberespionage?**

The Chinese Party-state's relationship with big tech companies is currently being re-written. As Adam Kozy noted in his testimony, there is an existing mandate for firms to support Chinese intelligence collection. The Chinese government has made clear in recent months that the CCP rules, and companies obey. The CCP has gone so far as to cause the delisting of Didi Chuxing, a ride hailing company, from the New York Stock Exchange.[10] CEOs have been cowed and even disappeared for months. How this new era of control over tech companies impacts their relationship with the security services is unclear, but we do know about their past relationship.

Some cybersecurity companies work hand-in-hand with the PLA and security services, supporting hacking campaigns, training operators, or educating the next generation of hackers. Companies like Beijing TopSec work on all three facets. Chinese media outlets indicate that Beijing TopSec trains PLA hackers. As discussed earlier, Beijing TopSec was also tied to the Southeast University hacking competition and hack of Anthem Insurance. The company has also set up shop at China's National Cybersecurity Center in Wuhan, where it works with the universities on campus to educate the next generation of cybersecurity professionals. Beijing TopSec is also a partner of the combined cybersecurity research institute on the National Cybersecurity Center's campus. Other cybersecurity companies, such as Qi'anxin, Qihoo360, and NSFocus, also fit the bill.

Thanks to reporting by Zach Dorfman, we know that some big tech companies are sometimes tasked with helping the security services process large swaths of data, and that such companies often do so begrudgingly.[11] Such labor is considered a cost of doing business, not another profitable venture for the firm. This relationship is interesting because it suggests a few things about the Chinese security services: 1) they are either not capable, or inadequately staffed, to deal with the tasks policymakers are asking of them, 2) they are not able to attract, retrain, or train the talent necessary to perform these tasks, and 3) they see existing talent in private-sector firms as both acceptable and accessible when help is required.

[10] Stevenson, Alexandra, and Paul Mozur. 2021. "With Its Exit, Didi Sends a Signal: China No Longer Needs Wall Street." *The New York Times*, December 3, 2021. https://www.nytimes.com/2021/12/02/business/china-didi-delisting.html.

[11] Dorfman, Zach. 2020. "Tech Giants Are Giving China a Vital Edge in Espionage." Foreign Policy. December 23, 2020. https://foreignpolicy.com/2020/12/23/china-tech-giants-process-stolen-data-spy-agencies/.

China has taken steps in recent years to increase its technical talent pipeline, so as these degree holders become more common, the pressure for collaboration on data processing may ebb.

China recently expanded its collection of private cybersecurity research to improve state capabilities. In late 2021, the Ministry of Industry and Information Technology began requiring any individual or company doing business in China to disclose software vulnerabilities to the ministry within 48 hours of becoming aware of the vulnerability. The rule effectively co-opts the entire software security ecosystem of China into its hacking operations, allowing operators to collect software vulnerabilities before the companies themselves become aware of them. According to the cybersecurity company Recorded Future, the MSS has run a capabilities pipeline like this in the past. The MSS delayed publication of submitted vulnerabilities to China's public software vulnerability database, and subsequently used vulnerabilities that were particularly severe to facilitate hacking operations.

A notable exception to this rule—one that apparently caused the company to lose a government contract—occurred in 2021 when an Alibaba employee first reported a now-famous Log4j vulnerability to Apache. China's government appears to have been skipped in the reporting process. Why the Alibaba researcher did not report the vulnerability to the government first is unclear. After his company was reprimanded, researchers might be hesitant to skip over the government again in the future.

The policy dramatically changes the relationship between private-sector cybersecurity researchers and state hacking teams, effectively conscripting researchers that might otherwise not have chosen to report a software vulnerability to the state.

6. **Is there any evidence that Chinese telecommunications companies based outside of China have built "backdoors" in their systems embedded in foreign countries' infrastructure that the PLA or MSS can take advantage of during a crisis or conflict?**

Purpose-built backdoors are difficult to identify. Faulty lines of code appear all the time by accident, so building some on purpose may not be necessary or worthwhile. Moreover, purpose-built backdoors are indistinguishable from accidental ones.

But backdoors are also unnecessary if the firm cooperates with the government. Documents obtained by The Washington Post indicate Huawei works with the Chinese government to facilitate domestic surveillance, using techniques like relationship mapping, voice ID, and other tools.[12] China's National Security Law allows the government to compel companies to work with the government to facilitate espionage. Huawei's prevalence in foreign telecommunications networks would be a great asset to Chinese intelligence services. After the

[12] *The Washington Post*. 2021. "Documents Link Huawei to China's Surveillance Programs," December 14, 2021. https://www.washingtonpost.com/world/2021/12/14/huawei-surveillance-china/.

African Union realized the data on its servers, which were running on Huawei tech, was downloaded to servers in Shanghai daily, scrutiny of the firm and its relationship with the Chinese government rightly increased.[13] Until leaked documents confirm China's use of Huawei's networks, we can only speculate about Huawei's involvement in the operation and its relationship with the intelligence services.

7. **The Commission is mandated to make policy recommendations to Congress based on its hearings and other research. What are your recommendations for Congressional action related to the topic of your testimony?**

In late 2021, a video of a Chinese woman in Australia on the phone with police in China went viral. The woman received a call from her father's cell phone. When she answered, she found herself face-to-face with a Chinese police officer. The officer pressured her about the content of a twitter account she was allegedly running. Her father sat in the police officer's office and looked on. The woman's distress throughout the phone call is, at times, haunting. She is pushed to return to China, asked when her visa will expire, and told to stop her online activity.

The episode highlights a dark reality about China's authoritarian system and its sweeping claim over Chinese people abroad. Individuals and their families can be subjected to cruel pressure and manipulated to perform tasks against their will. This extends to Chinese companies, too. In cases of scientific cooperation, research and development, and security research, that same pressure can open doors for the Chinese intelligence services and the PLA. In these instances, Chinese citizens are the victims of a deeply repressive system. I want to emphasize my personal feelings of grief and distress for people who live under authoritarian rule without recourse for change.

At the same time, the United States benefits from foreign talent, and China's graduates are among the best in the world. There are no policy mechanisms that will divorce the relationship between universities and the Chinese state—they are bound together under the CCP's authoritarianism. But this relationship does not mean the United States must cut itself off from interacting with these universities or hiring their graduates. Instead, policymakers should consider offering visas to family members of individuals immigrating from China. Such a policy could attract high-end, PhD talent that drives research and innovation. Without family members in China that can be subjected to pressure from the CCP, the United States can more assuredly welcome these talented individuals.

The United States should consider listing some universities, such as Shanghai Jiao Tong University or Southeast University, on the Department of Commerce's Entity List. Listing these schools will not prevent their work on cyber capabilities for the Chinese government, nor will it change their relationship

[13] Sherman, Justin. n.d. "What's the Deal with Huawei and This African Union Headquarters Hack?" New America. Accessed February 9, 2022. https://www.newamerica.org/cybersecurity-initiative/c2b/c2b-log/whats-the-deal-with-huawei-and-this-african-union-headquarters-hack/.
John Aglionby, Emily Feng And Yuan Yang. 2020. "African Union Accuses China of Hacking Headquarters." Financial Times. April 24, 2020. https://archive.vn/WRobn.

with the government. Their capabilities development will not slow either. But, by listing these universities, policymakers can prevent other departments at these universities from accessing United States talent via collaboration, or some high-end technologies necessary to conduct research. I will emphasize that these actions will not change China's hacking capabilities, slow their development, or fundamentally change the relationship with the Chinese government. But such actions could have knock-on effects in other areas of research.

In the course of my study of China's hacking teams, its universities, and its education system, it is clear to me that China has learned many lessons from the United States. China's university cybersecurity degree programs are based on the standards created by the NIST's National Initiative for Cybersecurity Education. Its awards for excellence in cybersecurity education are based on the joint National Security Agency/Department of Homeland Security program to certify some universities as centers of academic excellence in cyber defense, cyber operations, and cybersecurity research. China's Robot Hacking Games, referenced earlier in my testimony, are based on DARPA's 2016 Cyber Grand Challenge. China has hosted more than a dozen rounds of competitions for Robot Hacking Games. In contrast, the United States has not hosted any since 2016. Time and again, China has studied the U.S. system, copied its best attributes, and in many cases expanded the scope and reach.

Policymakers should be flattered. We are moving in the right direction. But the market for cybersecurity jobs in the United States indicates that we are not graduating enough students with relevant degrees. The resulting increase in wages for cybersecurity professionals as demand goes unmet will help draw students' attention to the field, but policymakers can do more to encourage interest in the field at the high school level. Supporting existing programs and expanding the opportunity for more rising students is the quickest path to success. Policymakers should look to work with high schools and universities to ensure access to quality computer science education and host public competitions and events that draw attention and interest to the field. Ongoing research by my colleagues at CSET preliminarily indicates that just over 1 percent of high school students in the United States are enrolled in AP Computer Science, with even fewer participating in cybersecurity competitions. Progress at the high school level is starting to take root, however. From 2018 to 2021, the proportion of high schools offering computer science courses lept from 35 percent to over 50 percent.[14] Twenty-three states even require high schools to offer computer science classes.[15] In the coming months, CSET will provide policymakers analysis and recommendations to support such programs.

In the face of an inadequate solution to separating China's universities and the government, policymakers should instead focus on infusing the United States' cybersecurity talent pipeline with vigor, attracting qualified professionals from abroad, and supporting ongoing cybersecurity education initiatives domestically. Xi Jinping is often quoted saying that "Cybersecurity is, ultimately, a competition for talent." He's not wrong.

[14] "2021 State of CS Report." Code.org. Accessed January 28, 2022. https://advocacy.code.org/stateofcs

[15] "State of Computer Science Education - CS Advocacy." Accessed January 28, 2022. https://advocacy.code.org/2018_state_of_cs.pdf.

Appendix for Testimony before the U.S.-China Economic and Security Review Commission on “China’s Cyber Capabilities: Warfare, Espionage and Implications for the United States”

February 17, 2022

Dakota Cary
Research Analyst, Center for Security and Emerging Technology

Appendix

U.S. companies that produce software often have bug reporting programs. These programs allow hackers to submit software vulnerabilities they find in a company's product to the firm in return for compensation. The more severe the bug, the higher the payout. Some security researchers earn enough money to make a career out of this process.

Some companies in the United States host a marketplace for firms and researchers. These marketplaces facilitate the submission of software vulnerabilities to firms and payment to researchers. In short, they are the middleman.

The software vulnerabilities submitted by researchers are the same kinds of vulnerabilities that facilitate hacking campaigns. In 2021, China's Ministry of Industry and Information Technology implemented a policy requiring researchers in China to submit any software vulnerability they find to the government for evaluation. This policy effectively weaponizes the cybersecurity researcher ecosystem in China—allowing state hacking teams to pull software vulnerabilities for campaigns from any researcher in China who discovers them.

The United States is home to many of the world's leading software companies. These companies pay researchers from around the world to help secure their products. This relationship is critical for firms to secure their products from exploitation by criminals and foreign governments. The table below shows the total dollar amount, as well as the percentage of overall payments, paid to researchers in a given country. One of the largest software bug platforms in the United States US provided this data, and wishes to remain unnamed. Behind researchers in the United States, those in China rank second in providing software vulnerabilities to U.S. firms in exchange for cash. In 2021, these Chinese researchers received 10 percent of the $44 million spent by U.S. companies on this particular platform.

The data provides the following insights:

- China's talent pool for software security rivals the United States, India, Russia, and the United Kingdom. Although this data is from one year and from one marketplace, a holistic analysis would likely position these countries in a similar order.

- China's policy that researchers must submit vulnerabilities to the Ministry of Industry and Information Technology creates an incredibly valuable pipeline of software capabilities for the state. The policy effectively bought at least $4m worth of research for free. Some vulnerabilities may fetch much more on the black market so these values are probably discounted. Moreover, there may be a significant gap between what a company pays for a vulnerability and the cost of the ensuring damage the same bug could have caused if left unpatched.
- U.S. companies benefit from the participation of Chinese cybersecurity researchers. Evaluating the counterfactual—if Chinese researchers did not, or were not allowed to submit vulnerabilities—is difficult. Some bugs might have just been found first by someone from China,

but also found later by other researchers. It's hard to know. But what is clear is that U.S. companies derive significant value from Chinese hackers who submit software vulnerabilities to firms.

- International researchers accounted for 85 percent of the payouts of software bugs submitted to U.S. companies on this particular platform in 2021. No other figure can capture the extent to which U.S. firms benefit from international cooperation. The data emphasizes that cybersecurity is a team sport.

Payments made by U.S. companies to researchers in 2021.

Country of Researcher/Recipient	Total Amount Paid	Percentage of Total Amount Paid by US
United States of America	$6,718,923	15%
China	$4,220,302	10%
India	$4,055,807	9%
Russian Federation	$2,047,212	5%
United Kingdom of Great Britain and Northern Ireland	$2,029,512	5%
Germany	$1,698,018	4%
Canada	$1,674,918	4%
Netherlands	$1,190,940	3%
Argentina	$1,103,724	3%
Australia	$1,072,930	2%
France	$1,029,796	2%

Spain	$982,472	2%
Belgium	$892,722	2%
Morocco	$820,959	2%
Sweden	$807,166	2%
Vietnam	$735,786	2%
Brazil	$730,918	2%
Ukraine	$712,147	2%
Nepal	$667,125	2%
Turkey	$661,353	1%

Source: Information provided to CSET on a private basis by a large U.S.-based software bug reporting platform.

PANEL II QUESTION AND ANSWER

COMMISSIONER BARTHOLOMEW: Thank you very much. We're going to do our questions in reverse alphabetical order this time, so I'm going to start with my co-chair, Chairman Wong.

CHAIRMAN WONG: Thank you, Carolyn. My first question is kind of a specific technical question for Mr. Kozy. In your recommendations on active defense and offense, you mention or recommend that we recommend that we deputize and create standards and procedures for private cyber security companies to assist in deception and denial techniques on behalf of their customers.

Could you explain, what is deception and denial technique, what does that actually mean?

MR. KOZY: Sure, I'd be happy to. In this specific case, I like to think of this less as letters of mark where you're kind of pursuing almost a piracy approach to cyber, private cyber companies going after these actors. But instead assisting in, this would be categorized more as active defense.

It's basically trapping an adversary within a network, which allows them to basically observe and collect intelligence on how this adversary operates. It gains a significant amount of intelligence for our intelligence agencies and private security firms while basically preventing the actor from accessing the crown jewel, so to speak.

CHAIRMAN WONG: And why would the government need to deputize and create standards on this and be involved in that?

MR. KOZY: I believe that this is something that needs careful consideration and control. Because if left unchecked, it could rapidly spiral out of control.

And there are specific entities that are already, you know, have these capabilities that I think would be up to the task. However, I believe that for the most part these private sector firms are sought out for their expertise for these types of scenarios.

And being former FBI myself, I can tell you that there's still a very significant gap sometimes between what the Bureau is able to see and what the private sector companies are able to respond to with signing NDAs with these companies and these companies preferring to maybe not seek federal help right away.

CHAIRMAN WONG: My second question's broader, and this could be for Mr. Kozy as well as Ms. Vanderlee considering your experience. You know, in traditional espionage, there are norms of conduct and understandings developed, you know, unwritten over decades and in some cases centuries of what is done. And if you fall outside of those norms, what could be done to you in retaliation.

Is it the -- am I getting this right that we can look at the cyber arena, particularly cyber espionage, and say we're in an early stage where these norms have not been developed and that it will simply take some time, a few decades, for these norms to develop, particularly as the technology evolves, where we can reach some sort of stability with our adversaries on what is and is not permissible in the espionage space in cyber?

And we'll go to Ms. Vanderlee first. Is that kind of a good way to think about this, or not?

MS. VANDERLEE: To be honest, I am not -- I don't necessarily agree that it is that norms do not exist. I think that the United States has its understanding of what behavior is acceptable and China has its understanding of what behavior is acceptable. And they will continue to conduct all the behavior that they consider to be acceptable until the cost outweighs the benefit.

So I don't think that it is that they do not understand our preferences or how we would define acceptable or unacceptable behavior. I think it is simply that they have more to gain by continuing to do the activity that we would prefer they not do than lose if -- if they were to persist in it.

CHAIRMAN WONG: Mr. Kozy.

MR. KOZY: Heartily agree with that. I do believe that they have significantly more to gain and they've done the risk, you know, analysis on why they are going to continue doing this. However, I would just add that the U.S. has -- they've followed the U.S.'s lead with a lot of these things, including how to conduct cyber warfare and cyber espionage. And so I do believe it is up to the U.S. to set some of those harder consequences for overstepping what we see as lines because we are in that leadership capacity and setting many of those cyber norms.

CHAIRMAN WONG: Thank you.

COMMISSIONER BARTHOLOMEW: All right, Commissioner Wessel.

COMMISSIONER WESSEL: Thank you to all our witnesses. Let me pull that thread that Chairman Wong just pulled at, because I don't think that's about norms. And Ms. Vanderlee, let me first ask you to respond.

You said it's -- there are norms, but then went on to say that it's really whether the costs outweigh the benefits. That's not to me a norm, that's just a cost equation.

Is there -- there are -- there are no clear norms that we think are appropriate for responsible stakeholders. It is simply a cost-benefit equation. Can you respond to that?

MS. VANDERLEE: Sure. So maybe to add some nuance to the previous response, I do think that China recognizes that there is at least a little bit of losing face or diplomatic cost to being seen as conducting activity that is not obviously above-board.

That's why we see them coming out with statements denying threat activity, saying there's no proof. Saying, you know, China's also targeted by significant cyber threat activity.

So they're definitely paying attention to what is being said in international media about their activity and obviously shaping -- attempting to shape the narrative, both at home and abroad, about what the Chinese Government is doing and the, you know, moral underpinnings of this activity and whether it should be considered righteous or not.

So there's the -- there's the symbolic norm public face element of the situation, but there's also the reality of the day-to-day collections priorities and economic development priorities and military and political priorities that may -- that may become more important than the more symbolic element in certain situations.

COMMISSIONER WESSEL: Okay, thank you. It sounds to me that's still a cost-benefit analysis, you know, that whether the shame, you know, results in certain diplomatic or other costs.

Do you believe we in the -- for the other panelists as well -- need to create a new cost arsenal, if you will, that we need to make this costlier for Chinese activities? You know, a series of indictments, you know, I think they view as a cost of doing business. There has not been any major disruptive responses yet to Chinese incursions -- cyber incursions.

MR. KOZY: I would love to hop in if that's all right.

COMMISSIONER WESSEL: Please.

MR. KOZY: I do believe that with regard to your question about norms, you know, it is a norm that every country commits espionage, including the U.S. But I would say that we say that we draw the line pretty firmly around the NSA doing cyber operations to benefit our technology companies, which China has no problem doing.

So that is a key difference that I believe China undertakes, and is one of those norms that we do need to set. And the way that we establish the boundaries around that is to establish meaningful consequences.

One of my top recommendations is to impose costs and consequences that actually have a bearing and will prevent these actors from undertaking these operations. I don't believe that there has been anything that has necessarily dissuaded China from carrying out these operations. And it is clear that the naming and shaming strategy that we've pursued over the past few years is relatively ineffective at curbing cyber espionage, and is basically akin to handing their intelligence services a report card on how their operations are functioning.

COMMISSIONER WESSEL: Thank you. Let me just quickly with my remaining seconds, I think all of us on the Commission have a high regard for our military, our men and woman in uniform, etc. None of us are questioning the work that they are doing. They are actively pursuing U.S. interests. We're not questioning that here today.

We are only seeking to address what Chinese capabilities are and how we might respond to those.

COMMISSIONER BARTHOLOMEW: All right, thank you. Commissioner Scissors.

COMMISSIONER SCISSORS: I have a question for Mr. Cary. First, a comment. I noticed a parallel between the way you described Chinese corporate cooperation in cyber with the way I described Chinese cooperation with the BRI.

You know, there's this -- the companies often dragged grudgingly into doing these things, they don't have any choice, it's costly for them. There may be benefits to them down the road, but it's interesting to -- that the relation between the state and the corporate sector can be similar in such different domains.

My question is you're in charge, you know, this is following up on Mike and it's following up on what a number of commissioners and witnesses said. I'm giving you authority, you get to apply the sanctions you want. Not the useless entities list, that's an editorial comment on my part.

Any sanction you want, and I'm going to -- I'm going to set up Shanghai Jiao Tong as possibly the worst, in terms of our interest, Chinese university. Would you say I'm bringing out the big guns on Shanghai Jiao Tong, or would you say look, even -- I can do anything.

They're the worst and you're the worst, I'm still not targeting Chinese universities at the top of the list. I got bigger fish to fry. So I'm trying to get a sense.

I did get a sense of how -- how you structured, you know, divide the universities up, but I'd like to get a sense of where the universities rank in terms of harming U.S. interests. They're way below the corporate sector, they're comparable with it, they're way below MSS, wherever.

You know, if you had full authority, would you put the universities near the top of the target list, or not really?

MR. CARY: I certainly think that some of the universities should be considered near the top of that list, and the reason is for their operational role. You know, the Chinese Government likes to work with some institutions because that's where the talent is.

And if we sanction particular institutions, it's quite easy to hire the same people at a different facility, fund them, and set up the, you know, use the same lab you were using under a different name.

So universities with an operational role should be considered alongside those other institutions that are conducting hacking operations. I think that some institutions are just a heavier weight than others, they deserve more scrutiny.

COMMISSIONER SCISSORS: Thank you, I appreciate that answer. Ms. Vanderlee, I have a completely unfair question to ask you, but it was sparked by your comment at the end of your testimony.

I, normally when I hear the U.S. should work with allies on economic issues, I think oh good, now I don't have to think about this for three years, because that's at least how long it's going to take for anything to happen in terms of our working with allies.

But that's not cyber, where I don't know what I'm talking about. At the end you were talking about cooperating with our allies to some extent. Can you briefly, and this is unfair, characterize our allied capabilities versus ours?

I mean, are we talking about they're small-scale versions of the U.S. but they're right there with us, and you know, narrower capabilities? Or they're terrible at offense, or whatever it happens to be. Can you, you know, take two minutes to just say this what our allies offer us in terms of capabilities?

MS. VANDERLEE: Sure. I will do my best. I do not have detailed or first-hand knowledge of specific capabilities of our allies and partners. However, China conducts collections, they conduct operations around the globe. Clearly the United States is one their collections priorities.

But China conducts significant activity in Japan, South Korea, Australia, the UK, France, Germany. So any of these countries may have access to data that we did not directly observe. And so if these allies and partners are able to provide the evidence and provide documentation and perhaps do proactive releases, as we have done, or partner with the United States, as we have done particularly with other Five Eyes countries, there's absolutely threat activity that they are observing and they can -- by them releasing information into the open source, then U.S. information comes into the open source.

And private sector and other companies or other organizations are able to collate this and bring a broader picture of what is going on in Chinese cyber espionage activity. We get a better understanding of their capabilities. And China has fewer, you know, fewer legs to stand on in terms of denying the activity.

COMMISSIONER SCISSORS: Thanks, I realize it was an unfair question. I yield my ten seconds.

COMMISSIONER BARTHOLOMEW: Thank you. Commissioner Shriver.

COMMISSIONER SHRIVER: Thank you. And thanks to our witnesses for excellent contributions.

I want to ask about something related to Chinese goals and data. They seem, by my reading, to be very obsessed with data, protection of their own and collection of others.

It seems that they're -- one of the main motivations for pulling down listings on our exchanges was fear of having to divulge, these companies divulging Chinese data, and particularly in the case of the rideshare company and the rich data that might be available to others if there were to closure -- disclosure requirements.

And they're clearly interested in data collection. Mr. Kozy, you mentioned the OPM hack, and I think mentioned others, where the primary goal seemed to be acquiring data. And I think you further said in your statement that one of the purposes is to further refine that -- get this big pool of data and then further refine that to conduct -- (telephonic interference).

COMMISSIONER BARTHOLOMEW: Whoops.

COMMISSIONER SHRIVER: I wonder if it's useful to broaden that a bit and talk about, you know, Chinese goals related to protection of data or maybe more to the point for this discussion, a collection of mass amounts of data, and what other vulnerabilities that might create and what other goals they might have just beyond targeting particular individuals of concern. Because this seems to be almost near obsession on the Chinese part.

MR. KOZY: Yeah, I would just comment that, you know, I think a lot of previous, especially U.S. intelligence community thinking was around, you know, the Chinese intelligence's stove-piping of intelligence and maybe not being able to share across lines with the PLA and the MSS.

Or I would also bring up the United Front Work Department, which focuses quite a bit on political side of things. And really what this proves is that these entities are all working together. That the collection of the data allows them to do follow-on targeting.

I specifically talked about that with the APT41 and Wicked Panda case, where they had, you know, compromised this data from previous intrusions, and then been able to sift through, find journalists, dissidents, you know, and do follow-on targeting with that.

And I believe that probably the greatest danger is actually that they're, I believe, actively starting to do this for political appointees within the U.S. and other governments. So I think that probably one of the key dangers is that they are probably doing this on, you know, the folks in this room.

We've seen, you know, quite a few spear phishes against folks on LinkedIn within the China researcher space. And I believe that that's also going to start picking up against U.S. political appointees as well. And that is the real danger, is that they can use that big data to do that follow-on targeting.

COMMISSIONER SHRIVER: Thank you. Another question, maybe for Ms. Vanderlee. As I -- sort of survey what other countries are doing related to protection on data, you see some that are more aggressive in banning Chinese apps. I mean, India comes to mind, pretty aggressive banning of Chinese apps, TikTok and others and now looking at e-sports and the like.

Is this a vulnerability that we are not sufficiently attuned to? I mean, we've taken some measures, but mostly within government and within, you know, particular agencies banning these apps and websites, but really not as broadly as some other countries. Is this something we should be considering more?

MS. VANDERLEE: That is a complex problem because on the one hand, any software, whether Chinese in origin or not as we learned via software supply chain compromise operations that I discussed, any software is one update away from being a backdoor.

Is there increased risk potentially with Chinese software where the company has to answer to the Chinese Government in a situation where there's a priority collection? Sure.

We've also noted, in my written testimony I describe an open source report of U.S. Government disclosures around suspicions of potential hardware coming from telecommunications companies in China that may have included malicious components. So there's certainly risk.

But you cannot, like, stop using all technology because of this. You have to balance your equities and figure out how to make the best decision with what you have.

COMMISSIONER BARTHOLOMEW: All right, thank you. Vice Chairman Glas.

VICE CHAIR GLAS: Many thanks to you all. This is not a topic that I've had a lot of experience in, so appreciate your in-depth knowledge here.

You know, I have a question, and maybe it seems a little basic, but how have some of the advances in quantum computing helped with the cyber espionage activities of China, in China, perpetrated against United States or others around the world?

And as we're thinking about our recommendations to Congress in this area, what do you think is one of your most important recommendations to address maybe disparities in technological advances? I've heard a lot of different kinds of recommendations today, I'm trying to hone in on what are the highest priorities.

And I'll start with Ms. Vanderlee.

MS. VANDERLEE: Sure. So quantum. My understanding of the benefit of quantum computing is more on the defensive side because you can guarantee secure communications via quantum technology, and China has tested this capability out. Although I believe that it is still at least somewhat experimental.

There's also the data processing advantage. Once the quantum systems are up and running reliably, they could be used to break encryption on previously stolen data that has just been sitting on servers waiting -- waiting for the capability to crack in and see what's there.

So that's what I have to say on quantum. I think others may have additional perspective. In terms of how to prioritize recommendations, I think that it may feel like silly or simple to be harping on incident reporting and defense and resiliency measures, but these can be effective, not only in the case of Chinese cyber espionage, but also in the fight against ransomware.

I think moving in that direction is going to help U.S. public and private sector be better about understanding what is the shape of the problem and how do we respond to it. I really think that that is important.

And I think that if our partners and allies were able to turn around a coordinated response after proxy log-on within three months, then maybe it's not such a pie-in-the-sky idea that we could be working better in terms of public messaging with our partners and allies. And I'll let the other folks weigh in as well.

VICE CHAIR GLAS: Yeah, Mr. Kozy or Mr. Cary?

MR. KOZY: Sure, just a brief note on quantum. I think that -- I'm by no means an expert, but I do think the difficulty with quantum is going to be the fact that due to how quantum functions, there will be a lot of extra noise.

Basically, if you have some sort of an entanglement with the quantum messaging, there's kind of no way to rebuild it. And I could see that being kind of a problem where you have almost DDoS capabilities with dynamite.

So but I do believe that it's still an important race to win for the capabilities that Kelli discussed about computing technology and being able to crack other encryption.

Regarding recommendations, mine are, you know, divided into hardened defense, active defense and offense and education, which I think all three of those are critical to curbing this behavior. Hardened defense I think has been discussed at length within the government and there are a lot of really good solutions that have come out of it.

On the offensive side, I would just say, again, imposing meaningful consequences, because that's the only way that China's going to respond to this.

And on the education side, I think opening up, you know, alternate bug bounty programs, because China has been kind of cordoned off into its own silo at this point, to bring some of these Chinese researchers back to the table.

Because for them, it is less about patriotic fervor and more about bending technology to their will and sharing knowledge. So we need to open some of those doors back up.

VICE CHAIR GLAS: Thank you, Mr. Kozy. You only have a few more seconds.

MR. CARY: Thank you. I would just say that the research that I've come across on quantum, one university stands out: the BUAA, which is the Beijing University of Aeronautics. They have a PhD program that is certified as a world-class cyber security school by the Chinese Government. And part of their PhD program that is certified is working on quantum computing.

And as for the recommendations, I would foot-stomp that education is incredibly important, because U.S. education is directly tied to our capabilities and our ability to respond.

COMMISSIONER BARTHOLOMEW: Great, thank you all. Commissioner Friedberg.

COMMISSIONER FRIEDBERG: Thank you very much and thanks to all of our witnesses.

I have a question about the use of cyber for political influence operations. My understanding that in contrast to the Russians, the Chinese that been thus far relatively cautious about engaging in this kind of activity with the partial exception of Taiwan. And I think I direct this question to Mr. Vanderlee.

You mentioned in passing that in 2018, there was evidence that China had engaged in cyber operations that were intended to influence an election in Cambodia. I wonder if you can say more about that. And you also mentioned in passing their possible interest in the use of artificial intelligence to hone and improve cyber political influence operations. And I would be interested in hearing more about that as well.

MS. VANDERLEE: Okay. So the campaign that Mandiant wrote on describing threat activity around the elections in Cambodia and I want to say it was 2018, were not influence operations per se. There was effort to collect intelligence about polling and voting software and voting practices and results.

We believe that they were trying to monitor what was going on, what were the opinions being shared and basically what was going to be the status of Chinese BRI investments in the country.

However, we do see Chinese information operations expanding into dozens of languages, including a recently released report where we described Chinese influence operations that we believe were mimicking Russian tactics to stage real lifee protests in the United States, to induce U.S. individuals to participate in narratives that China was trying to promote and engage physically in political activity in the United States.

We see -- we also see extensive use of deep fake technology specifically for creation of the profile images so that they can create credible looking accounts and then propagate them and use many accounts across many platforms to create a false identity and then use that and a network of additional identities to share and promote the ideas that they're talking about.

And so in terms of activity that has affected the United States, there's been a little bit of commentary, for example, in the last election, but there has been a great deal of content shared criticizing U.S. responses to coronavirus and accusations about, you know, the true origin of the coronavirus not being China and the U.S. is spreading lies and these kinds of ideas.

COMMISSIONER FRIEDBERG: Thank you. Can you or any of the other witnesses comment on information regarding possible operations by China intended to influence political outcomes on Taiwan?

Again, my impression based on casual reading is that Taiwan may be something of a laboratory in which China is experimenting with techniques which might appear in other democracies in the future.

DR. KOZY: I can comment on that. And I would definitely say that yes, Taiwan, has consistently been kind of a research lab for a lot of cyber capabilities in general. And I do believe that although we've definitely seen it in the U.S., that Taiwan is probably where we will see the most political influence operations in the next couple of years because it is very much one of China's top priorities.

I would just back up a second and say that the comparison to Russia running disinformation campaigns, Russia has been operating disinformation campaigns on kind of a human basis for many decades at this point. I believe that China will perfect that via technology because they are able to ingest this data. They are doing work on deep fake technology and they are very calculated in their approach whereas Russia has typically been a little bit messier and these operations have been exposed. I do believe that China will take that to the next level and that is of grave concern to not just the U.S., but all of our allies.

COMMISSIONER FRIEDBERG: Thank you.

COMMISSIONER BARTHOLOMEW: All right, Commissioner Fiedler.

COMMISSIONER FIEDLER: I have two questions. One is a technical question that I'm curious about. How difficult would it be to disrupt on a sustained basis the Chinese Great Firewall?

Anybody?

MR. KOZY: I would just say fairly difficult, that this is essentially taking down China's backbone networks because how the Great Firewall functions as part of an earlier Golden Shield project, is very much tied to how the CCP is able to control and restrict and sometimes release information. So that involves really some very heavy technical consequences that would be noticed, I would say, and be very loud.

Not to say that it's not possible. I think very recently there was a case of a single security researcher going by PAX, taking down North Korea's internet pretty much single handedly which is pretty interesting when you think about it. So the capability exists. It just depends on really how much noise we would like to make and knock on consequences that that would entail.

COMMISSIONER BARTHOLOMEW: Jeff, you're muted.

COMMISSIONER FIEDLER: Sorry, I'm supposed to mute myself when there's talking.

The second question is what knowledge do we have about Chinese attacks or espionage against our military-related artificial intelligence production companies, contractors?

MR. CARY: I'm not aware of any intrusions targeting these systems. I'm probably the person who can talk about it most at the table and I would say that it's likely that those are targeted systems, that they would like to collect those systems, and that upon collection, they would review them and see what's valuable and not valuable and keep what they would like. I'm not aware of any disclosed circumstances where that has occurred.

MR. KOZY: Yes, I would just add that that is a very high-tier target for the Chinese, however, there is very little proof at this point that they are -- yes, in the open source, I would say that they are actively going after this type of information, but I would say it's expected.

COMMISSIONER BARTHOLOMEW: Jeff, unmute.

COMMISSIONER FIEDLER: I did. My mute button doesn't -- and it gives me on the screen.

So we had a high-value target in the United States that we don't know in an open-source, but I guess in a classified context we might.

The MSS subsidiaries, MSS uses commercial companies like every other, whether it’s the Ministry of Public Security or what not. What do we know about their commercial fronts or their commercial retail companies?

MR. KOZY: Sure. So this is its use of the contractor model to carry out many of these operations. Most of the time this is kind of an informal relationship. I would say that they are monetarily compensated, but the MSS likes to keep things relatively fluid for plausible deniability and the ability to compartmentalize what specific entities are tasked with collecting.

This also enables them to cut things off, potentially, you know, rely on their MPS partners to make arrests if they feel like they need to trot out some victims or some blame at this point. However, yes, the CNITSEC, I would say, keeps a very long list of contractors. Many of these are prominent cyber -- Chinese cybersecurity companies that folks here are probably very familiar with, Qihoo 360, NSFOCUS, even via some of the conferences, the cybersecurity conferences that are taking place domestically are fertile recruiting grounds where they can meet some of these contractors, recruit from universities, as my colleague, Dakota, talked about, and kind of interface with these hackers.

COMMISSIONER BARTHOLOMEW: All right, Commissioner Cleveland.

COMMISSIONER CLEVELAND: I'd like to build on what Jeff just raised and Mr. Cary, you said in your written testimony that big tech is tasked to help the security services to process large swaths of data. And you note that the three interesting issues which it may be that the security services themselves are not capable of dealing with requests from policymakers, and so they task these companies to take these responsibilities on or the security services can attract the talent or that they see the private sector challenges acceptable to carry out these tasks or duties.

I'd like, if you could, to elaborate on your thinking on the relationship between the private sector and particular companies like Alibaba.

I'd like, as a second part of that, for you to address what you see as the highest priority activities of these non-state actors. Are they identifying vulnerabilities? Are they exploiting, acquiring? Are they processing the data? What are the priority tasks being assigned by the security services?

And then, if you could elaborate on what Mr. Kozy said about who are the entitles that fall into the top five? Are they focused in the cyber space, as he suggested, or are they more familiar companies like Alibaba and Huawei?

MR. CARY: Yes, absolutely. So on the topic of big tech and data processing, there are a number of large companies that were known with, BAT, Baidu, Alibaba, Tencent are the go-to for large data cloud computing processing, so we know this from reporting from Zach Dorfman, who covered the relationship between these large companies and processing data for the MSS.

As I pointed out in my written testimony, there are three explanations that stick out to me as what's possible. It's either that the security services want their people to focus their time elsewhere and so they've asked these large companies to do that.

They have chosen or are not able to compensate their employees at a high enough level to attract talent that is currently at private companies and so not being able to retain that talent, they choose to just make use of it anyway because they can under Chinese law.

As it relates to Alibaba specifically, I think I'd like to highlight the most recent high-profile vulnerability which was the Log4 vulnerability or Log4j. This is an incident in which a researcher at Alibaba reported a software vulnerability apparently to Apache before reporting it to the Chinese Government as required by a new law implemented last year. And in so doing, incurred the wrath of the government. So although it's on the books that the companies are supposed to disclose software vulnerabilities first to the government, that's not always the case.

As it relates to the actual priorities, I think there's a significant differentiation and lines to be drawn between large tech companies like Baidu, Alibaba, and Tencent, Aand then smaller companies that are specifically focused on cybersecurity, Beijing Topsec, Eversec, NSFOCUS, Qihoo 360. There are a number of cybersecurity-focused companies that specifically focus on talent cultivation on one end. So at the National Cybersecurity Center in Wuhan, there are a number of private firms who help train students at a national cybersecurity school. They operate offense-defense labs. They operate cyber ranges, all on contract for the government and in order to facilitate the development of offensive and defensive capabilities, cyber research, and talent pipeline development.

And so I would differentiate these two and say cybersecurity companies that work with the government, which is most of them, are very good at doing cybersecurity-focused and large companies who kind of begrudgingly engage with the government on these particular tasks are the larger companies that we're familiar with.

COMMISSIONER CLEVELAND: Of the companies that you identified, how many of them raise capital on U.S. markets?

MR. CARY: I'm aware that Eversec raised private equity in the United States. Eversec provides data services at the National Cybersecurity Center in Wuhan. I am unaware or I'm personally unfamiliar with the raising of funds by the other three large companies, though I do know most of those are publicly listed, and so if you'd like to bucket them as raising capital in the United States, we definitely can. But I would differentiate their activities between those large firms and the cybersecurity firms.

COMMISSIONER CLEVELAND: And could you just elaborate a little bit more when you said that begrudgingly provides these capabilities? These capabilities being what? Data crunching?

MR. CARY: From what we know publicly, thanks to reporting by Zach Dorfman, he articulates that data processing on the back end on hacking campaigns, so after data is stolen, that these companies have provided these services. His reporting has not indicated to my recollection any other relationship than these one-off requests, although his reporting may indicate otherwise.

COMMISSIONER CLEVELAND: Thank you.

COMMISSIONER BARTHOLOMEW: Alright. Commissioner Borochoff.

COMMISSIONER BOROCHOFF: Thank you. I just want to say first off that I am not an expert on what you all do, but I'm very, very, very comforted by the fact that someone is doing a deep dive into what's actually happening on the ground technologically over there and I'm less comforted that no one is paying attention in the general sense yet.

Mr. Cary, in your written testimony that I read, you were asked a little bit about cooperation between universities overseas and here and you, you raised the valid point that we don't want to cut off our nose in spite of our other needs by just not accepting good employees and smart people.

I'm curious, is there any -- do you have any knowledge of whether the Confucius Institutes are involved with the organizations that are working as sister universities cooperating with each other?

MR. CARY: I don't recall any specific instances and I'd ask my co-panelists to perhaps fill in the gaps on my knowledge on that, although I am aware that there are organizations within China, the United Front Work Department specifically, who do help facilitate those types of operations.

COMMISSIONER BOROCHOFF: I thought that might not be the area all of you work in, but I'd love to hear from the rest of you if you have a comment.

MR. KOZY: Sure. I would just say that they, in my opinion, are separate, but related. The Confucius Institutes do have espionage components that are tied to the various intelligence services. However, they have kind of a separate mission, I would say, and many of the universities that Dakota highlighted have those cyber space specialties and again, very specific equipment to conduct, often to attack and defense labs and cyber ranges. And those are pretty -- they stand out pretty much.

COMMISSIONER BOROCHOFF: Thank you.

COMMISSIONER BARTHOLOMEW: Bob, anything else?

COMMISSIONER BOROCHOFF: That's it for me. Thanks.

COMMISSIONER BARTHOLOMEW: Great. Thanks. All right, my turn.

Are there any constraints on Chinese cyber espionage activities? Are there any red lines that we know of that they wouldn't cross?

Ms. Vanderlee, do you want to start?

MS. VANDERLEE: Sure. I think that we have not yet observed, to my knowledge, Chinese cyber threat activity conducting destructive operations within the United States. And the disruptive operations that have affected North America and Europe today have been quite limited in scale.

We have seen indications of some operations in Taiwan that would be concerning, but in terms of using cyber capabilities to collect political and military intelligence, commercial IP, we're seeing these kinds of operations on a fairly regular basis.

So I think that the red line of war versus not war associated with a large destructive operation including potential ransomware or destructive malware disguised as ransomware that affects civilian populations is something that is not likely to happen outside of the context of an armed conflict.

COMMISSIONER BARTHOLOMEW: Thank you. Mr. Cary or Mr. Kozy, anything to add?

MR. CARY: Yes, I think that the only thing that I would add is that there have been no indication that hacking operations have occurred with anything related to nuclear command and control. And without having access to classified information, I feel confident that that has not happened because it would be incredibly escalatory and I think that that is a red line that our nations probably won't ever cross.

COMMISSIONER BARTHOLOMEW: Mr. Kozy?

MR. KOZY: Yes, I would just add that I second Kelli's point about computer network attacks that there is less information readily available, but that probably those capabilities reside with the PLA and specifically the Strategic Support Force post re-org, less so with the MSS.

However, I would point to the Wicked Panda APT41 case as a prime example of kind of tacit approval. These actors were seen deploying ransomware and cryptojacking occasionally which did affect actual civilian victims. So it appears that that red line has not really been firmly established within China in my opinion.

COMMISSIONER BARTHOLOMEW: It's been said to me it's an important issue when we talk about norms and trying to establish some sort of norms, but switching gears, it would seem to me that the CCP has the ability to leverage hackers, Chinese hackers, to get them to cooperate and do work for them in a way that we just don't. I'm thinking about that particularly because, Mr. Kozy, I think it was you who mentioned that one of the people had been put in jail. We see what they're doing to try to silence people outside of China by affecting their families inside. So again, are there any limits or constraints on what the Chinese Government can do to harness all of the talents that it's got inside China to participate in these activities?

MR. KOZY: I would say I don't necessarily see any limits and I would point back to my written testimony and verbal testimony, talking about how yes, that the PLA showed early aptitude at finding some of these talented hackers and the MSS quickly followed on by cultivating essentially these ecosystems within the cybersecurity community, domestic to China, as well as universities as Dakota talked about.

And then yes, because of China's kind of authoritarian capabilities, they are able to pressure, in this case, even a security researcher who considers himself white hat or researching for purely security abilities, they are able to pressure those folks to work for the state which is extremely different from how we handle things here in the U.S. And again, I think as some of my co-panelists have discussed, puts us in some ways at a disadvantage, although I'm not advocating that we force anyone into these positions. However, developing the talent pipeline can go a long ways towards at least helping us catch up.

COMMISSIONER BARTHOLOMEW: Great. Thank you.

We have a few minutes left if anybody has a second round of questions?

Jeff? Mike, sorry.

COMMISSIONER WESSEL: Thank you, Madam Chair, and --

COMMISSIONER WONG: We also have Derek, just FYI.

COMMISSIONER WESSEL: We refrain from asking questions about parkour which seems to me to be a great event opportunity for you. Let me ask after Commissioner Bartholomew's questions, we saw the Aurora event years ago here in the U.S. We saw the Germans' steel mill taken over by hackers. I'm not sure that was fully attributed. We know about Stuxnet, et cetera.

Do each of the witnesses have any question about Chinese capabilities in the destructive use of the cyber domain in a Taiwan or another scenario?

Mr. Kozy, do you want to start?

MR. KOZY: Sure. I would just say that yes, there's less known about those destructive capabilities. However, I think it's very safe to assume that they've developed those. They've watched what North Korea and Iran is doing with destructive attacks. And I believe that if they were to undertake any of those that it would be fairly surgical and that both the MSS could be involved in kind of setting up some of these targets in a war-time scenario, but that the SSF specifically is now focused on being able to compromise targets and then internally be able to assess whether it's better for espionage purposes or later attack purposes.

COMMISSIONER WESSEL: But the level of their current capability is another domain so their vectors wouldn't give you question about their capabilities in this area, just that we have not seen public evidence. Is that right?

MR. KOZY: Correct, yes. I think there's no question that they possess those capabilities. It is not technically out of their reach.

MR. CARY: If I may, I would add that there are research facilities in China called cyber ranges that are specifically being built to mirror physical facilities and in some cases use that same physical equipment to practice attacks and that these facilities are connected to both the MSS and PLA. So I would foot stomp that we have not seen these attacks occur publicly yet, but I can say with confidence that there are facilities to practice such operations.

COMMISSIONER WESSEL: And in terms of those cyber ranges, are those military targets that they've mocked up? Are they civilian targets such as water treatment, et cetera? Do you have any knowledge there?

MR. CARY: I have data to show that there are ranges for industrial control systems that include simulating smart cities, so these would include electrical grid, water, you name it, that a civil government provides.

There's also indications that they have cyber ranges for satellites. These are not satellites currently in space, but satellites on the ground that can be used for training to attack and defend satellites which is obviously an important part of command and control during armed conflict.

COMMISSIONER WESSEL: Great. Ms. Vanderlee, anything to add there?

MS. VANDERLEE: Not a lot. I would echo my colleague that it is almost certain that they indeed do have these capabilities. In fact, if APT41 has indeed used ransomware, then that's all you need to conduct a destructive attack.

There was also a U.S. Government report that was disclosed within the last two years discussing, I think 2012 era activity where APT1 had gained access to ICS systems 10 years ago within the United States. So there has certainly been interest in this that would suggest for quite some time.

COMMISSIONER WESSEL: Thank you.

COMMISSIONER BARTHOLOMEW: Great. Thanks. I have two more people who are interested in asking a second round, Commissioner Friedberg and then Commissioner Scissors.

Commissioner Friedberg?

COMMISSIONER FRIEDBERG: Yes. I had a question for Mr. Cary. You make the point that cyber defense is a team sport, but the way you describe it, it doesn't seem like the Chinese side is playing by the same rules that, for example, they develop means so that they're not sharing exploits in the ways that they might have once and that they obviously are conducting offensive research. They're not sharing that either. So what actually do we get out of any kinds of exchanges with them or exchanges between universities on these topics?

You said U.S. may benefit more, but why? Why do you think so?

MR. CARY: Absolutely. So the U.S. benefits first because China is of the opinion that they can conduct offensive research at universities and that we won't pay attention. And we are paying attention and they continue to conduct such research. So we have an advantage by being able to understand their capabilities, development, and priorities.

I submitted an appendix late yesterday and I hope that it's been made available to you. If not, I'll make sure that you get it after I testify, but thanks to a large software bug supporting our reporting platform in the United States is this marketplace where security researchers find software vulnerabilities, submit them to the platform. The platform notifies the company and the company remits payment.

The United States has a number of companies on this platform. They've remitted $44 million in payments for software vulnerabilities in 2021 and 10 percent of that money went to security researchers in China who found software vulnerabilities, reported them to U.S. firms, and helped secure those products. The other 85 percent outside of the United States, 15 percent, were from U.S. researchers. Eighty-five percent of software bugs reported through this platform to U.S. companies were from outside the United States. So it is in a lot of ways a very collaborative effort to conduct cybersecurity research and cyber defense research and it does benefit everyone when a cutting-edge technology becomes standard.

COMMISSIONER BARTHOLOMEW: All right, Commissioner Scissors.

COMMISSIONER SCISSORS: All right. Happily between us and lunch.

Mr. Cary, I’m going to throw in an analogy and you can tell me what's wrong with it. On occasion, the U.S. has thought of sanctions against Chinese entities that are doing what we consider to be illegal and harmful business with North Korea. Most of the time those sanctions are against glorified shell companies that have no value whatsoever. I wouldn't say all the time.

I'm not aware of everything, but there have definitely been times when we have said it's a bad Chinese actor. And it's just meaningless. It's a diplomatic statement with no economic content.

I'm going to draw the parallel to sanctioning APT groups instead of MSS. Are we just -- oh, we stamped out APT40 and now APT43 is doing exactly the same thing three months later. Is that a reasonable analogy that we can't -- that we need to go to the heart of the matter here with sanctions when we're serious and that attacking an individual group doesn't do any good or am I taking something from the economic realm and moving it into cyber that doesn't work?

MR. KOZY: Yes, I would basically just say that yes, it is a bit a hydra problem where they consistently are able to pop up and I think as some of my co-panelists discussed earlier, there were very little drop-in operations even when supposedly they had stopped in 2015. And I would even point to the Wicked Panda APT41 case. I have on some good authority that basically those actors were barely, after the indictment, and the FBI Wanted poster came out, there was barely a lapse of two weeks between when their next operation occurred. And I would guess, knowing Tan Dailin, that some of that was probably having some celebratory drinks for making an FBI Wanted poster, and I think that highlights the exact problem that we're facing.

COMMISSIONER SCISSORS: Thank you.

COMMISSIONER BARTHOLOMEW: All right, anybody else? We have four more minutes before we're scheduled to end. Does anybody have any other questions?

Robin?

COMMISSIONER CLEVELAND: Just to follow up on that $44 million in compensation, going to individuals in China. We assume that the Chinese Government is fully aware of those people who are assisting U.S. companies?

MR. CARY: Yes. So if I could clarify, the U.S. firms in one year paid out $44 million in total, 10 percent of which went to China which -- $4.4 million. The Chinese Government, at the end of last year, implemented a policy which requires software security researchers to disclose software vulnerabilities to the government first. They're supposed to disclose these software vulnerabilities within two days. That puts the government in a position to evaluate all software security vulnerabilities in China for operational value.

Whether or not those researchers choose to disclose to foreign firms is a choice. They often choose to do so because there is monetary compensation for doing so. But the Chinese Government has situated itself on top of the research pipeline, effectively weaponizing all software security research in China.

So despite the fact that these companies do receive these software vulnerabilities and researchers are paid for their work, the Chinese Government has put itself in a position to weaponize that research.

COMMISSIONER CLEVELAND: This is what happened with Apache, the case that you mentioned.

MR. CARY: Yes, and I would actually note that in Apache it seems that the researchers skipped the Chinese Government and that Alibaba incurred costs for that person's actions. We don't know about the motivation, whether or not it was on purpose or accidental. I think my co-panelist, Adam, would like to add to this.

MR. KOZY: Yes, just to piggyback off of that. I do think that that's one of kind of a joint recommendation that we share is creating those alternative pipelines for reporting and potentially creating almost kind of holding or delayed monetary compensation to make sure that the MSS and these other entities are not able to benefit immediately from those vulnerabilities, so some sort of escrow holding for bug bounties, but making it worth their while to wait and report it to U.S. firms could help stem some of this problem.

COMMISSIONER BARTHOLOMEW: All right. Thank you very much for interesting and alarming testimony here today. But it's one of those the more I learn, the more concerns that I get and I started with a pretty high level of concern.

We're going to break for lunch now. We will reconvene at 1:20. Thank you.

(Whereupon, the above-entitled matter went off the record at 12:20 p.m. and resumed at 1:20 p.m.)

PANEL III INTRODUCTION BY CHAIRMAN ALEX WONG

CHAIRMAN WONG: Good afternoon and welcome back. So, we are now starting our third panel today. In this panel we'll evaluate the implications of China's cyber activities for the United States and what our response is and should be.

First, we'll hear from Adam Segal with the Council of Foreign Relations. Next, we'll be hearing from Dr. Jacquelyn Schneider of the Hoover Institution and the Naval War College's Cyber and Innovation Policy Institute. And third, we'll be hearing from Dr. Neil Jenkins with the Cyber Threat Alliance.

We look forward to your testimony, and I think we will have ample time, hopefully, for Q&A. So, Dr. Segal.

OPENING STATEMENT OF STATEMENT OF ADAM SEGAL, IRA A. LIPMAN CHAIR IN EMERGING TECHNOLOGIES, DIRECTOR, DIGITAL & CYBER PROGRAM, COUNCIL ON FOREIGN RELATIONS

DR. SEGAL: Thank you. I want to thank the Commissioners for inviting me to speak today. I'm disappointed not to be there with you in person.

As you've heard from the earlier panels today, State-backed Chinese hackers are engaged in a range of cyber operations that threaten U.S. national security and economic interests.

The United States and China differ on the norms of responsible State behavior in cyberspace.

In particular, Washington and Beijing hold conflicting views on the applicability of international law to cyberspace, as well as the legitimacy of cyber-enabled industrial espionage.

For almost a decade, the United States has unsuccessfully tried to shape Chinese behavior with a combination of diplomatic dialogues, multilateral engagements, and attempts to impose costs more directly.

The strategy appeared to succeed briefly in 2015. That year, President Xi stood next to President Obama and declared that China would no longer support or tolerate cyber-enabled theft of international property for competitive advantages.

In that same year, Chinese representatives signed off on the Consensus Report produced by the Group of Government Experts at the United Nations, which accepted some common norms of State behavior, including the norm of State responsibility and the norm not to interfere with critical infrastructure during peace time.

2015 signaled a pause, however, not a conversion of U.S. and Chinese views. Beijing never embraced Washington's distinction between legitimate State operations, what the U.S. considers good spying, or political military espionage, and what it considers bad operations, or bad spying, cyber-enabled theft of intellectual property. And there is no reason to believe that it will do so in the future.

In fact, China may believe that it can and has reached a standoff of sorts, where the Ministry of State Security deploys a level of trade craft equivalent to the hacking conducted by the National Security Agency.

In the wake of the failure of the agreement, the U.S. ramped up attribution of indictments of Chinese State-backed hackers.

DOJ, for example, announced indictments in November 2017, in December 2018, in May 2019, in February 2020, in July 2020, in September 2020, and again in July 2021. Two of the indictments, December 2018 and July 2021, also involved joint attribution.

The United States was joined by Five Eye partners and others in calling out the Cloud Hopper operation, a sophisticated attack against service providers in Europe and the United States.

The attribution of the Microsoft Exchange Hack in July 2021 was joined by an even larger group, including Canada, the U.K., EU and, for the first time notably, NATO.

Still, attribution and indictments alone have not imposed significant costs on Chinese hackers.

The vast majority of Chinese hackers will never see the inside of a U.S. court. And while the joint attribution process may eventually serve as a basis for more efficient sanctions, now it is much more successful in signaling to like-minded countries, than it is to changing Beijing's behavior.

On discussing the rules of cyberwarfare, the United States remains engaged with China through the Group of Government Experts process and the Open-ended Working Group process in the U.N.

But here, the two sides remain divided by the process and the eventual outcome. China, like Russia, believes that cyberspace requires a new type of treaty: that the characteristics of cyber are so different from what came before, that we need a new binding agreement.

In the February 2020 joint statement during President Putin's visit to China this February, called, for example, for a universal international legal instrument regulating the activities of states in the field of information and communication technology.

The United States has consistently argued that a new treaty would be unworkable and unenforceable.

In addition, the U.S. efforts to discuss the applicability of international law in particular, the law of countermeasures and the inherent right of self-defense have met with opposition from China, Russia, Cuba and others, who argue that any further discussions of those topics are tantamount to militarizing cyberspace.

There should be little expectation that China will significantly change its views on these issues.

The United States should continue to engage China through the U.N. process, but the priority should be direct dialogues that bring cyber operators together.

Given the lack of shared understandings of both thresholds, escalation ladders, and signaling, there are legitimate concerns about spillover between a cyber event and a kinetic conflict.

There are also, I think, very serious concerns about cyberattacks on nuclear command and control systems.

The U.S. should insist that the PLA send cyber operators, not foreign affairs officers, like it has done in the past.

These dialogues should be designed to improve mutual understanding of each other's cyber operations and doctrine, and may involve confidence-building measures, such as greater information exchanges during cyber incidents, and identifying points of contact and communication during a cyber crisis.

The United States should also not expect Beijing to accept a norm against cyber-enabled industrial espionage, or to cease those operations.

While U.S. friends and allies will be more willing to call out Chinese industrial espionage in a joint attribution process, they will likely remain hesitant to sanction Beijing on those same issues, because of economic and other political interests.

To deal with cyber-enabled espionage, the United States should rely on persistent engagement and disruption, the imposition of costs on those who benefit from the theft, and improved defense.

The Administration should authorize Treasury Department to sanction companies and universities, researchers and individuals who benefit from cyberattacks designed to steal U.S.

intellectual property, and the Department of Commerce should also consider the barring of exports of U.S. technology to companies that benefit from cyberespionage.

U.S. Government should also help small companies increase their cyber defense against cyber hackers, and strengthen counterintelligence to identify sectors and companies under threat.

Small companies and startups and AI, quantum semiconductor and telecommunications and other sectors central to Chinese technology strategies are unlikely to be aware of the threat of Chinese actors, or have the resources or expertise to reduce vulnerabilities.

In the end, the United States must plan for China to remain a highly sophisticated actor in cyberspace, with increasing ambitions to project its influence on the norms of responsible State behavior, and a proven interest in United States' commercial secrets.

Thank you. And I look forward to your questions.

PREPARED STATEMENT OF ADAM SEGAL, IRA A. LIPMAN CHAIR IN EMERGING TECHNOLOGIES, DIRECTOR, DIGITAL & CYBER PROGRAM, COUNCIL ON FOREIGN RELATIONS

U.S. Responses to the China Cyber Challenge: Diplomatic Efforts to Establish Norms in Cyberspace

Prepared statement by

Adam Segal

Ira A. Lipman Chair in Emerging Technologies and National Security and Director, Digital and Cyberspace Policy Program
Council on Foreign Relations

Before the

U.S. China Economic Security Review Commission
February 17, 2022

Hearing on China's Cyber Capabilities: Warfare, Espionage, and Implications for the United States

The United States and China differ on the norms of responsible state behavior in cyberspace. In particular, Washington and Beijing hold conflicting views on the applicability of international law to cyberspace as well as the legitimacy of cyber-enabled industrial espionage. For almost a decade, the United States has unsuccessfully tried to shape Chinese behavior with a combination of diplomatic dialogue and attempts to impose costs more directly. The strategy appeared to succeed briefly in 2015, when President Xi stood next to President Obama and declared that China would not support cyber-enabled espionage, but today Chinese state-backed hackers continue to conduct operations that threaten U.S. economic security. In addition, while the two sides have both agreed to a shared set of norms of state behavior developed through a United Nations process, they remain sharply divided over how to move forward.

U.S. diplomatic efforts will continue to have little impact on Chinese behavior. Moving forward, the United States should look for more effective means to disrupt Chinese operators, impose costs on those who benefit from the theft of U.S. intellectual property, and improve U.S. cyber defenses. In addition, multilateral discussions need to be supplemented with a direct dialogue with Beijing on cyber doctrine and operations.

International Law and Cyber Conflict

The United States' position is that international law is applicable to cyberspace, and Washington believes that states should discuss how they understand their rights and obligations, including in regard to self-defense, use of force, non-interference, and armed conflict. The United States also holds that sovereignty is a principle of international law, and so there is no absolute prohibition on cyber operations that may touch on other's territory as a matter of international law. While violations would depend on circumstances, the United States appears to be referring to instances when "defending forward" activities in another state's territory have no effects or de minimize effects.

China agrees that international law is applicable in cyberspace, but has resisted concrete descriptions of state rights and responsibilities. In fact, Beijing has tended to characterize the call for greater explication of rights and responsibilities, especially jus ad bellum (the body of law that addresses uses of force triggering the use force in self-defense) and jus in bello (the body of law governing the conduct of hostilities), as leading to the "militarization of cyberspace." In an October 2021 prepared statement on China's position, for example, the Ministry of Foreign Affairs warned of the need to "handle the applicability of the law of armed conflicts and jus ad bellum with prudence, and prevent escalation of conflicts or turning cyberspace into a new battlefield."[1] Beijing has also tended to stress that sovereignty is a rule, and so would assert that cyber operations, even if they had limited effects, would be violations of sovereignty.

In addition, along with Moscow, Beijing has often suggested that the unique characteristics of cyberspace require a new international treaty. In September 2011, China and Russia, supported by Tajikistan and Uzbekistan, submitted a letter proposing a Draft International Code of Conduct for Information Security to the United Nations General Assembly.[2] The code supported a UN process in developing norms and rules for information, calling on states to agree that they will not "use information and communications technologies, including networks, to carry out hostile activities or acts of aggression, pose threats to international peace and security or proliferate information weapons or related technologies." The code was submitted to the UN again in 2015 by the Shanghai Cooperation Organization (SCO), the Eurasian regional organization that includes China, Russia, Kazakhstan, Kyrgyzstan, Tajikistan, and Uzbekistan.[3]

Norms and State Behavior

China has been a participant in the UN process to discuss the rules of the road for cyberspace, the Group of Government Experts (GGE) on Developments in the Field of Information and Telecommunications in the Context of International Security, since the first meeting in 2004. In June 2013, for the first time, the GGE, which included China, Russia, United States, and representatives from twelve other nations, issued a consensus report. The members of the group agreed that "international law, and in particular, the United Nations Charter applies to cyberspace."[4] After the report was issued, U.S. officials used the consensus to argue that by agreeing to the UN Charters, the signers were also accepting the Geneva Conventions and the applicability of the Laws of Armed Conflict to cyberspace. In contrast, Chinese official highlighted the GGE's embrace of state authority, non-interference, and equality, not the international law implications of accepting the UN Charter's application to cyberspace.[5]

The 2015 GGE group was tasked with examining "norms, rules or principles for responsible [behavior] of States" as well as "how international law applies to the use of information and communications technologies by States." Beijing, along with Moscow, signed off on four norms promoted by Washington in the 2015 report. Those norms included: norms of state responsibility and the duty to assist as well as that states should not intentionally damage or impair others' critical infrastructure or target another state's computer emergency response teams during peacetime. But China and Russia, along with Pakistan, Malaysia, and Belarus, opposed a US effort to include a reference to Article 51 of the U.N. Charter, which authorizes the use of force in self-defense against an "armed attack."

China and Russia also used the 2015 GGE to express concern about the increasing willingness of the United States to name and shame state-backed hackers. As it has called out Chinese, Iranian, Russia, and North Korean hackers, Washington has argued that attribution is not as difficult as once believed. When Chinese hackers have been publicly name, Chinese officials have often responded that such efforts are "unprofessional" and "unscientific." The 2015 report notes that while states must meet their obligations for internationally wrongful acts attributable to them, "indication that an ICT activity was launched or otherwise originates from the territory or the ICT infrastructure of a State may be insufficient in itself to attribute the activity to that State." Given this challenge, the report concludes that "accusations of organizing and implementing wrongful acts brought against States should be substantiated."[6]

In the run-up to the 2017 GGE meeting, U.S. officials warned that they hoped the group would not identify new norms but rather explain how states should adopt existing rules. State Department Deputy Coordinator for Cyber Issues Michele Markoff said, "We don't need a continual norms machine ramping out a lot of norms. What we need to do is consolidate what we've done and get states to implement."[7] The group, however, failed to issue a consensus report, and divisions over the question of the applicability of the law of countermeasures and the inherent right of self-defense proved especially contentious. The Cuban representative publicly opposed these measures, arguing that they would lead to a militarization of cyberspace that would "legitimize … unilateral punitive force actions."[8] This is a view shared by Russia and China, and they may have supported Cuba making it from behind the scenes.[9]

After the failure of the group to reach a consensus, the norms discussion split into two parallel processes. Russia proposed an Open-Ended Working Group (OEWG) to study the existing norms contained in the previous UN GGE reports, identify new norms, and study the possibility of "establishing regular institutional dialogue ... under the auspices of the United Nations." The United States entered a proposal to continue the work of the GGE, and both resolutions passed.

While many feared that the two processes would result in competing norms, the chairs of the two groups closely coordinated with each other. The OEWG's report reaffirmed the norms of the 2015 GGE report, but it did omit references to international humanitarian law, the laws designed to protect civilians during times of armed conflict. As with the 2017 GGE report, opposition to the incorporation of international humanitarian probably stems from the argument that its inclusion would normalize the militarization of cyberspace and legitimize cyber attacks.

China, along with Russia, will remain unwilling to discuss any further how international law applies in cyberspace, and instead will want to shift conversations to the need for a new treaty covering cyber norms. The joint statement issued by China and Russia during Putin's February 2022 visit, for example, stressed the "principles of the non-use of force, respect for national sovereignty and fundamental human rights and freedoms, and non-interference in the internal affairs of other States, as enshrined in the UN Charter, are applicable to the information space application of UN Charter and state sovereignty over information space." The two sides also called for consolidation of norms into a binding treaty: the two sides "consider it necessary to consolidate the efforts of the international community to develop new norms of responsible behavior of States, including legal ones, as well as a universal international legal instrument regulating the activities of States in the field of ICT."[10]

Bilateral Discussions

Outside of the UN process, Washington has tried to engage Beijing in bilateral discussion on cyber conflict. U.S. officials and analysts have long worried that, without shared understanding of thresholds, signaling, and escalation in cyberspace, a cyber incident could spur a kinetic conflict. Cyber issues were discussed at the Strategic and Economic Dialogue, which met eight times between 2009 and 2016. In addition, the two sides agreed to a cyber expert working group during the September 2015 summit between presidents Xi and Obama, but that group only met once in May 2016, led by the State Department and the Ministry of Foreign Affairs. President Xi and President Trump agreed to four dialogues, including the Law Enforcement and Cyber Strategic Dialogue and the Diplomatic and Security Dialogue. The latter reportedly met in June 2017 and discussed issues of stability and international standards; the former, led by the Department of Justice and the Department of Homeland Security, focused on intellectual property theft and crime.[11]

The pattern of these bilateral talks mirrors many of the challenges that affected military-to-military and strategic dialogues between the United States and China.[12] Bilateral cybersecurity discussions were clearly something Washington wanted more than Beijing. While the United States wanted to engage broadly with the People's Liberation Army (PLA), the talks were generally limited to diplomats through the Strategic and Economic Dialogue. The PLA representatives who attended these talks were from the foreign affairs office, not cyber operations. According to the *New York Times*, in 2014 the Pentagon briefed PLA officials on American doctrine on the use of offensive cyber operations in an effort to convince the Chinese that the United States was exercising restraint in cyberspace. The PLA did not reciprocate.[13] Moreover, China often treated the talks as a bargaining point, something to be offered or withdrawn depending on the state of the relationship. China, for example, cancelled a military dialogue on cyber issues to signal displeasure after the Department Justice indicted five alleged PLA hackers for cyberespionage in May 2014.

Given the difficulties of the official dialogues, there have also been a number of semi-formal channels. Starting in 2009, Center for Strategic and International Studies and China Institutes of Contemporary International Relations held at least nine Track 1.5 and 2 cybersecurity dialogues, attended by think tankers and academics, as well as U.S. and Chinese officials from State, Defense, DHS, FBI, and Ministry of Foreign Affairs, Ministry of Public Security, Cyberspace Administration of China, and PLA respectively.[14] These meetings usually included an update on national and international developments in cybersecurity, as well as broader discussions on issues such as norm, strategic stability and use of force.

The Norms of Cyber Espionage and the Bilateral Agreement

Washington's effort to establish a normative difference between espionage conducted for competitive advantage and espionage for national security purposes is its longest standing, highest profile effort with Beijing. In the United States' framing, cyber espionage for national security purposes is to be expected by all states and is fair game. Hacking private companies for commercial gain, on the other hand, is illegitimate. This leads to the somewhat incongruous scene of U.S. officials essentially tipping their hats to certain types of operations. When China, for example, was suspected of being behind the hack of the Office of Personnel Management, Director of National Intelligence James Clapper stated "you have to kind of salute the Chinese for what they did. If we had the opportunity to do that, I don't think we'd hesitate for a minute."[15]

In the face of a massive, multi-year cyber campaign conducted to steal U.S. intellectual property and business secrets—a campaign former director of the NSA and commander of Cyber Command General Keith Alexander once described as the "greatest transfer of wealth in history"—the United States at first hesitated to publicly call out or confront China. The hesitation derived from a fear that public attribution would reveal U.S. technical measures as well as an unwillingness to risk other, higher priority issues that required Beijing's cooperation, such as restarting the economy after the global recession and containing Iran's and North Korea's nuclear programs.

That calculus changed around 2013. In February, cybersecurity firm Mandiant released a report stating that Unit 61398 of the PLA was behind attacks on 115 companies in the United States, and around the same time, the Department of Homeland Security provided internet service providers with the internet addresses of hacking groups in China In a speech at the Asia Society in March, National Security Advisor Thomas Donilon warned of "cyber intrusions emanating from China on an unprecedented scale" risked destabilizing the bilateral relationship.[16] Months later, U.S. President Barack Obama confronted Chinese President Xi Jinping with the issue at the Sunnylands Summit. Then, in May 2014, in a significant escalation of public pressure, the Department of Justice indicted five People's Liberation Army officers for stealing trade secrets from Westinghouse, U.S. Steel, and other companies.[17]

In the summer of 2015, news reports suggested that the administration was ready to use Executive Order 13694, which authorizes sanctions against companies or individuals that profit from cyber theft, to sanction state-owned enterprises and senior Chinese officials associated with cyber theft.[18] These punishments would have overshadowed President Xi's first summit in Washington, and in response, Beijing dispatched Meng Jianzhu, one of the Chinese Communist Party's highest-ranking officials, to negotiate an agreement. In the agreement, which was announced by both presidents in the Rose Garden, China and the United States announced that neither would "conduct or knowingly support cyber-enabled theft of intellectual property, including trade secrets or other confidential business information, with the intent of providing competitive advantages to companies or commercial sectors."[19] In the months after the summit, China reached similar agreements with Australia, Canada, and the United Kingdom. Beijing also signed off on Group of Seven and Group of Twenty statements that proscribed cyber industrial espionage.[20]

Despite initial skepticism about the agreement's efficacy, cybersecurity companies recorded a steep decline in Chinese attacks against U.S. companies in the first year after it was concluded. FireEye released a report in June 2016 that showed that the number of network compromises by the China-based hacking groups they tracked dropped from sixty in February 2013 to less than ten by May 2016.[21] However, experts warned that the decrease in the number of publicly disclosed attacks might be the result of Chinese attackers becoming more stealth. The decline also appeared to predate the agreement, suggesting that internal forces, such as the consolidation of control over PLA cyber units through the creation of the Strategic Support Force (the PLA's space, cyber, and electronic warfare arm), was as much as a rationale as U.S. diplomatic pressure.

The norm against cyber economic espionage is not universally held. A number of close U.S. allies and partners engage in the practice. Moreover, Chinese officials never seem to have embraced the distinction, often calling the United States' denunciations of Chinese cyber operations as violating international norms as hypocritical, especially in the wake of the revelations of widespread U.S. espionage activities by Edward Snowden. By 2018, it was clear that Chinese cyber espionage had returned, with Chinese groups targeting companies operating in sectors that Beijing believes are important for future economic competitiveness, such as aerospace, semiconductors, and information technology.

The hiatus in Chinese cyber operations may have had two sources.[22] First, Beijing might never have intended to give up cyber espionage entirely but instead saw an opportunity to gain diplomatic advantage in implementing changes it already planned to make, shifting espionage from PLA hackers to more skilled operators in the Ministry of State Security (MSS). Although this would result in a temporary downturn in activity as hacking infrastructure was reoriented, its main purpose was to allow the PLA to focus on warfighting operations and reduce the number of incidents the United States could attribute to China. The agreement also prevented Xi's visit from being ruined or cancelled. In effect, Beijing always intended to continue commercial espionage—it just intended to stop getting caught.

Second, the return to industrial hacking might have been a reaction to the increased political and trade tensions between Washington and Beijing. With the Trump administration restricting Chinese investment in high-technology sectors, blocking Chinese telecommunication companies from doing business in the United States, levying tariffs against Chinese exporters, and blocking the sale of sensitive technology to Chinese firms, Chinese policymakers might have believed they had little to gain from continuing to honor the agreement.

Indictments and Joint Attribution

U.S. discussions with and pressure on China have been accompanied by public attribution and indictments of Chinese hackers. These include the indictment in 2014 of five PLA hackers for economic espionage; in November 2017 of three Chinese hackers who worked at the cybersecurity firm Boyusec for the theft of confidential business information; in December 2018 of two Chinese individuals for theft of intellectual property; in May 2019 for the hack on Anthem; in February 2020 of four military hackers for targeting Equifax; in July 2020 of two MSS hackers for targeting intellectual property, including COVID-19 research; in September 2020 of members of a Chinese hacking group known as APT 41; and in July 2021 of hackers associated with Hainan MSS.

The December 2018 indictment was part of the United States' effort to include friends and allies in public attribution of cyber-espionage operations. The campaign, known as Cloud Hopper, was a supply chain attack that targeted managed service providers like Hewlett Packard and IBM that provide cloud and other IT services to customers. The DOJ indicted two Chinese individuals, Zhu Hua and Zhang Shilong. According to the indictment, Zhu and Zhang were members of a hacking group operating in China known as Advanced Persistent Threat 10 (APT10). The defendants worked for Huaying Haitai Science and Technology Development Company and acted in association with the Ministry of State Security's Tianjin State Security Bureau.[23] Thirteen additional countries either joined the attribution or expressed concern about malicious cyber behavior. The five eyes joined in the attribution; Berlin and Tokyo issued statements approving of and supporting the attribution.

The European Union also participated, although slowly, and at first, indirectly. Almost five months after the U.S. attribution, in April 2019, Federica Mogherini, High Representative of the Union for Foreign Affairs and Security Policy, expressed concern about "the rise in malicious behavior in cyberspace that aim at undermining the EU's integrity, security and economic competitiveness, including increasing acts of cyber-enabled theft of intellectual property."[24] The statement did not name China. In November 2020, almost two years after the initial US attribution, the EU imposed travel restrictions on Zhang, and another individual, Gao Qiang, who it claimed was active in Cloud Hopper and was associated with APT 10 and Hauying Haitai.[25]

In July 2021, the United States attributed "with a high degree of confidence" the Microsoft Exchange Server attack to the MSS. The attack exploited a zero day vulnerability and appears initially to have targeted think tanks and other espionage targets. Moreover, knowing that Microsoft was pushing out a patch for the vulnerability, the Chinese scanned almost the entire internet to find exposed servers to be compromised. The White House called out China's "irresponsible behavior in cyber space" as being "inconsistent with its stated objective of being seen as a responsible leader in the world."[26] The statement also accused Beijing of using criminal groups as hacking proxies, and announced an indictment of four MSS hackers for a multi-year espionage campaign that spanned 2011 to 2018, separate from Microsoft Exchange hack. The Biden administration has not yet officially responded to the hacks, perhaps because it does appear to be an act of political espionage, not an attempt to steal intellectual property.

The White House also trumpeted that an "unprecedented" group of allies and partners joined the attribution of the Microsoft Exchange Server attack. The group included Canada, UK, EU, and, for the first time, NATO. Yet there was some difference on how directly partners were willing to assign responsibility to Chinese actors. NATO did not directly attribute to China, but rather acknowledged national statements by allies "attributing responsibility for the Microsoft Exchange Server compromise to the People's Republic of China."[27] The EU assessed that the activity had been "conducted from the territory of China for the purpose of intellectual property theft and espionage," rather than directly calling out the Ministry of State Security.[28]

The indictments and public attribution have not deterred or slowed Chinese operations. Proponents of the strategy argue, however, that the release of evidence in support of the indictments is a useful demonstration of U.S. attribution capabilities. They also may convince others to join attribution based on intelligence shared by the U.S. The goal eventually is to build a broader set of partners who are both prepared to call out malicious actions and act to punish China.

Persistent Engagement and Chinese Behavior

In 2018, the Pentagon adopted a cyber strategy that was more offense oriented. Describing a competitive environment in which Cyber Command would persistently engage with adversaries, the strategy states that U.S. operators "will disrupt or halt malicious cyber activity at its source, including activity that falls below the level of armed conflict." Most of the public information on how persistent engagement has been implemented has concerned disrupting Russian influence operations, but former National Security Advisor John Bolton suggested that Cyber Command was also launching operations against Chinese hackers.

Persistent engagement has two expected paths to change Chinese behavior. First, and most directly, defending forward and disrupting operations should impost costs on Chinese hackers. As Chinese hacking groups find it harder to operate, the total number of attacks should go down. Second, over time, persistent engagement is expected to create shared understandings of acceptable cyber behavior. Tit-for-tat, action-reaction cycles will eventually make clear to both sides what the other sees as legitimate actions in cyberspace.

What is Next?

Moving forward, it is clear that the United States shares with its friends and allies a similar perception of the Chinese threat in cyberspace. The 2021 report from the National Cyber Security Centre, for example, states that "China remained a highly sophisticated actor in cyberspace with increasing ambition to project its influence beyond its borders and a proven interest in the UK's commercial secrets. How China evolves in the next decade will probably be the single biggest driver of the UK's future cyber security." In addition, for the first time, the 2021 Brussels Communique framed Chinese actions as a challenge to NATO's security interests, with the alliance calling out "cyber, hybrid, and other asymmetric threats, including disinformation campaigns, and by the malicious use of ever-more sophisticated emerging and disruptive technologies."[29]

While U.S. friends and allies will be more willing to call out Chinese industrial espionage, they are likely to remain hesitant to sanction Beijing on cyber issues. The coordination of attribution among states with different methods and procedures is difficult, though in the wake of the SolarWinds hack, the White House announced that it was providing training on the policy and technical aspects of publicly attributing cyber incidents.[30] Moreover, high economic interdependence with China, fear of retaliation, and a desire to make progress on higher priority issues all combine to make it difficult for countries to follow through with sanctions.

The United States should not expect Beijing to accept the norm against cyber-enabled industrial espionage. Joint attribution and indictments do little to impose costs on Chinese hackers, though they help in binding allies and partners together in shared norms and in preparing the ground eventually for collective action. To deal with cyber-enabled industrial espionage, the United States should rely on persistent engagement and disruption, the imposition of costs on those who benefit from the theft, and improved defense. The administration should authorize the Treasury Department to sanction companies, universities, researchers, and individuals who benefit from cyberattacks designed to steal U.S. intellectual property. The Department of Commerce could also bar the exports of U.S. technology to companies that benefit from cyber espionage.

The U.S. government should help small companies increase their cyber defenses against Chinese hackers and strengthen counterintelligence to identify sectors and companies under threat. Small companies and start-ups in AI, quantum, semiconductor, telecommunications, and other sectors central to Chinese technology strategies are unlikely to be aware of the threat of Chinese actors or have the resources and expertise to reduce vulnerabilities.[31]

Washington should be similarly clear eyed about the multilateral norms process and international security. In the near term, Beijing is unlikely to drop its long held position that cyberspace requires a new treaty or abandon its resistance to explicating the application of international law to cyberspace. As with joint attribution, the GGE and OEWG processes are more successful in defining acceptable behavior among allies and partners than constraining malicious actions by potential adversaries.

The United States should continue to engage China through the UN process, but the priority should be direct dialogues that bring cyber operators together.[32] These dialogues should be designed to improve mutual understanding of each other's cyber operations and doctrine, and may involve confidence-building measures such as greater information exchanges during cyber incidents and identifying points of contact for communication during a cyber crisis.

[1] Available at National position of the People's Republic of China (2021), https://cyberlaw.ccdcoe.org/wiki/National_position_of_the_People%27s_Republic_of_China_(2021)
[2] https://www.rusemb.org.uk/policycontact/49%20

[3]U.N. General Assembly, "Letter dated 9 January 2015 from the Permanent Representatives of China, Kazakhstan, Kyrgyzstan, the Russian Federation, Tajikistan and Uzbekistan to the United Nations addressed to the Secretary-General," U.N. Doc. A/69/273 (2015), http://www.un.org/Docs/journal/asp/ws.asp?m=A/69/723.

[4] https://undocs.org/A/68/98

[5] Adam Segal, *Chinese Cyber Diplomacy In A New Era Of Uncertainty*, Hoover Institution, June 2, 2017, https://www.hoover.org/research/chinese-cyber-diplomacy-new-era-uncertainty

[6] https://undocs.org/A/70/174

[7] Joseph Marks, "The US Does An About-Face on New Cyber Norms," *DefenseOne*, February 7, 2017, https://www.defenseone.com/technology/2017/02/us-does-about-face-new-cyber-norms/135227/

[8] https://www.justsecurity.org/wp-content/uploads/2017/06/Cuban-Expert-Declaration.pdf

[9] Elaine Korak," UN GGE on Cybersecurity: The End of an Era?" *The Diplomat*

[10] Joint Statement of the Russian Federation and the People's Republic of China on the International Relations Entering a New Era and the Global Sustainable Development, February 4, 2022, http://en.kremlin.ru/supplement/5770?s=08

[11] Secretary of State Rex Tillerson and Secretary of Defense Jim Mattis at a Joint Press Availability (U.S. State Department, June 21, 2017) (www.state.gov/secretary/remarks/2017/06/272103.htm); "First U.S.-China Law Enforcement and Cybersecurity Dialogue: Summary of Outcomes, Department of Justice," October 6, 2018 (www.justice.gov/opa/pr/first-us-china-law-enforcement-and-cybersecurity-dialogue).

[12] Kurt Campbell and Richard Weitz, "The Limits of U.S.-China Military Cooperation: Lessons from 1995–1999," *Washington Quarterly*, Winter 2005-2006.

[13] David E. Sanger, "U.S. Tries Candor to Assure China on Cyberattacks," *New York Times*, April 6, 2014, https://www.nytimes.com/2014/04/07/world/us-tries-candor-to-assure-china-on-cyberattacks.html?_r=0.

[14] https://www.csis.org/programs/strategic-technologies-program/cybersecurity-and-governance/other-projects-cybersecurity-3

[15] Julianne Pepitone, "China is 'Leading Suspect in OPM Hacks, Says Intelligence Chief James Clapper," *NBC News*, June 25, 2015, https://www.nbcnews.com/tech/security/clapper-china-leading-suspect-opm-hack-n381881

[16] "The United States and Asia-Pacific in 2013," Complete Transcript: Thomas Donilon at Asia Society New York, March 11, 2013, https://asiasociety.org/new-york/complete-transcript-thomas-donilon-asia-society-new-york

[17] Mark Clayton, "US indicts five in China's secret 'Unit 61398' for cyber-spying on US firms," *Christian Science Monitor*, May 19, 2014, https://www.csmonitor.com/World/Passcode/2014/0519/US-indicts-five-in-China-s-secret-Unit-61398-for-cyber-spying-on-US-firms

[18]White House, Blocking the Property of Certain Persons Engaging in Significant Malicious Cyber-Enabled Activities, April 1, 2015, https://home.treasury.gov/system/files/126/cyber_eo.pdf

[19] https://obamawhitehouse.archives.gov/the-press-office/2015/09/25/fact-sheet-president-xi-jinpings-state-visit-united-states

[20] Cody Poplin, "Cyber Sections of the Latest G20 Leaders' Communiqué," *Lawfare*, November 17, 2015, https://www.lawfareblog.com/cyber-sections-latest-g20-leaders-communiqu%C3%A9

[21] Mandiant, *Red Line Drawn: China recalculates its use of cyber espionage*, https://www.mandiant.com/resources/red-line-drawn-china-recalculates-its-use-of-cyber-espionage

[22] Next two paragraphs come from Lorand Laskai and Adam Segal, "A New Old Threat: Countering the Return of Chinese Cyber Industrial Espionage," Council on Foreign Relations, December 6, 2018, https://www.cfr.org/report/threat-chinese-espionage

[23]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, December 20, 2018, https://www.justice.gov/opa/pr/two-chinese-hackers-associated-ministry-state-security-charged-global-computer-intrusion

[24] Council of the European Union, "Declaration by the High Representative on behalf of the EU on respect for the rules-based order in cyberspace", press release, Brussels, 12 April 2019, https://www.consilium.europa.eu/en/press/press-releases/2019/04/12/declaration-by-the-high-representative-on-behalf-of-the-eu-on-respect-for-the-rules-based-order-in-cyberspace/

[25] Council of the European Union, "Council Implement-ing Regulation (EU) 2020/1744 of 20 November 2020 Imple-menting Regulation (EU) 2019/796 concerning restrictive measures against cyber-attacks threatening the Union or its Member States", Official Journal of the European Union, no. L 393/1 (23 November 2020), https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=uriserv%3AOJ.L%5F.2020.393.01.0001. 01.ENG&toc=OJ%3AL%3A2020%3A393%3ATOC

[26] The White House, The United States, Joined by Allies and Partners, Attributes Malicious Cyber Activity and Irresponsible State Behavior to the People's Republic of China, July 19, 2021, https://www.whitehouse.gov/briefing-room/statements-releases/2021/07/19/the-united-states-joined-by-allies-and-partners-attributes-malicious-cyber-activity-and-irresponsible-state-behavior-to-the-peoples-republic-of-china/

[27] Statement by the North Atlantic Council in solidarity with those affected by recent malicious cyber activities including the Microsoft Exchange Server compromise, July 19, 2021, https://www.nato.int/cps/en/natohq/news_185863.htm

[28] Council of the EU, China: Declaration by the High Representative on behalf of the European Union urging Chinese authorities to take action against malicious cyber activities undertaken from its territory, July 19, 2021,

https://www.consilium.europa.eu/en/press/press-releases/2021/07/19/declaration-by-the-high-representative-on-behalf-of-the-eu-urging-china-to-take-action-against-malicious-cyber-activities-undertaken-from-its-territory/

[29] Bussels Summit Communique, June 14, 2021, https://www.nato.int/cps/en/natohq/news_185000.htm

[30] White House, Fact Sheet: Imposing Costs for Harmful Foreign Activities by the Russian Government, April 15, 2021, https://www.whitehouse.gov/briefing-room/statements-releases/2021/04/15/fact-sheet-imposing-costs-for-harmful-foreign-activities-by-the-russian-government/

[31] Laskai and Segal, New Old Threat

[32] Adam Segal, "Strategic Stability in Cyberspace," in *Enhancing U.S.-China Strategic Stability in an Era of Strategic Competition*, United States Institue of Peace, April 26, 2021, https://www.usip.org/sites/default/files/2021-04/pw_172-enhancing_us-china_strategic_stability_in_an_era_of_strategic_competition_us_and_chinese_perspectives.pdf

OPENING STATEMENT OF JACQUELYN SCHNEIDER, HOOVER FELLOW, HOOVER INSTITUTION, STANFORD UNIVERSITY

CHAIRMAN WONG: Thank you, Dr. Segal. Dr. Schneider. Dr. Schneider, I apologize. Your microphone, please.

DR. SCHNEIDER: Is it working now? See, it's my first time back in like real life. So, you have to excuse me. I was ready for my Zoom, but I was off mute on Zoom, you know? There we go.

Okay, so thank you for inviting me today. I've been asked to talk about U.S. military cyber strategy and capabilities, and to give my assessment about our force posture to combat the Chinese cyber threat.

I want to make it clear that I'm here in my civilian capacity as a Hoover Fellow at the Hoover Institution, and do not speak on behalf of the U.S. Government or the Department of Defense.

Additionally, all my assessments come from public and unclassified documents. And therefore, I want to caveat that there may be U.S. military capabilities and operations that are not open source, and therefore are not within the realm of my analysis.

So, today I'm going to give an overview of the evolution of the Department of Defense cyber strategy.

I'll outline continuities and changes within these strategies, and then detail more concretely how the U.S. military has built and organized its cyber capabilities, and then touch on whether this is really optimized for the Chinese threat.

So, we can trace the Department of Defense's first real cyber strategy to July 2011. The 2011 strategy represented the DoD's first nascent attempt at organizing and prioritizing what was an extremely profound and uncertain new cyber domain.

Unlike later versions of the DoD cyber strategies, no adversaries are named explicitly, and the document is as much concerned with non-State and in cyber threats as any one particular nation State.

This vagueness is likely a representation of a larger uncertainty that existed a decade ago about the role that the U.S. military would play in cyberspace.

Nevertheless, the document foreshadows a continuity across U.S. cyber strategies over the next decade, including a clear prioritization of protecting and respecting the principles of privacy and civil liberties, free expression, and innovation.

So, the four years after the 2011 strategy saw an exponential increase in the scope, severity and diversity of cyber hacks and attacks.

It also saw four years of learning and building, in which the U.S. Government focused on creating a federal approach to cyberspace.

This rise in cyber threats, as well as the evolution of U.S. Government roles and responsibilities, led to a significantly more mature 2015 Defense Department cyber strategy.

It is the first strategy to identify priority adversaries   namely, Russia, China, Iran, North Korea, and non-State actors   and then to articulate the Department of Defense's responsibilities within the federal government; most notably, to deter and defend the U.S. homeland, in order to control escalation.

I want to highlight this first period was a period of relative restraint in U.S. responses to cyber threats.

And coming into the Trump Administration in 2018, State-sponsored cyber activity was in no way slowing down.

The Obama Administration had been very concerned about the risks of escalation from U.S. military cyber operations.

Leading into the Trump Administration and after the Russian hack-and-release and disinformation campaigns of the 2018 election, there was a push from within both the private sector and the Department of Defense for a more active and forward-leaning strategy.

In response in 2018, the U.S. rewrote all of its cyber strategies, and moved from a diplomacy deterrence-first-to-be-prepared stance under the Obama Administration, to a forward-leaning risk acceptant and active strategy under the new administration.

In particular, the 2018 summary of the Department of Defense's cyber strategy introduced the concept of Defend Forward, confronting adversaries before cyberattacks even occur, to disrupt or halt malicious cyber activity at its source, including activity that falls below the level of armed conflict.

There are a few core assumptions that changed here. Whereas the Obama Administration had assumed that cyber operations were inherently escalatory, the Trump Administration believed the risks from attacks outweighed the risk of escalation. This led the administration to delegate more authorities down to the military.

Secondly, where previous strategies had focused on deterring and responding to cyber events, the new DoD cyber strategy presented cyber as a more or less constant competition below a threshold of armed conflict.

Despite the maturation of U.S. cyber strategy over the last decade, there are still elements that are inconsistent or undeveloped.

The first issue is clarity. Unclear language within Department of Defense strategies in the cyber command vision led onlookers to question what military cyber was really doing.

While public statements and DoD-sponsored articles painted a picture of Defend Forward that included cyber defense teams or intelligence sharing, unofficial reports by the New York Times suggested U.S. was placing malware exploits in Russian critical infrastructure.

This led onlookers to question how far forward exactly the U.S. was defending.

At its core, the ambiguity and language represented a two-threshold logical inconsistency within the U.S. strategy. U.S. wanted to deter adversaries in taking cyberattacks against the U.S. However, it didn't hold its own actions to the same thresholds.

Beyond the logical inconsistencies, even those who supported Defend Forward voiced concerns that these operations would become never-ending task forces, expensive to sustain, and difficult to tell whether they were more or less effective.

So, what is the DoD posture? Well, at the top four-star level is Cyber Command, which controls the Cyber National Mission Force. This includes teams who defend the nation by seeing adversary activity, blocking attacks, and maneuvering in cyberspace to defeat them.

In other words, CNMF is in charge of DoD operations to defend and protect non-military cyber targets within the United States. They are, therefore, the primary lead on Defend Forward operations designed to protect U.S. critical infrastructure.

The Cyber Command is in charge of coordinating all DoD cyber activities. This extensive defense, it includes coordinating with the Defense Information Systems Agency, which is in charge of enterprise-wide defensive measures.

Most of the DoD’s cyber funding and manpower actually resides in each of the respective Armed Services cyber components   ARMYCYBER, TENTH Fleet, the Sixteenth Air Force, and MARFORCYBER.

Each of these services has its own cyber mission teams, which are dedicated to service specific missions, whether those are in defense or offense.

The Armed Services also own their own networks and data, so each has its own version of a CIO office, as well as its own units devoted to cybersecurity. So, large variation in offense and defense within these services.

This creates an inherent tension between the manning and resources allocated at the functional level   for example, Cyber Command   as well as what resources are given to the Armed Services and the combatant commanders.

So, what does this mean for U.S. and China? First, China is an able cyber adversary that harnesses a large workforce, much larger than the United States, especially in cyber, and extensive research and data and information networks.

So, in a crisis or violent conflict, China will likely use these cyber capabilities to attack American command, control, and communications, as well as vulnerable digitally-enabled weapons systems.

While Chinese doctrine a decade ago suggested the PLA may conduct cyberattacks against American critical infrastructure early in a crisis, more recent discourse suggests that China's concerned about its own critical infrastructure.

Now, there's an inherent tension between developing U.S. military cyber forces that deal with Chinese status quo actions, which would primarily rely or reside in Cyber National Mission Force, and those forces that are developing Chinese cyber capabilities to combatant command campaign plans which reside primarily with the Armed Services.

In the future, they'll have to prioritize these force postures. That has not been done so far.

The solution for the U.S. military is to rely on resilience, building networks and data. But unfortunately, tied intimately to resilience is the DoD's struggle to modernize software procurement, development, sustainment, which has an outsized negative effect on cybersecurity.

Finally, the DoD should use a new cyber strategy as an opportunity to resolve some of the ambiguity and logical inconsistencies of the 2018 strategy.

In the past, the U.S. has stopped short of binding its own hands or credibly threatening anything beyond sanctions or tit-for-tat cyber punishment for these cyberattacks.

In the Biden Administration, we have the opportunity to solve both of these logical inconsistencies.

Thanks so much for your time.

PREPARED STATEMENT OF JACQUELYN SCHNEIDER, HOOVER FELLOW, HOOVER INSTITUTION, STANFORD UNIVERSITY

Jacquelyn G Schneider, PhD

Hoover Fellow, Hoover Institution, Stanford University

U.S. MILITARY STRATEGY AND DOMESTIC POLICY COORDINATION

Testimony before the U.S.-China Economic and Security Review Commission

Hearing on China's Cyber Capabilities: Warfare, Espionage, and Implications for the United States

February 17, 2022

Distinguished members of the Commission, thank you for the opportunity to speak with you today. I have been asked to talk about U.S. military cyber strategy and capabilities and to give my assessment about our force posture to combat the Chinese cyber threat. I want to make it clear that I am here in my civilian capacity as a Hoover Fellow at the Hoover Institution and do not speak on behalf of the U.S. government or the Department of Defense. Additionally, all my assessments come from public and unclassified documents and therefore I want to caveat that there may be U.S. military capabilities and operations that are not open source and therefore are not within the realm of my analysis.

Today I am going to give an overview of the evolution of the Department of Defense cyber strategy leading up to the 2018 concepts of "persistent engagement"[1] and "defend forward."[2] I will outline continuities and changes in assumptions within these strategies and assess their success. I will then detail more concretely how the U.S. military has built and organized its cyber capabilities and whether these capabilities and organizations are optimized to combat the Chinese cyber threat. Finally, I will conclude with policy recommendations for the U.S. military as it continues to deal with a growing Chinese cyber threat.

Department of Defense Cyber Strategy Overview

We can trace the Department of Defense's first real cyber strategy to July 2011, almost a full year after the creation of U.S. Cyber Command—what was then a sub-unified command under Strategic Command.[3] This 2011 strategy represented the DoD's first nascent attempt at organizing and prioritizing what was an extremely profound and uncertain "new" cyber domain. As such, the strategy is a starting point for how the U.S. military should think about cyber—more of a declaration that cyber mattered than an articulation of priorities, threats, or lines of effort. Unlike later versions of the DoD's cyber strategies, no adversaries are named explicitly and the document is as much concerned with non-state and insider threats as any one particular nation-state. It is also quite vague about how the U.S. military will combat the threat. This

[1] https://www.cybercom.mil/Portals/56/Documents/USCYBERCOM%20Vision%20April%202018.pdf?ver=2018-06-14-152556-010

[2] https://media.defense.gov/2018/Sep/18/2002041658/-1/-1/1/CYBER_STRATEGY_SUMMARY_FINAL.PDF

[3] https://csrc.nist.gov/CSRC/media/Projects/ISPAB/documents/DOD-Strategy-for-Operating-in-Cyberspace.pdf

vagueness is likely a representation of the larger uncertainty that existed a decade ago about the role that the U.S. military would play in cyberspace as well as the Department of Defense's relationships with other federal agencies in combating cyber threats. Nevertheless, the document foreshadows a continuity across U.S. cyber strategies over the next decade, including a clear prioritization of "protecting and respecting the principles of privacy and civil liberties, free expression, and innovation" while mitigating the vulnerabilities of the department's reliance on digital technologies.

The 2011 DoD cyber strategy came on the heels of the Obama Administration's International Cyberspace Strategy which articulated a largely optimistic view of cyberspace as an environment with a clear collective good for humanity—a perspective informed by the Arab Spring. Accordingly, the strategy sought to uphold the universal good of an open and interoperable, secure and reliable cyberspace primarily through norms, diplomacy, active law enforcement, as well as dissuasion and deterrence. The document called for little from the Defense Department, asking the military simply to "recognize and adapt to the military's increasing need for reliable and secure networks, build and enhance existing military alliances, and to expand cyberspace cooperation." Even the document's understanding of deterrence was predicated largely on resilience and proportional threats of punishment, promising to "reserve the right to use all necessary means—diplomatic, military, and economic—as appropriate and consistent with applicable international law ... we will exhaust all options before military force whenever we can; we will carefully weigh the costs and risks of action and of inaction; and will act in a way that reflects our values and strengthens our legitimacy and international support whenever possible."[4]

The four years after both of these 2011 strategies saw an exponential increase in the scope, severity and diversity of cyber hacks and attacks. It also saw four years of learning and building, in which the U.S. government focused on creating a unified federal approach to cyberspace (the infamous bubble chart which laid out the primary roles and responsibilities for DOD, DHS, Department of State, and the FBI/DOJ).[5] The Obama administration developed and articulated normative principles about appropriate behaviors in cyberspace (such as a norm against attacks on critical infrastructure), and focused on propagating these norms within the United Nations and relationships with allies.[6]

This rise in cyber threats as well as the evolution of U.S. government roles and responsibilities led to a significantly more mature 2015 Defense Department Cyber Strategy.[7] This is the first defense strategy to identify priority adversaries (namely Russia, China, Iran, North Korea, and non-state actors), to articulate the Department of Defense's responsibilities within the federal government, and to lay out defense cyber lines of effort. There are similarities across the 2011 and 2015 strategies. Most notably for the DoD, the 2015 strategy still focused mostly on norms and deterrence to combat cyber threats. The document called for the Defense Department to "be prepared to" defend the U.S. homeland and to "build and maintain viable

[4] https://obamawhitehouse.archives.gov/sites/default/files/rss_viewer/international_strategy_for_cyberspace.pdf

[5] "Cyber Strategy and Policy," *Committee on Armed Services, United States Senate, One Hundred Fifteenth Congress, First Session,* March 2, 2017.

[6] https://2009-2017.state.gov/secretary/remarks/2015/05/242553.htm

[7] ttps://media.defense.gov/2018/Sep/18/2002041658/-1/-1/1/CYBER_STRATEGY_SUMMARY_FINAL.PDF

cyber operations" in order to "control escalation." This strategy focused on responding to and preparing for cyber incidents and leaned heavily on deterrence—by denial and vague threats of punishment—as the primary line of effort for ensuring the open and secure use of cyberspace.

Government responses to cyber incidents from 2011 to 2015 centered mostly on economic, diplomatic and legal activities, and the Department of Defense was largely postured to support[8] other agencies rather than acting on its own. As former Secretary of Defense Chuck Hagel asserted in 2014, the Pentagon "will maintain an approach of restraint to any cyber operations outside the U.S. Government networks. We are urging other nations to do the same."[9] The Defense Department's 2015 cyber strategy may have primarily placed DoD cyber capabilities in a reserve and deter posture, however, they were experiencing exponential growth: 133 new cyber mission teams were developed, and four service cyber commands began to equip, train and operate cyber forces to support operations on the air, land and sea.[10]

I want to highlight that this first period was a period of relative restraint in U.S. military responses to cyber threats, and, coming into the Trump administration in 2018, state sponsored cyber activity was in no way slowing down. The Obama Administration was very concerned about the risks of escalation from U.S. military cyber operations including cyber network exploitation and therefore offensive cyber operations played a very limited role in the overarching cyber strategy. Leading into the Trump Administration and after the Russian hack-and-release and disinformation campaigns of the 2018 election,[11] there was a push from within both the private sector and the Department of Defense for a more active and forward leaning strategy.[12] In response, in 2018 the U.S. rewrote all of its cyber strategies and moved from a diplomacy deterrence-first, "be prepared" stance under the Obama Administration to a forward-leaning, risk acceptant, and active strategy under the new administration. In particular, the 2018 summary of the Department of Defense's Cyber Strategy introduced the concept of "defend forward," confronting adversaries before cyber-attacks even occur "to disrupt or halt malicious. cyber activity at its source, including activity that falls below the level of armed conflict."[13] In general, the Trump Administration's approach was highly decentralized, giving much more autonomy and responsibilities to the Department of Defense and Cyber Command (which was now elevated to a unified command).[14]

There were a few core assumptions that changed from 2015 and 2018. The first was an assumption about cyber risk. Whereas the Obama Administration had assumed that cyber operations were inherently escalatory, the Trump Administration believed the risk from adversary cyber attacks outweighed the potential risks of escalation. This led the administration to delegate more authorities down to the military. Secondly, whereas the previous. strategies had

[8] http://nationalsecurity.gmu.edu/wp-content/uploads/2018/05/Alexander-Testimony-A-Borderless-Battle.pdf
[9] https://archive.defense.gov/Speeches/Speech.aspx?SpeechID=1837
[10] https://www.defense.gov/News/News-Stories/Article/Article/1524747/cyber-mission-force-achieves-full-operational-capability/
[11] https://www.washingtonpost.com/technology/2018/12/16/new-report-russian-disinformation-prepared-senate-shows-operations-scale-sweep/
[12] https://www.academia.edu/34619726/Navy_Private_Sector_Critical_Infrastructure_War_Game_Report
[13] https://warontherocks.com/2018/09/defending-forward-the-2018-cyber-strategy-is-here/
[14] https://www.defense.gov/News/News-Stories/Article/Article/1966758/esper-describes-dods-increased-cyber-offensive-strategy/

focused on deterring and responding to cyber events, the new DoD cyber strategy and Cyber Command vision (colloquially nicknamed persistent engagement) presented cyber as a more or less constant competition below a threshold of armed conflict. This was a key assumption for the DoD as it framed cyber operations (both offensive and defensive) as pre-conflict, non-geographic problems. This is important because it carves out an operational space for the new Cyber National Mission Forces to plan and execute cyber campaigns outside of the joint planning or combatant command process. Finally, whereas the Obama Administration outlined five priority actors in its 2015 defense cyber strategy, the 2018 focuses more narrowly on China and Russia as the primary competitors and therefore the focus of cyber efforts.

This newfound defense cyber autonomy, combined with very operationally focused leaders like new commander, General Nakasone, led to large scale experimentation in Department of Defense cyber operations. Meanwhile, the Department of Homeland Security leaned forward under new leadership in its Cyber and Infrastructure Security Agency, ushering in a much more publicly responsive face to cybersecurity and new partnerships with both the private sector and the Department of Defense. Cyber Command and the Cyber and Infrastructure Security Agency began to release information about malware and threats broadly and created new operational structures centered around issue-specific task forces (for instance election security) that appeared to be relatively successful. Meanwhile, Cyber Command used its new authorities to develop new missions like "hunt forward,"[15] which sent U.S. cyber troops into allied and partner networks to search for adversary activity and to grow the new Cyber Mission Force (in both mandate and personnel).

Despite the maturation of U.S. cyber strategy over the last decade, there are still elements that are inconsistent or underdeveloped. The first issue is clarity. Unclear language (in particular the concepts of defend forward and persistent engagement) within Department of Defense strategies and Cyber Command Vision led onlookers to question what military cyber was really doing. While public statements[16] and DOD-sponsored articles[17] painted a picture of defend forward that included cyber defense teams in allied states or intelligence sharing with private sector, unofficial reports by the New York Times[18] suggested U.S. was placing malware exploits in Russian critical infrastructure. This led onlookers to question how far forward exactly the U.S. was defending. Faced with this ambiguity, some critics worried the U.S.' new strategic concept could inadvertently lead to retaliation, potentially violent.

At its core the ambiguity in language represented a two-threshold logical inconsistency within U.S. strategy. The U.S. wanted to deter adversaries from taking cyber attacks against the U.S., going so far in the 2018 Nuclear Posture Review[19] as to imply that cyber attacks *could* be responded to with nuclear retaliation. However, it didn't hold its own actions to the same threshold. In fact, in its own strategy, the U.S. asserted that most cyber attacks were below a "threshold of armed conflict" and therefore that the U.S. intended to conduct undefined cyber

[15] https://www.cybercom.mil/Media/News/Article/2433245/hunt-forward-estonia-estonia-us-strengthen-partnership-in-cyber-domain-with-joi/
[16] https://www.fifthdomain.com/smr/cybercon/2019/11/12/heres-how-cyber-command-is-using-defend-forward/
[17] https://ndupress.ndu.edu/Portals/68/Documents/jfq/jfq-92/jfq-92.pdf
[18] https://www.nytimes.com/2019/06/15/us/politics/trump-cyber-russia-grid.html
[19] https://media.defense.gov/2018/Feb/02/2001872886/-1/-1/1/2018-NUCLEAR-POSTURE-REVIEW-FINAL-REPORT.PDF

actions prior to conflict without anticipating retaliation. The ambiguity in language made it hard to differentiate between what cyber attacks were appropriate and which were inappropriate, suggesting the U.S. might have different interpretations about what it believed it could do in cyberspace versus what its adversaries could do.[20] This analytical slippage had secondary effects on deterrence credibility as it called into question whether the U.S. was really willing to punish (up to nuclear weapons) for cyber attacks.

Beyond the logical inconsistencies, even those who supported defend forward voiced concern that these operations could become never ending task forces, expensive to sustain, and difficult to tell whether they were more or less effective.[21] This leads to the second real problem with U.S. cyber strategies across time. None of these cyber strategies outlined how to assess whether the strategy or its implementation was more or less effective. Even the 2018 Joint Publication 3-12 on cyberspace operations (the Department of Defense's more or less guidebook on how it organizes and U.S.es cyber capabilities) punts on measures of performance in cyberspace, declaring that "development of operational-level MOPs/MOEs (measures of performance/measures of effectiveness) for CO (cyber operations) is still an emerging aspect of operational art."[22] Additionally, all of the strategies struggled to articulate time horizons, a problem when assessing their effectiveness. Cyber Command's vision of persistent engagement intentionally downplays the role of events or time-bounded crises in cyber strategy, but also fails to delineate any differentiation between short term and long term effectiveness for the vision For example, Obama Administration efforts at the end of their term to clamp down on Chinese IP theft in cyberspace were initially successful; however, five years later Chinese IP theft is on the rise at potentially greater levels than seen before 2015.[23] Does that mean that defend forward wasn't a successful strategy?

Finally, while all of the DoD cyber strategies so far have prioritized the need for an open, free, and secure internet; they stop short at identifying the DoD's role in safeguarding valid information. What role, if any, should the DoD play in combatting campaigns of disinformation or the manipulation of data to degrade trust in economic or governance systems? The DoD has devoted cyber capabilities to foreign disinformation campaigns against COVID[24] as well as foreign campaigns of electoral disinformation. However, disinformation scholars find it difficult to disaggregate many foreign disinformation campaigns from domestic. This complex relationship between foreign and domestic actors in disinformation complicates the scope of DoD authorities when it comes to combatting disinformation. Future strategies will have to assess what the appropriate role for the DoD should be in these information campaigns.

Department of Defense Cyber Capabilities and Posture

[20] Schneider, Jacquelyn. "A strategic cyber no-first-use policy? Addressing the U.S. cyber strategy problem." *The Washington Quarterly* 43, no. 2 (2020): 159-175.

[21] https://cisac.fsi.stanford.edu/news/herb-lin-and-max-smeets-what-absent-us-cyber-command-vision; https://www.lawfareblog.com/persistent-engagement-foundation-evolution-and-evaluation-strategy

[22] JP 3-12, July 2018, pg. IV-22.

[23] https://www.wsj.com/articles/china-violated-obama-era-cybertheft-pact-u-s-official-says-1541716952

[24] https://www.defense.gov/News/News-Stories/Article/Article/2147566/DoD-works-to-eliminate-foreign-coronavirU.S.-disinformation/

The last ten years of DoD cyber strategy shaped U.S. cyber capabilities—both defensive and offensive. So how is the U.S. military's cyber force organized and how do we understand what U.S. military cyber capabilities are? There are many layers of cyber forces within the DoD. At the highest level are the joint organizations—Cyber Command and the Defense Information Systems Agency. Cyber Command is a 4-star level functional command whose commander, Gen Nakasone, also leads the National Security Agency. Cyber Command, like any functional command, is in charge of the larger joint bureaucratics of cyber operations: planning, joint cyber intelligence, coordinating operations, equipping and generating the force. It also, unique to a functional command, is in charge of its own Cyber National Mission Force (CNMF), which includes teams who "defend the nation by seeing adversary activity, blocking attacks, and maneuvering in cyberspace to defeat them."[25] This force, which includes National Mission Teams, National Support Teams, and National-level Cyber Protection Teams is in charge of "protection of non-DODIN blue cyberspace."[26] In other words, CNMF is in charge of DoD operations to defend and protect non-military cyber targets within the United States. They are, therefore, the primary lead on defend forward operations designed to protect U.S. critical infrastructure. It is a bit unclear what this means in practice, but could include counter-cyber attacks against nation states and foreign non-state actors that might target the United States.

Cyber Command is in charge of coordinating all DoD cyber activities. This coordination extends to defense: for example, in generating cyber protection teams and creating defensive strategies. It also includes coordinating with the Defense Information Systems Agency and the Joint Force Headquarters-Department of Defense Information Network. DISA is run by a three star, currently Air Force General Lt Skinner, who is also in charge of Joint Forces Headquarters—Department of Defense Information Network (JFHQ-DODIN). DISA can be thought of as the DoD's joint enterprise level manager of information systems. They are in charge of enterprise level network architecture and information technology management as well as "defensive cyber operations—internal defensive measures"[27] which include vulnerability assessments and incident response analysis.

[25] https://sgp.fas.org/crs/natsec/IF10537.pdf

[26] JP 3-12, July 2018, pg. I-9.

[27] DISA Fiscal years 2019-2022 Strategic Plan Version 2, pg. 14: https://disa.mil/-/media/Files/DISA/About/Strategic-Plan.ashx.

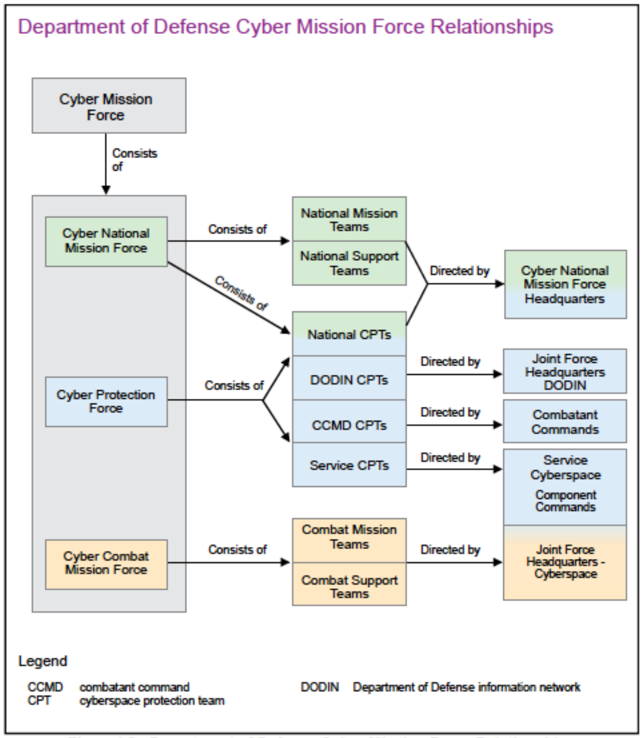

Department of Defense Cyber Mission Force Relationships
Cyber Mission Force
Consists of
Cyber National Mission Force
Consists of
Consists of
National Mission Teams
National Support Teams
Directed by
Cyber National Mission Force Headquarters
National CPTs
Cyber Protection Force
Consists of
DODIN CPTs
Directed by
Joint Force Headquarters DODIN
CCMD CPTs
Directed by
Combatant Commands
Service CPTs
Directed by
Service Cyberspace Component Commands
Cyber Combat Mission Force
Consists of
Combat Mission Teams
Combat Support Teams
Directed by
Joint Force Headquarters - Cyberspace
Legend
CCMD combatant command
CPT cyberspace protection team
DODIN Department of Defense information network

Figure I-2. Department of Defense Cyber Mission Force Relationships [28]

In addition to DISA, the Department of Defense also has a Chief Information Office which includes the Deputy Chief Information Officer for Cybersecurity who is in charge of “the integration of Defense-wide programs to protect the Department's critical infrastructure against advanced persistent threats, and assures coordination of cybersecurity standards, policies, and procedures with other federal agencies, coalition partners, and industry. The DCIO CS organizes and implements DoD efforts to transform the cyberspace workforce in support of U.S. national security priorities.”[29]

[28] JP 3-12, July 2018, pg. I-10.

[29] https://DoDcio.defense.gov/about-DoD-cio/organization/dcio-cs/

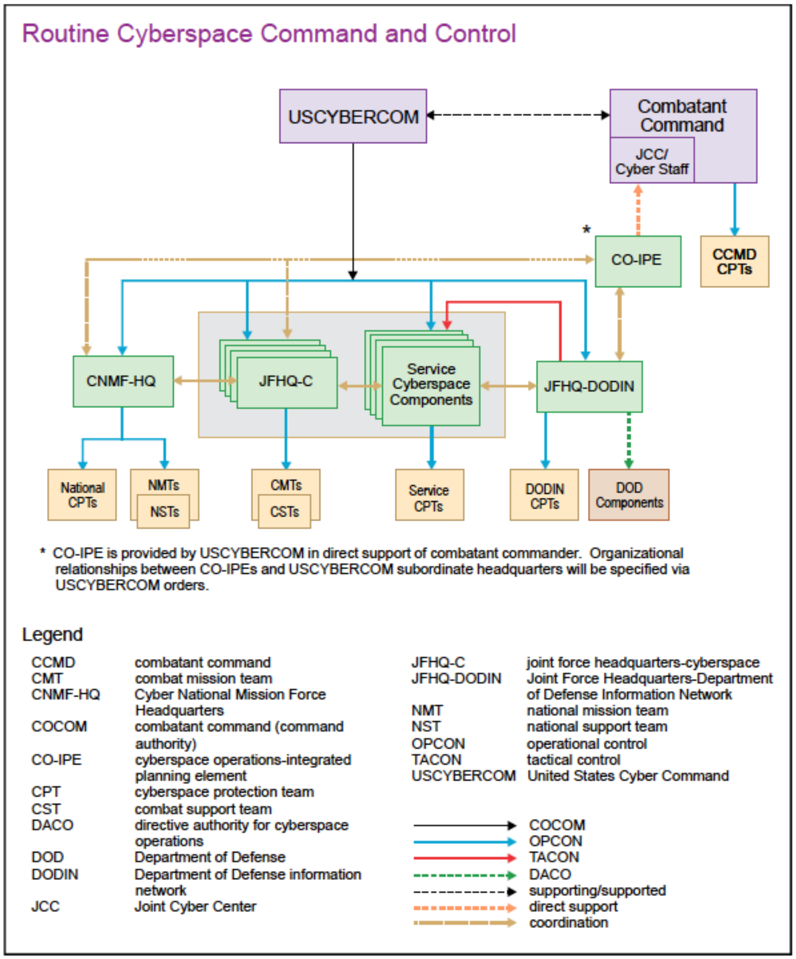

Routine Cyberspace Command and Control
USCYBERCOM
Combatant Command
JCC/ Cyber Staff
*
CO-IPE
CCMD CPTs
CNMF-HQ
JFHQ-C
Service Cyberspace Components
JFHQ-DODIN
National CPTs
NMTs
NSTs
CMTs
CSTs
Service CPTs
DODIN CPTs
DOD Components
* CO-IPE is provided by USCYBERCOM in direct support of combatant commander. Organizational relationships between CO-IPEs and USCYBERCOM subordinate headquarters will be specified via USCYBERCOM orders.
Legend
CCMD combatant command
CMT combat mission team
CNMF-HQ Cyber National Mission Force Headquarters
COCOM combatant command (command authority)
CO-IPE cyberspace operations-integrated planning element
CPT cyberspace protection team
CST combat support team
DACO directive authority for cyberspace operations
DOD Department of Defense
DODIN Department of Defense information network
JCC Joint Cyber Center
JFHQ-C joint force headquarters-cyberspace
JFHQ-DODIN Joint Force Headquarters-Department of Defense Information Network
NMT national mission team
NST national support team
OPCON operational control
TACON tactical control
USCYBERCOM United States Cyber Command
COCOM
OPCON
TACON
DACO
supporting/supported
direct support
coordination

Figure IV-1. Routine Cyberspace Command and Control

These organizations are all joint. However, most of the DoD's cyber funding and manpower actually resides in each of the respective armed services cyber components. Cyber Command is lead for the Cyber Mission Force; Army Cyber,[30] 10th Fleet,[31] the 16th Air Force,[32] and MARFOR Cyber[33] are the service leads. Each of the services has its own cyber mission teams which are dedicated to service-specific missions, whether those are in defense (cyber protection teams) or offense (cyber mission teams). Service cyber teams often focus on domain-specific targets: for instance, the 16th Air Force may specialize in cyber operations that support air campaigns by taking down radars or integrated air defense systems. In contrast, the 10th Fleet, may be concerned with cyber support to the aircraft carrier or anti-submarine warfare. Resources to develop offensive capabilities usually reside at the service cyber level (minus those resources allocated specifically to the Cyber National Mission Force). The armed services also own their own networks and data so each service has its own version of a CIO office as well as units devoted to cybersecurity on their service networks.[34] This means that there is large variation in both cyber offense and defense within each of the armed services.

[30] https://www.arcyber.army.mil/
[31] https://www.fcc.navy.mil/
[32] https://www.16af.af.mil/About-U.S./Fact-Sheets/Display/Article/1957318/sixteenth-air-force-air-forces-cyber/
[33] https://www.marforcyber.marines.mil/
[34] https://warontherocks.com/2021/12/the-air-force-isnt-doing-it-right/

The armed services own most of the personnel, resources, and infrastructure that man and equip DoD cyber. However, the geographic component commands use some of these service cyber resources in support of combatant plans and operations. Like in the other domains, there is an inherent tension between the manning and resources allocated at the functional level (Cyber Command) and within the armed services and what the combatant commanders have available to execute their combatant operations.

What does this all mean for U.S. military cyber capabilities? Measuring cyber capabilities is extremely difficult. Whereas in other domains capability is measured by orders of battle, performance in exercises, physical defense measures, or even the kinetic effects of different weapon systems—cyber capabilities are virtual, rarely static, difficult to predict their effect, and quite often classified. We therefore turn to proxies like number of personnel, maturity of organizations or doctrine, resident expertise, or past examples as a crude way to estimate capabilities. Using these proxies to evaluate US military cyber capabilities reveals some clear strengths and weaknesses.

First and foremost, the U.S. has perhaps the most mature cyber doctrine of any other country in the world. Additionally, U.S. Cyber Command and the service cyber elements have become the exemplar for military cyber institutional growth. Despite the institutional growth of U.S. military cyber, the U.S. is by no means the largest cyber force by number of personnel. Although it is difficult to estimate the entire DoD cybersecurity workforce, the military arm of the Cyber Mission Force includes 133 teams of approximately 6,000 personnel.[35] This is a far smaller number than estimates of the PLA's cyber workforce which can be as large as 50,000-60,000.[36] Additionally, the U.S. has struggled to attract and retain cyber talent in the military,[37] a challenge which all of the previous DoD cyber strategies discuss in depth. Finally, we know based on open source reporting that the U.S. has sophisticated cyber accesses and exploits.[38] It is unclear, however, the extent of these capabilities, partly because there are very few historical examples of known U.S. cyber exploits (especially ones that have significantly changed the course of a crisis or conventional military campaign). Similarly, defensive capabilities are difficult to assess. Government accountability office reports have critiqued the Defense Department for cyber vulnerabilities in weapons systems[39] and there are public reports of successful hacks against the Department of Defense—most notably the Russian led Solarwinds hack[40] and Chinese backed Microsoft exchange hack.[41] Perhaps critically, an arcane and difficult acquisitions process has made it difficult for the DoD to keep up with cutting edge commercial cybersecurity technology[42] while the byzantine bureaucratic administration of DoD networks has made it difficult to implement enterprise-wide cybersecurity solutions.[43]

[35] https://www.c4isrnet.com/cyber/2021/05/14/will-the-cyber-mission-force-soon-receive-more-personnel/

[36] https://www.nationaldefensemagazine.org/articles/2021/3/3/mumbai-incident-spotlights-chinas-cyber-capabilities

[37] https://digital-commons.U.S.nwc.edu/cgi/viewcontent.cgi?article=1044&context=U.S.nwc-newport-papers

[38] https://www.iiss.org/blogs/research-paper/2021/06/cyber-capabilities-national-power

[39] https://www.gao.gov/products/gao-19-128

[40] https://www.nytimes.com/2020/12/14/U.S./politics/rU.S.sia-hack-nsa-homeland-security-pentagon.html

[41] https://apnews.com/article/microsoft-exchange-hack-biden-china-d533f5361cbc3374fdea58d3fb059f35

[42] https://fcw.com/acquisition/2021/11/why-dod-is-so-bad-at-buying-software/259180/

[43] https://taskandpurpose.com/news/air-force-cybersecurity-nicolas-chaillan/

China: Cyber Competition and Conflict

What does all of this mean for U.S. and China, especially through the lens of competition or conflict? First, China is an able cyber adversary that harnesses a large workforce, extensive research in data and information networks, and who has shown a willingness to use cyber operations to steal intellectual property and exploit sensitive information. In a crisis or violent conflict, China would likely use these cyber capabilities to attack American command, control, and communications as well as vulnerable digitally enabled weapons systems. While Chinese doctrine a decade ago suggested the PLA might conduct cyber attacks against American critical infrastructure early in a crisis, more recent discourse suggests that China is concerned about its own critical infrastructure as well as escalation risks of targeting American civilians. These factors may induce restraint and limit Chinese cyber attacks on American critical infrastructure.

There is an inherent tension between developing U.S. military cyber forces to combat Chinese status quo cyber operations and preparing cyber capabilities for a U.S.-China crisis or conflict. On the one hand, countering Chinese intellectual property theft and network exploitation focuses on public-private partnerships, cyber defense, and broad national resiliency—potentially with the addition of counter cyber operations that target PLA cyber units or government sponsored hackers. These types of responsibilities would mostly reside with the Cyber National Mission Forces. In contrast, focus. on cyber capabilities for a conflict with China means devoting resources to cyber accesses and exploits within China's conventional military forces, command and control, and potentially that dual-use infrastructure that China might rely on to move and supply troops and weapons. These types of cyber missions would primarily be conducted by service cyber elements in conjunction with the combatant commands. Optimizing military cyber for status quo competition with China suggests prioritizing the Cyber National Mission Forces and Cyber Command over the geographic commands while focusing on cyberspace resources for military conflict with China prioritizes geographic commands. None of the cyber strategies so far have delineated priorities amongst these missions but manpower and resource limitations suggest that it will be hard the U.S. to devote adequate resources to both of these missions (as well as emerging challenges with disinformation campaigns, ransomware, and ongoing attacks from Russia, North Korea, and Iran).

Absent an ability to prioritize between a force postured for cyber competition with China versus a force focused on building targets and capabilities to use in a conflict, the U.S. military should invest in cyber capabilities that extend across competition and conflict: cyber defense, information and network resilience, and counter-cyber capabilities. None of these lines of effort are new to U.S. cyber strategy; the 2018 strategy introduced the concept of defend forward as a way to counter China in competition and conflict and talked explicitly about investments in defense and resiliency. However, it's unclear whether the U.S. has implemented or prioritized these lines of effort in its cyber posture against China. There is no open source reporting to suggest the U.S. has exercised defend forward by conducting offensive cyber operations to degrade PLA cyber capabilities. While the Cyberspace Solarium Commission recommended greater partnerships between the DoD and the defense industrial base, to include a threat hunting initiative, there is no evidence that either DoD or defense industrial base networks are less vulnerable than they were four years ago. Chinese intellectual property theft and network exploitation has increased since the last cyber strategy, suggesting that either the strategy or the implementation is not working against the status quo China cyber threat.

Policy Recommendations

What should the U.S. military do in order to better prepare its cyber force for both status quo competition and conflict with China?

The solution starts with resilience, or as Dr. Erica Borghard explains, "the ability to anticipate and withstand a disruptive event, and to rapidly restore core functions and services in its wake, whether it be a pandemic, financial crisis, terrorist attack, or large-scale cyber incident."[44] Resilience requires not only investing in networks and technologies that are more technically resilient, but also in building data users that are more resilient. For the Department of Defense, this involves building networks that gracefully degrade and campaigns that can be executed with limited access to data. At the core for any data user, whether it is a military officer, a federal civilian, or an American citizen is building human resilience—educating data users to question their data's biases, to look at data sources, and to have a back-up plan in place when they don't have access to digital resources.

Tied intimately to resilience are three activities: defense, intelligence, and information sharing. All three of these activities benefit from investments in commercial technology, as well as federal investment in research and development in cybersecurity. The DoD's struggle to modernize software procurement, development, and sustainment has an outsized negative effect on cybersecurity. Further, the Biden administration should continue to build out the interagency and public-private information sharing that matured over the Trump Administration. There continue to be difficulties sharing information between the public sector and defense; continued investments in clearinghouses and procedures to automate this information sharing will lead to better cyber defense for both the DoD and U.S. industry writ large.

The DoD should also use a new cyber strategy as an opportunity to resolve some of the ambiguity and logical inconsistencies of the 2018 strategy. Here the Biden Administration has a real opportunity with China—not only to ensure the success of its own strategy, but also to build norms of appropriate behavior in cyberspace. To do this a new strategy first needs to announce to adversaries and allies what is off limits, and subsequently deter these strategic cyber-attacks by threatening credible retaliation options. We've come close to this before. The Obama Administration crafted an Executive Order on sanctions[45] in response to cyber-attacks on critical infrastructure and Trump's State Department has called out cyber-attacks on health infrastructure as inappropriate behavior in cyberspace. However, the U.S. has always stopped short of binding its own hands or credibly threatening anything beyond sanctions or tit for tat cyber punishment for these cyber-attacks.

This is partially because the U.S. has been too expansive in what it has deemed as "off limit" cyber targets for adversaries. The Obama Administration's definition of critical infrastructure spanned 14-16 sectors and both Administrations have struggled to define what

[44] https://warontherocks.com/2021/01/a-grand-strategy-based-on-resilience/
[45] https://home.treasury.gov/policy-issues/financial-sanctions/sanctions-programs-and-country-information

kinds of cyber operations against these infrastructures they seek to deter. If everything is important, then nothing is important. Absent an understanding of what the U.S. cares about in cyberspace, ambiguous cyber deterrence by punishment policies have been unable to stem the increasingly prolific and sophisticated wave of cyber operations against U.S. civilian enterprises.

The first step, therefore, in solving the U.S. cyber strategy problem is to decrease strategic ambiguity about what cyber-attacks are serious enough to warrant a violent response from the U.S. To date, the U.S. has not resorted to violence in response to cyber-attacks, even though the U.S. has threatened up to nuclear response to cyber-attacks. Instead of these ambiguous threats, the U.S. needs to focus strategic deterrence on the cyber-attacks which are the most likely to have credible deterrence options. This is a high bar. Most cyber-attacks will not be able to be credibly deterred, but the U.S. may be able to credibly threaten cross-domain punishment for truly strategic cyber-attacks: those that create violent effects against civilian populations or threaten a state's nuclear control. At this high strategic level, which is only reserved for the most dangerous cyber operations, the U.S. can credibly threaten its vast and lethal military force and therefore shore up deterrence.

But defining and deterring what the U.S. cares about at the strategic level is only the first necessary step to solving the U.S. cyber strategy problem. The U.S. must not just assert these targets off limits for U.S. adversaries, but also declare them off limits for the U.S. The adoption of a no-first-use cyber strategic attack policy, especially one buttressed by credible threats of retaliation across military options, can help signal credible U.S. restraint and scope appropriate "status. quo" cyber activity, thus shoring up both a strategic threshold of restraint and a lower threshold of status quo cyber activity that occurs without violent retaliation. Both of these thresholds are essential for the current U.S. cyber strategy to succeed. And while a no first use policy was never adopted in the nuclear world, there are important differences in cyberspace that make no first use more credible and more advantageous. than in the nuclear domain.

While the adoption of a no first use strategic cyber-attack policy will help shore up strategic restraint, the U.S. will have to go beyond no first use in order to ensure strategic success. It must also pair strategic no first use policy with clearer statements about what types of activities fall under defend forward—thus making both ends of the cyber spectrum less ambiguous and more defined. Ideally, defend forward is a concept scoped to include only counter-cyber operations against cyber adversaries and not to target adversary civilian infrastructure. While defend forward may include up to offensive cyber activity, a clearer articulation of the focus of defend forward activities should help assure adversaries (and allies) that the U.S. will restrain these attacks and not target civilian infrastructure preemptively. This may help to solve the U.S. strategy's hypocrisy problem and correct the logical inconsistencies of an otherwise ambiguous defend forward. All of these actions support norms that the strategy should propagate about what are responsible actions in cyberspace—what is off limits (for U.S. and our adversaries) and where we need to invest in resiliency, defense, and punishment to make cyber exploits less likely to succeed.

Finally, the DoD will have to carve out of an already tight budget investments in crisis response, cyber support to conventional campaigns, and law enforcement. All of these lines of effort require more cybersecurity talent as well as federal funding for technology and coordination between local governments and federal agencies. The DoD should not be afraid of creative approaches to talent in the federal workforce, including a better use of the military reserves, the development of a civilian reserve corps, and more government fellowships for both academic and industry leaders to contribute to the federal workforce, even for a short time.

These efforts also require a closer look at whether our current planning and organizational structures are optimized for the threat. For example, the development of task forces within Cyber Command was an important innovation that replaced a rigid military campaign planning structure that never worked for cyber. But how do we organize task forces for non-time-delineated tasks like dealing with China? Further, these never-ending task forces are expensive and manpower intensive. How do we know how these task forces should be manned and what is working (or not working)?

The Department of Defense has made significant strides over the last decade to organize, prepare, and combat cyber threats. But China has only become more assertive and willing to use its cyber capabilities to compete with the U.S. economically and militarily. The Department of Defense will have to make difficult decisions to prioritize Chinese cyber threats and to allocate resources to combat status quo cyber operations while also building the reserve cyber capability necessary to combat China in a violent conflict. In the end, what will make the biggest difference will be investments in resiliency, defense, and countering PLA cyber capabilities.

OPENING STATEMENT OF NEIL JENKINS, CHIEF ANALYTIC OFFICER, CYBER THREAT ALLIANCE

CHAIRMAN WONG: Thank you, Dr. Schneider. And Dr. Jenkins.

DR. JENKINS: Thank you very much. Chairman Wong, Commissioner Bartholomew and distinguished Commissioners and staff, thank you for the opportunity to provide testimony today on the United States Government and private industry responses to the cyber challenge from China. It's an honor to be here with my fellow panelists.

I wanted to emphasize that cybersecurity is a risk management issue. Organizations must establish a layered defense and act on the information available to them.

They must follow best-practices, enact basic cyber hygiene, enable multi-factor authentication, and routinely patch vulnerable systems.

These basic actions go a long way in defending from all cyber threats, whether it be a Chinese spy trying to steal intellectual property, a ransomware affiliate based in Russia, or a common cybercriminal sending you a spear phishing link.

Of course, no organization has the resources available to take every recommended action possible. Even if they did, there's no guarantee that a persistent actor would not be able to find their way in.

Organizations must learn to manage their risk and tailor their defenses for the types of threats they are likely to face.

This is where the federal government comes in. Agencies like the Department of Homeland Security Cybersecurity and Infrastructure Security Agency, or CISA, the Federal Bureau of Investigation, and the National Security Agency, have greatly improved their information sharing to the public.

Information sharing from government agencies used to come from multiple agencies. It would be late and full of technical indicators that were old and no longer applicable.

Now, reports are released jointly and provided publicly. They do more attribution to malicious cyber actors, and describe what sectors they are targeting.

They include recommended actions that organizations should take to adapt their defenses. And while the technical indicators may still be old, they aren't as old as they used to be.

CISA, in particular, has taken on the role of the nation's risk advisor. CISA currently provides dedicated websites to highlight alerts on the threat from China and other nation State actors.

Information is available in a single location for organizations to review to see if they are at risk, and adapt their cybersecurity strategies accordingly.

While not related to the Chinese cyber threat, CISA’s Shields-Up website, which was established last week, is an excellent example of the progress that has been made.

With Russia continuing to threaten Ukraine, cybersecurity experts and policymakers are concerned that Russia may take actions in cyberspace that impact organizations outside of Ukraine.

CISA’s Shields-Up page serves to alert organizations to the risk. They provide recommended actions to take and technical documents to review to ensure that organizations are aware of the threat and ready.

This type of strategic warning from the government is welcome, and I hope it will continue to improve over time with feedback from the broader cybersecurity community.

Unfortunately, information sharing from the private sector to the government, especially information about incidents the government wouldn't otherwise have visibility into, has proven difficult.

It's hindered by legal issues, organizational policies, technology, and the lack of trust between government and private sector.

Congress and federal agencies have worked diligently to remove identified barriers to information sharing, but progress remains slow.

One way that CISA and their government partners are working to address these barriers is to establish the Joint Cyber Defense Collaborative.

The JCDC is an effort to evolve the public-private partnership and shift the focus to operational collaboration.

Operational collaboration seeks to build trust between people and organizations, expanding the possibility of what can be shared and what actions can be taken together in the common cause of strengthening the nation's cyber defenses.

JCDC partners currently include government agencies like CISA, FBI, Cyber Command and NSA, platform and cloud providers like Microsoft, Google Cloud and Amazon Web Services, and cybersecurity providers, such as Palo Alto Networks, CISCO, Symantec, CrowdStrike and Mandiant.

CISA is focusing initial JCDC efforts on the organizations that will have the most impact on the broader cyber ecosystem.

These private sector partners can take action on behalf of their customers, extending their reach beyond just a single organization. These partners have excellent visibility into the malicious cyber activity occurring in organizations all over the globe.

The insight they can bring can help fill gaps in U.S. government situational awareness. But we must find additional ways to bolster the public-private partnership.

While the U.S. has historically favored less cybersecurity regulation on organizations that maintain innovation, recent cyber incidents, such as the Colonial Pipeline ransomware attack, have shown how cyber actors can impact critical services on a national level.

There's a growing recognition that the market has not kept up with the threat and its impact. New legislative requirements may be necessary. I'd like to highlight two:

A requirement for critical infrastructure organizations to report cyber incidents to the federal government, and identifying systematically important critical infrastructure.

The reporting requirement will help government understand what incidents are occurring and their impact. This will help to shape government responses and improve future cybersecurity policy.

I also point to the Cyberspace Solarium Commission's recommendations to identify the nation's most important critical infrastructure, and requires the organizations that own it to participate in collaborative joint security efforts with the U.S. Government.

In exchange for special assistance and support from the U.S. Government to these organizations and enhanced liability protections, they would be required to certify their security compliance on a regular basis.

This proposal would go a long way in filling the gaps in the voluntary public-private partnership model.

More generally, the federal government should continue to increase the incentives for organizations to implement better cybersecurity.

Government should leverage existing regulations, where possible, to promote good cybersecurity behavior, support and encourage the use of best-practices, and drive industries that set standards of care for cybersecurity.

In conclusion, there are no easy fixes for cybersecurity. We must accept that cybersecurity requires more than just technology. It requires collaboration. This is especially true in the face of the complex cyber threat from China.

Thank you for the opportunity to discuss these topics, and I look forward to your questions.

PREPARED STATEMENT OF NEIL JENKINS, CHIEF ANALYTIC OFFICER, CYBER THREAT ALLIANCE

17 February 2022

Dr. Neil E. Jenkins
Chief Analytic Officer
Cyber Threat Alliance

Testimony Before the US-China Economic and Security Review Commission on U.S. Private Industry Responses to the China Cyber Challenge

Introduction

Thank you for the opportunity to provide testimony United States government and private sector responses to cyber threats from China. In the testimony below, you will note that the fundamentals of cybersecurity for the Federal government and the private sector are – for the most part – independent of the specific cyber threat from China. Organizations must manage the risk from the full spectrum of malicious cyber actors of all types, including nation state actors, cyber criminals, and hacktivists.

Malicious cyber actors leverage various tactics, techniques, and procedures, or TTPs, to achieve their end goals. At times, the TTPs that actors use to gain access to systems, such as spearphishing or password guessing, will be very similar. But what they do with that access can be very different. Through intelligence gathering, information sharing, and operational collaboration, organizations can begin to understand their specific risk profiles and adapt their defenses appropriately.

This testimony first describes the roles and responsibilities of Federal government agencies in cybersecurity, how the Federal government organizes for cybersecurity efforts, and how it shares information and collaborates with the private sector. I then describe private sector cybersecurity risk management and how collaboration between the public and private sectors fosters resilience. Next, I highlight the cyber threat from China, emphasizing how it is more of a long-term strategic threat in comparison to other nation state adversaries such as Russia, Iran, and North Korea. I conclude with a discussion of critical infrastructure cybersecurity efforts and recommendations for further improvements.

Roles and Responsibilities of U.S. Government Agencies in Cybersecurity

The roles and responsibilities of U.S. government agencies in cybersecurity are quite complex, reflecting the nature of cyberspace itself. Information technology (IT) is used to enhance our abilities to communicate, conduct business, store our information, and make processes more efficient. However, malicious actors can use those same IT systems to undermine trust in that same information, conduct disruptive ransomware attacks, steal intellectual property, and lead to destructive attacks against critical infrastructure. A discipline that covers this much territory cannot be managed effectively by a single government agency. The government must bring various agencies together to work toward a common goal and use their various authorities and capabilities in a coordinated and collaborative way, providing guidance and information to the private sector so they may manage their own cyber risk.

National cyber strategy and policy is guided by the White House by the National Security Council (NSC) and the newly established Office of the National Cyber Director (ONCD). The National Security Advisor develops national security strategy and policy for the President, of which cyber is and will continue to be an important factor, and connects cyber to the broader geopolitical strategic approach to China and other nation states. The development of a National Cyber Strategy will be conducted by the NSC, in coordination with the ONCD and other government agencies.[1] The NSC also has a role in coordinating military and intelligence cyber operations with the operational activities of other government agencies.

The ONCD intends to guide cooperation and collaboration between government agencies to improve public-private collaboration, align resources across the government, and increase present and future resilience.[2] The ONCD and the NSC must work together closely to model the cooperation and collaboration needed across federal agencies. The Office of Management and Budget (OMB) also has a role in setting cybersecurity policy for Federal departments and agencies through the Federal Chief Information Officer and the Federal Chief Information Security Officer.

The bulk of the federal government's cybersecurity efforts are conducted by the Department of Homeland Security's Cybersecurity and Infrastructure Security Agency (CISA) and the Department of Justice's Federal Bureau of Investigation (FBI). CISA leads "the National effort to understand, manage, and reduce risk to our cyber and physical infrastructure"[3] and acts as the Nation's risk advisor. CISA is the operational lead for Federal cybersecurity (the .gov) and acts as the National Coordinator for critical infrastructure security and resilience. CISA provides technical assistance, incident response, tools, information, and training that organizations across the public and private sectors can use to manage their risk. To differentiate the responsibilities of CISA and the NCD, CISA Director Jen Easterly noted in recent Congressional testimony that CISA is "the quarterback" and NCD is the "coach of the team" that brings a "sense of coherence and unity of effort," reflecting their respective operational and strategic roles.[4]

Whereas CISA focuses their cybersecurity efforts on information technology assets, organizations, and sectors, the FBI focuses on the threat actors at the source of cyber intrusions. The FBI's cyber strategy is to "impose risk and consequences on cyber adversaries" through their role as the lead federal agency for investigating cyber attacks and intrusions.[5] The FBI conducts law enforcement investigations related to cyber activity, attributes malicious

[1] https://www.lawfareblog.com/how-national-cyber-director-position-going-work-frequently-asked-questions
[2] https://www.whitehouse.gov/wp-content/uploads/2021/10/ONCD-Strategic-Intent.pdf
[3] https://www.cisa.gov/about-cisa
[4] https://twitter.com/ericgeller/status/1403002705702916096?s=20
[5] https://www.fbi.gov/investigate/cyber

activity to specific actors, and responds to incidents to provide technical assistance and collect evidence. Federal agencies such as the U.S. Secret Service and Immigration and Customs Enforcement also have cyber law enforcement authorities, and these various investigations are coordinated through the FBI's National Cyber Investigative Joint Task Force (NCIJTF).

Other government agencies with significant cybersecurity responsibilities include:

- Sector Risk Management Agencies (SRMAs) such as the Department of Energy and the Treasury, work with the 16 critical infrastructure sectors to understand their risks and build trusted partnerships with the U.S. government.[6]
- Members of the Intelligence Community provide strategic indications and warnings, situational awareness of threat actors, and technical indicators of threat activity.
- Within the Department of Defense (DoD), the National Security Agency provides cyber related intelligence and protects National Security Systems, while the U.S. Cyber Command provides options for military cyber operations, defends the DoD networks, and supports the defense of national interests in cyberspace.[7]
- The State Department conducts diplomacy with other countries on cybersecurity issues.
- The Department of Justice uses tools such as criminal indictments or asset seizures against malicious cyber actors.
- The Department of Treasury imposes sanctions on malicious adversaries at the direction of the President.
- The Department of Commerce can place an organization on its Entity List, which restricts the US organizations from trading with specific entities, including Chinese companies like Huawei and ZTE.
- The Federal Communications Commission regulates access to U.S. telecom markets.
- The Federal Trade Commission and the Securities and Exchange Commission provide regulatory oversight roles for cybersecurity in the private sector.

When government agencies collaborate, they can synthesize information from various sources inside and outside of government to help the private and public sectors manage their risk and find the best ways to punish malicious cyber actors. The level of collaboration within the government has improved greatly over the last decade. Ten years ago, agencies would often release different information to different stakeholders, confusing the private sector and reducing the strategic impact of the releases. Now, agencies are much more likely to coordinate the release of technical indicators and risk management advice in a joint report. I will return to this in a later section of this testimony.

Private Sector Cybersecurity and Resilience – Improving, but still room for growth

The cybersecurity of an individual organization is the responsibility of that organization and not of the federal government. The information technology and systems that organizations use to conduct business, operate critical infrastructure, and communicate internally and externally are

[6] https://www.cisa.gov/sector-risk-management-agencies
[7] https://www.cybercom.mil/About/Mission-and-Vision/

deeply embedded in business practices. Organizations must constantly make risk-based decisions on how best to secure themselves while maintaining their ability to operate. Cybersecurity decisions are often resource-intensive and patching a new vulnerability or setting up multi-factor authentication can slow business operations. Organizations are in the best position to understand how to best implement cybersecurity practices and mitigate their risks.

An organization's overall level of cybersecurity is dependent on the resources and budget available. Cybersecurity is complex, requires a well-trained workforce, and is often costly to implement at scale. Over time, managing cybersecurity risk has gotten easier as cybersecurity providers have improved their products and services and many organizations that provide IT solutions have improved the security of their products. But the complex nature of systems that operate on code and are connected to the internet require constant monitoring and updating to address new vulnerabilities and threats.

What steps do organizations take to build a cybersecurity program? Most organizations, especially those that own and operate critical infrastructure, will leverage a layered, defense-in-depth strategy to cybersecurity. They will do their best to follow general cybersecurity best practices, like the NIST Cybersecurity Framework[8] and the Center for Internet Security's Critical Security Controls,[9] and practice good cyber hygiene, like scanning their environment for known vulnerabilities and patching them. They will train their workforce to improve their ability to identify and avoid phishing emails. They will develop and exercise cyber incident response plans.

They will use a cybersecurity provider to operate a detection and response capability on their endpoints and networks. They will manage a Security Operations Center or use a Managed Security Services Provider to comb through alerts from their systems to look for signs of malicious activity and subscribe to commercial threat intelligence feeds to get access to indicators of compromise or strategic warning on cyber attacks. Some organizations will staff their own threat intelligence teams to focus on specific threats to their organizations and use that intelligence to adapt their defenses against the threats most likely to target them.

Organizations may also employ threat hunters who look for signs of adversary TTPs being used on their networks that their sensors missed. They could hire external services to act as penetration testers that act like hackers and try and break into an organization, testing and probing their cyber defenses.

They can also join an Information Sharing and Analysis Center (ISAC) with companies in the same critical infrastructure sector to learn about threats and vulnerabilities their competitors face and apply those lessons. For any risks they can't mitigate with technology, outside contractors, training, or information sharing, they may purchase cyber insurance and transfer their risk.

[8] https://www.nist.gov/cyberframework

[9] https://www.cisecurity.org/controls/

The bottom line is that each of these layers of defense represent a cost for an organization. C-suites must make decisions on whether to spend their budget on additional cybersecurity protections, on other security provisions, or on a new manufacturing line. The larger the organization, in general, the more of these steps they can take. Unfortunately, most organizations are not able to take all these actions and must make choices, eventually accepting a level of cyber risk. This includes organizations in the supply chain of critical infrastructure owners and operators who provide important services and embedded technology.

All organizations need good, actionable information to understand the threats they face and the vulnerabilities inherent in their systems and help them make their risk management decisions. This information comes from multiple sources, such as their product and security vendors and their ISACs. It can also come from the Federal government.

Cooperation Between the U.S. Government and Private Industry on Cybersecurity Issues

Historically, cooperation between the U.S. government and private industry has been focused on information sharing between the private and public sectors to ensure that threats and mitigations are widely known and actioned accordingly. Information sharing should be bidirectional to be most effective, from the government to the private sector and vice versa. The government should strive to get the right information to the right recipients in time to make a difference. This section focuses on the cooperation between the government and the private sector in general. We will discuss how the government conducts enhanced collaboration with critical infrastructure in a later section.

Over time, information sharing from the government has improved and expanded in scope and scale. 15 years ago, cybersecurity information may have only been shared to organizations in classified environments where the government would give a Chief Executive Officer a one-day security clearance. The company may not have been able to do much with the information to make themselves more secure. Now, CISA and FBI work together and with their partners in the intelligence community to declassify information, combine that with reporting from the cybersecurity industry, and produce a single alert with strategic warning and technical indicators that can be used to secure systems and look for signs of malicious cyber activity. CISA posts that alert on their public website[10] and will tweet links to it, imploring organizations to take action.

CISA provides dedicated websites to highlight the threat from nation state actors such as China,[11] Russia,[12] Iran,[13] and North Korea.[14] Each website provides an overview of the cyber

[10] https://www.cisa.gov/uscert/ncas/alerts
[11] https://www.cisa.gov/uscert/china
[12] https://www.cisa.gov/uscert/russia
[13] https://www.cisa.gov/uscert/iran
[14] https://www.cisa.gov/uscert/northkorea

threat from these nation states and the latest advisories related to that activity. CISA has released more advisories on China over time, providing one China-specific alert each in 2017, 2018, and 2019, and then 4 alerts in 2020 and 5 in 2021. These alerts provide details on how to mitigate and detect this activity and report any incidents to the government.

Despite these advances, information sharing is far from perfect. The Federal government has tried to implement automated sharing of technical information with limited success and its most current efforts in this realm have little utility.[15] Federal agencies have greatly improved their timeliness when releasing alerts and technical information, but indicators shared in these reports can still be months old – a lifetime in cybersecurity. Organizations are relatively unwilling to share information to the government because of concerns with information becoming public and negatively impacting their reputation, increasing regulations on them or their sector, or exposing the organization to legal liability.

Legislation such as the Cybersecurity Information Sharing Act of 2015[16] helped clarify how the private sector can report incidents to the Federal government and provides liability protection to entities that share appropriately. Unfortunately, this legislation has not had the impact that many had hoped as the information sharing environment has proven to be complex. Additional steps may be required correct issues. It's likely that the entire community needs to completely reset expectations for what will be shared to the government and to the private sector. We must continue to address issues with information sharing and improve them whenever possible, but, in parallel, we must realize that information sharing alone is not enough and we must focus on actual operational collaboration between the Federal government and the private sector.

Operational collaboration is the act of bringing organizations together to share information, but then working together to act on that information to plan, prioritize, and synchronize activity to protect networks, disrupt malicious cyber activity, and respond to cyber incidents. Operational collaboration happens today in various pockets and sectors, such as the Cyber Threat Alliance,[17] the Analysis and Resilience Center,[18] and any number of trust communities within the cybersecurity ecosystem. These groups actively work together to have a broader impact on the cybersecurity of the whole ecosystem and organizations they represent. At its heart, operational collaboration builds trust between people and organizations, expanding the possibility of what can be shared and what actions can be taken together.

CISA has recently taken steps towards operational collaboration with the private sector, establishing the Joint Cyber Defense Collaborative (JCDC) to bring together public and private sector actors to "unify defensive actions and drive down risk in advance of cyber incidents occurring" and "strengthen the nation's cyber defenses through planning, preparation, and

[15] https://www.oig.dhs.gov/sites/default/files/assets/2020-09/OIG-20-74-Sep20.pdf
[16] https://www.congress.gov/bill/114th-congress/senate-bill/754/text
[17] https://www.cyberthreatalliance.org/
[18] https://systemicrisk.org/

information sharing."[19] JCDC partners currently include platform and cloud providers, like Microsoft, Google Cloud, and Amazon Web Services, as well as cybersecurity providers, such as CrowdStrike, Mandiant, Palo Alto Networks, Cisco, and Symantec. CISA is rightly focusing their initial collaborative efforts on the organizations that can have the most impact on the broader cyber ecosystem. They plan to include more critical infrastructure and state, local, tribal, and territorial (SLTT) partners over time.

While operational collaboration is clearly the correct next step and CISA should be applauded for moving in this direction, we must acknowledge that there are two key factors that shape the extent and limits of cooperation between private sector and the Federal government. First, the fundamental interests of the parties are not always the same. Private sector companies seek a profit while governments protect the national interest. One goal is not necessarily better or more important than the other, but these interests shape the relationship in steady state. The area of interest for the private sector is also not the same for the government. Many companies are multinational and must work with non-U.S. government entities (sometimes including China) while the U.S. government is solely focused on the United States. Partners in operational collaboration must understand that everyone's interests will not always be the same and focus efforts on common goals and objectives.

Malicious Cyber Activity from Chinese Actors

Before I describe how the U.S. government collaborates specifically with U.S. critical infrastructure, let's first discuss recent trends and malicious cyber activity from emanating specifically from China. Chinese nation-state activity in cyberspace has been different than the activity we see from the other nation-state actors we typically focus on. Russia, Iran, and North Korea see it in their national interests to be disruptive, attempting to upend the international system. China, on the other hand, seeks to remake the international system in its favor, without entirely upsetting the current economic and geopolitical order. They want to compete and win within the current system. Rob Joyce, the Director of the NSA's Cybersecurity Division, makes a useful analogy: "I kind of look at Russia as the hurricane. It comes in fast and hard. China … is climate change: long, slow, pervasive."[20,21] When asked by the Washington Post which nation is the United States' most dangerous cyber adversary, Katie Nickels, the director of intelligence for cybersecurity firm Red Canary said, "When dangerous is defined as having the greatest potential to threaten the strategic role of the U.S. as an enduring great power, the answer is China."[22]

This strategic competition in cyberspace from Chinese actors has manifested in espionage and the theft of intellectual property targeting various sectors and technology that the Chinese

[19] https://www.cisa.gov/jcdc

[20] https://www.washingtonpost.com/news/powerpost/paloma/the-cybersecurity-202/2019/03/06/the-cybersecurity-202-u-s-officials-it-s-china-hacking-that-keeps-us-up-at-night/5c7ec07f1b326b2d177d5fd3/

[21] https://warontherocks.com/2020/01/russia-as-a-hurricane-china-as-climate-change-different-ways-of-information-warfare/

[22] https://www.washingtonpost.com/politics/2022/01/20/is-russia-or-china-biggest-cyber-threat-experts-are-split/

government has prioritized. In recent years, this activity has focused on the sectors identified in their “Made in China 2025” plan.[23] FBI Director Christopher Wray recently highlighted the threat to intellectual property and U.S. economic security from Chinese activity, noting that “it’s reached a new level – more brazen, more damaging than ever before, and it’s vital – vital – that all of us focus on that threat together.”[24]

China’s ”Made in China 2025” plan provides a useful guide to the industries that Chinese state actors have targeted for intellectual property theft, including information technology, robotics, aerospace, biopharmaceuticals, medical, electrical, farming, rail, new energy vehicles and green technologies. As Director Wray notes, “Whatever makes an industry tick, they target: source code from software companies, testing data and chemical designs from pharma firms, engineering designs from manufacturers, personal data from hospitals, credit bureaus, and banks.”[25]

Chinese targets have also obtained personal data of cleared civilian U.S. government employees and contractors through the 2015 Office of Personnel Management (OPM) incident. Experts speculate that combining data gained through the OPM hack with stolen data from other entities such as hotels and credit bureaus could lead to identification of U.S. intelligence agents and assets.[26]

Chinese nation-state actor TTPs have become more sophisticated over time. Prior to the 2015 Obama-Xi agreement, Chinese activity was relatively “loud” from a cybersecurity perspective. They leveraged spearphishing emails to target entities across nearly every critical infrastructure sector, and multiple threat actors from various Chinese government agencies would be found targeting the same data. Of late, Chinese actors “now concentrate on lower-volume but more-sophisticated, stealthier operations collecting strategic intelligence to support Chinese strategic political, military, and economic goals.”[27] They have transitioned away from spearphishing and often use harder-to-detect TTPs such as software vulnerabilities, living-off-the-land binaries, dual-use tools like Cobalt Strike, and exploitation of network devices and web facing applications. They also have been seen leveraging supply chain vulnerabilities and targeting third party providers, such as Managed Security Providers, to gain access to their eventual end targets.[28,29]

While intellectual property theft and espionage are the primary ways Chinese actors have impacted U.S. entities, we have seen signs of other cyber activity that trends towards more

[23] https://www.cfr.org/backgrounder/made-china-2025-threat-global-trade
[24] https://www.fbi.gov/news/speeches/countering-threats-posed-by-the-chinese-government-inside-the-us-wray-013122
[25] https://www.fbi.gov/news/speeches/countering-threats-posed-by-the-chinese-government-inside-the-us-wray-013122
[26] https://www.wired.com/story/china-equifax-anthem-marriott-opm-hacks-data/
[27] https://www.mandiant.com/resources/updates-on-chinese-apt-compromising-pulse-secure-vpn-devices
[28] https://www.mandiant.com/resources/updates-on-chinese-apt-compromising-pulse-secure-vpn-devices
[29] https://www.reuters.com/investigates/special-report/china-cyber-cloudhopper/

brazen and disruptive actions. In February and March of 2021, Chinese state-sponsored actors that Microsoft calls HAFNIUM began targeting zero-day vulnerabilities in on-premises Microsoft Exchange Servers through automated attacks, installing malicious webshells on any vulnerable server they could access.[30] Cybersecurity firm ESET noted that multiple Chinese groups beyond HAFNIUM were using this vulnerability to compromise email servers around the world.[31] This indiscriminate activity from multiple Chinese threat actors was out of character compared to their activity in recent years for and required many organizations to interrupt their normal business activities to patch and remediate this activity.

Additionally, CISA and FBI provided evidence of a Chinese campaign targeting U.S. oil and national gas pipeline companies from 2011 to 2013 "for the purpose of holding U.S. pipeline infrastructure at risk."[32] The report noted that the activity "was ultimately intended to help China develop cyberattack capabilities against U.S. pipelines to physically damage pipeline or disrupt pipeline operations." U.S. government officials have also accused actors working for Chinese intelligence of using ransomware to extort U.S. businesses,[33] but it is unclear if this ransomware activity was directed by the Chinese government. These insights into potentially disruptive cyber activity from China are few and far between, but they provide a glimpse into what could be possible in the event of an escalation in global tensions.

U.S. Critical Infrastructure Cybersecurity, Regulatory Frameworks, and Recommendations

Critical infrastructure in the United States is defined in the Patriot Act of 2001 (42 U.S. Code § 5195c) as the "systems and assets, whether physical or virtual, so vital to the United States that the incapacity or destruction of such systems and assets would have a debilitating impact on security, national economic security, national public health or safety, or any combination of those matters."[34] Presidential Policy Directive 21 (PPD-21) makes it the policy of the United States to "strengthen the security and resilience of its critical infrastructure against both physical and cyber threats"[35] and provides guidance to Federal government agencies to work with critical infrastructure owners and operators to take proactive steps together to manage their risk.

PPD-21 defines 16 critical infrastructure sectors and assigns agencies to serve as their sector-specific agency to manage the day-to-day Federal interface with the sector and represent their risk management needs and priorities to the rest of the Federal government. The FY21 National Defense Authorization Act codified Sector-Specific Agencies as Sector Risk Management Agencies (SRMAs) to better reflect their role with the critical infrastructure sectors.[36] The

[30] https://www.microsoft.com/security/blog/2021/03/02/hafnium-targeting-exchange-servers/
[31] https://www.welivesecurity.com/2021/03/10/exchange-servers-under-siege-10-apt-groups/
[32] https://www.cisa.gov/uscert/ncas/alerts/aa21-201a
[33] https://www.nbcnews.com/tech/tech-news/us-accuses-china-abetting-ransomware-attack-rcna1448
[34] https://www.law.cornell.edu/uscode/text/42/5195c
[35] https://obamawhitehouse.archives.gov/the-press-office/2013/02/12/presidential-policy-directive-critical-infrastructure-security-and-resil
[36] https://www.cisa.gov/sector-risk-management-agencies

Secretary of Homeland Security coordinates the activities of SRMAs through CISA's National Risk Management Center (NRMC)[37] which also maintains a list of National Critical Functions to help further refine the government's support of critical infrastructure.[38] Businesses and organizations within the U.S. voluntarily choose to participate in sector risk management activities with the Federal government.

The security and resilience of U.S. critical infrastructure can only be attained through partnership between the private and public sectors, which includes Federal and SLTT governments. The private sector owns and operates the vast majority of the Nation's critical infrastructure (you will commonly hear that the private sector owns as much as 85% of critical infrastructure, though this oft quoted percentage is not based on hard data[39]). The private sector operates their critical infrastructure to ensure their businesses operate effectively for the benefit of shareholders, customers, and the general public that relies on their goods and services. The Federal government has little to no directive authority over most of this infrastructure and is limited to providing information to help manage risk, such as threats and vulnerabilities that may affect critical infrastructure, and fostering analysis of cross-sector activities to highlight dependencies between sectors.

Voluntary participation in critical infrastructure activities with the Federal government confers several benefits to the participating entities. Engagement provides insights into national security priorities and a forum for the private sector to inform Federal policy security priorities and initiatives. Critical infrastructure organizations are eligible to receive security clearances and access to classified intelligence and unclassified non-public information that can be useful in managing their risk. The Protected Critical Infrastructure Information (PCII) program enhances sharing from the critical infrastructure entities to the government.[40] Sensitive and proprietary information shared with the government through PCII cannot be released to the public through Freedom of Information Act (FOIA) requests, SLTT disclosure laws, or civil litigation, and it cannot be used for regulatory actions.

Regulation related to the cybersecurity of critical infrastructure is sparse and affects a small number of sectors, such as Energy and Financial Services, where Federal regulation in general is more common. The U.S. has historically favored less cybersecurity regulation on organizations to maintain innovation and allow the market to be nimble. There is also a danger that the U.S. government could regulate poorly in cybersecurity, resulting in a compliance heavy approach that does not improve security.

However, this policy environment is shifting as recent cyber incidents like the ransomware incident targeting Colonial Pipeline have impacted critical services on a national level and there is a growing recognition that the market has not been able to keep up with the threat. Suzanne

[37] https://www.cisa.gov/national-risk-management
[38] https://www.cisa.gov/national-critical-functions
[39] https://www.lawfareblog.com/it-really-85-percent
[40] https://www.cisa.gov/pcii-program

Spaulding, the former Under Secretary for the DHS office that has become CISA and a member of the Cyberspace Solarium Commission, noted in recent House testimony that "we cannot rely upon markets alone to ensure the continuity of nationally critical functions upon which the American public relies."[41]

Policy makers and legislators have been discussing ways to strengthen the private-public partnership through new legislative requirements. One of the most prominent legislative approaches has been a proposed requirement for critical infrastructure organizations to report cyber incidents to the Federal government. The Cyberspace Solarium Commission provides a useful legislative proposal for cyber incident reporting.[42] The latest series of discussions around this proposed legislation has framed a reporting requirement as a way to understand the scope and scale of the ransomware. Providing the Federal government with information related to all cyber incidents, including intellectual property theft and espionage like that from China, will help policy makers define the scope and scale of incidents and lead to better responses.

The Cyberspace Solarium Commission also proposed that Congress codify the concept of "systematically important critical infrastructure" (SICI) where "entities responsible for systems and assets that underpin national critical functions are ensured the full support of the U.S. government and shoulder additional security requirements consistent with their unique status and importance."[43] SICI entities are the most critical parts of our critical infrastructure. As noted above, participation by entities in government efforts is currently voluntary, but this proposal would seek to identify the infrastructure that is most important to the public health and safety, economic security, and national security of the U.S. and require them to participate in "collaborative joint security efforts." In exchange for special assistance and support from the U.S. government to these organizations and enhanced liability protections, they would be required to certify their security compliance on a regular basis.

This proposal would go a long way in filling the gaps in the current voluntary private-public partnership model and foster the operational collaboration necessary to better manage cybersecurity risk nationally. Focused information sharing and collaboration with SICI entities that are likely targets of Chinese intellectual property theft should be a priority.

More generally, the Federal government should continue to increase the incentives for organizations to implement better cybersecurity. Government should leverage existing regulations where possible to promote good cybersecurity behavior, support and encourage the use of best practices, and drive industries to set standards of care[44] for cybersecurity. Establishing a generally accepted level of cybersecurity for organizations within an industry would remove uncertainty and enable businesses to plan investments, as well as addressing concerns about liability and reduce barriers to collaboration and information sharing. Existing

[41] https://homeland.house.gov/activities/hearings/transportation-cybersecurity-protecting-planes-trains-and-pipelines-from-cyber-threats
[42] https://www.solarium.gov/
[43] https://www.solarium.gov/
[44] https://www.bens.org/file/publications/CyberStandardofCare-101.pdf

efforts such as the National Telecommunications and Information Administration's (NTIA) Software Bill of Materials (SBOM), which provide an inventory of the software components and dependencies in the supply chain, would go a long way in helping organizations understand their risk to newly discovered vulnerabilities.[45] Like the previous recommendations, these efforts would improve the overall cybersecurity of the U.S. private sector against all threats, including the specific threat from Chinese nation state actors.

Conclusion

Cybersecurity is a risk management issue and there are no easy fixes. It requires organizations to look holistically at their business practices and take proper precautions. It requires collaboration across government agencies to properly understand the scope and the scale of the threat and share information effectively so that organizations can properly manage their risk. Most of all, it requires a partnership between the private and public sectors to ensure that the critical infrastructure we all rely on is secure and resilient. The current approach to critical infrastructure cybersecurity is fundamentally correct and we have made great strides over the last two decades, but in practice we do need some tweaks to fully realize its potential.

Likewise, there are no easy solutions to the threat from China's nation state actors in cyberspace and no there is no reason to expect this threat will diminish. China has leveraged stolen intellectual property from Western companies to make great gains in their economic standing. Recent indications suggest they continue to innovate their tactics and target organizations or their service providers to target the information they need to meet their strategic objectives. While the cyber threat from China is not as immediately disruptive as the threat from other nation states, organizations most at risk must continue to improve their defenses.

While these problems are hard, they are not unmanageable. The Federal government must continue to improve internal collaboration among agencies to provide timely, relevant technical and strategic information to the private sector. New organizations like the Office of the National Cyber Director, CISA, and CISA's JCDC will bring a focus on operational collaboration with the private sector that will pay dividends over time. Congress should move forward with cyber incident reporting requirements for critical infrastructure to ensure we understand the scope and scale of the problem and resource it accordingly. Identifying and prioritizing systematically important critical infrastructure will be a key objective for private-public partnership efforts. Smart regulations of critical infrastructure, security certifications for these most important entities, and making it easier for organizations to know what software is included in their information technology are all steps we need to take to shore up our Nation's defenses against malicious cyber actors.

Thank you for the opportunity to discuss these topics and I look forward to your questions.

[45] https://www.ntia.gov/SBOM

PANEL III QUESTION AND ANSWER

CHAIRMAN WONG: Thank you, Dr. Jenkins. And thanks to our other panelists as well. We'll begin the Q&A. We will go in alphabetical order, beginning with my Co-Chair, Commissioner Bartholomew.

COMMISSIONER BARTHOLOMEW: I'm going to pass on this round and drop to the bottom of the list.

CHAIRMAN WONG: Okay. Commissioner Borochoff?

COMMISSIONER BOROCHOFF: Thank you. First, Dr. Segal, it's nice to see you in front of us again and I thank you. And, Dr. Jenkins, the whole subject of power, addressing what you spoke about, is of immense interest to me. I'll be interested in hearing the other questions.

Dr. Schneider, in your written testimony, and you alluded to it a little when you were giving your testimony, you talked about the new cyber command. And there are two things that caught my eye: Defend Forward and Hunt Forward.

And my question is, first, I understand from reading it what they both do, but I don't understand in a practical sense what Hunt Forward is, how aggressive is it, and then do our allies and partners really allow us to do that?

And then, secondly, Defend Forward sounds to me like even more aggressive. And I'm curious if you have any hard examples of how that might work.

DR. SCHNEIDER: Awesome. So, Hunt Forward is basically the idea that we're going to send one of our cyber protection teams   these are kind of our defensive teams   physically often to an ally or a partner country.

And we're going to use the capabilities that are resident within that group of people to help that country find bad guys   Russian, Chinese   on their own networks.

And so, there are examples of these teams for deploying to places in Eastern Europe, for example.

Do nations like this? Yes, they like it. Is it super effective? I think this is really kind of a small hammer at a large problem. I think the true effective Hunt Forward is actually more symbolic.

I mean, there's a real difficulty about saying, I'm partnering with Ukraine, for example, to help with a Russian cyber threat, but there's no visual representation of that.

Like, we don't have aircraft, or tanks or people. That's actually what these teams really provide symbolically. They are human beings that come with a logistical package.

And so, part of it is the actual kind of forward deployment of these troops that provides a symbolic partnership.

This is, I do not think, probably enough. And actually, the vast majority of this cybersecurity work can probably be done remotely. But there's a strong signaling component.

In terms of what Defend Forward is, this has been a real problem. And when you aggregate all the discussion about what Defend Forward is, you realize that there's probably a disagreement within the U.S. military about what Defend Forward is.

For me, if I was in charge for a day, which I'm not, I would conceptualize Defend Forward as counter-cyber operations.

It's using my cyber teams in order to attack the Russian IRA or the PLA. Not attacking tanks necessarily, or taking the command and control, but instead attacking the networks that they use to conduct cyber operations. So, it's more of an intelligence tit-for-tat.

That said, my perception of what Defend Forward is, is not necessarily what it really is. And to be fair, what I've heard in testimonies like these about what Defend Forward is in practice, is a lot more benevolent.

It's sharing information between partners. It's giving information to the public sector. It's sharing relationships with CISA. So, it's actually far more benevolent.

I think we probably actually, and could be if we're not already, perhaps a little more assertive using Defend Forward in more of a counter-cyber role.

COMMISSIONER BOROCHOFF: So, I think you for that. And I would just say that I know there's a strong desire out there to be more aggressive in that area. And I'm aware because I was told by someone who works there that cyber command in San Antonio, they're identifying some three million intrusions a day.

And when I said, what are you doing about it, he said, I can't tell you, but in some cases it's kinetic.

And I said, what does that mean? And then he wouldn't answer me. So, I don't know if that was wishful thinking or real. But your answer was very helpful. Thank you.

CHAIRMAN WONG: Wonderful. Commissioner Cleveland.

COMMISSIONER CLEVELAND: I join my colleagues, and thank you all for testifying. This is a topic that I find often over my head, but you have managed to communicate it with clarity and really been helpful.

I'm interested, Dr. Jenkins, you made the comment that PBD21 defines 16 critical infrastructure sectors, and assigns agencies to serve as managing the day-to-day operations or interface. Given that that flowed from the Patriot Act way back in 2001 when we defined our interests somewhat differently, is there any need to update what are defined as critical sectors? And more importantly, are they the sectors that the Chinese are targeting?

MR. JENKINS: Thank you for your question. So, I believe the definition of critical infrastructure which dates back to the Patriot Act is still adequate and still does a good job of defining what infrastructure we would consider to be critical. If it has an impact on, if losing it, a degradation of it, has an impact on national security, public health and safety, economic security.

That's all pretty solid. In terms of how the critical infrastructure sectors are defined, which goes back to the Obama Administration, PBD, PBD21, those 16 sectors, I think that's in pretty good shape as well.

The gap is in when organizations that own critical infrastructure don't necessarily participate in that sector's structure.

We rely on that as a voluntary partnership. Sometimes the organizations that are in key places in our infrastructure may not be aware that they are in key places in our infrastructure, and therefore don't participate in the critical infrastructure sectors in a robust way to get security information to work with the government to improve their security and resilience.

I believe that's one of the reasons why the Cyberspace Solarium Commission brought up this idea of systematically important critical infrastructure, identifying what that infrastructure is, those key nodes within our infrastructure that are important, then tracking who owns and operates that infrastructure.

And then, the proposal would require them to participate with the federal government in security activities. I think that's really the missing gap in the structure at this point.

COMMISSIONER CLEVELAND: I hate to be an idiot, but could you give me a for-instance that sort of traces what you just described?

MR. JENKINS: Sure. So, the one example I can probably point out that I can't know for certain what their involvement is in their critical infrastructure sector, but a hypothetical would probably be Solar Winds. So, the company, I guess almost a year-and-a-half ago now in 2020, in December 2020, who had a big security incident where Russian actors got into their software development chain, poisoned that, and then when organizations downloaded that software, they downloaded essentially malware.

A lot of people had not heard of Solar Winds before that incident took place. And I do not believe   and I could be corrected on this   but I do not believe that they were actively involved in information technology sector activities within the critical infrastructure sector.

So, that could be an example where an organization that has something that's critical, an operation that's used in a lot of different places that a cyber actor could use as a supply chain entry into other companies, may not be aware of how important they are to the rest of the functioning of the critical sectors around the country.

COMMISSIONER CLEVELAND: Thank you. And would you or anybody else like to comment on when it comes to these 16 sectors, which ones do we understand are Chinese priorities?

MR. JENKINS: From my understanding, I think you can map to the Made-in-China 2025 plan, to see a pretty good example of what they're interested in, things that they're interested in, moving forward on, like information technology, quantum technology, biopharmaceuticals, health care, those kinds of sectors.

And looking through that plan, I did map all of those to the existing sectors, I believe, without much issue or debate.

DR. SEGAL: I would also add that there's been public testimony that suggests that the Chinese hackers have mapped oil pipeline, energy grid, transportation structure, other things for possible disruptive attacks in case of a kinetic conflict.

COMMISSIONER CLEVELAND: And they fall outside the 16 critical sector domain. Is that your point?

DR. SEGAL: No, no. They would fall inside the

COMMISSIONER CLEVELAND: Inside. Okay.

DR. SEGAL: Yeah. Dr. Jenkins' comments I think were mostly about intelligence collection based on strategic technology desires. But we also know that they've mapped critical infrastructure for more disruptive attacks, and they would fall within those 16.

COMMISSIONER CLEVELAND: I'll save for second round, but thank you.

CHAIRMAN WONG: Thank you Commissioner. We'll move to Commissioner Fiedler.

COMMISSIONER FIEDLER: Adam, let me ask. The Chinese haven't sort of abided by many, if any, of the agreements they've made with us. And I don't know if this is cynical or realistic, but that norms will not be established in the cyber world until there's a catastrophic conflict where the principal actors get damaged. That's the incentive, right?

DR. SEGAL: So, yes. There does seem to be a lot of reaction after a destructive attack.

But I think using the nuclear example, which people don't want to use for cyber and I think there are lots of reasons why not to, I think we do want to start pointing out in some shared interests about how we want to prevent worse things happening in a cyber conflict.

So, we're not going to be relying on them abiding because they've accepted the norm. We're going to rely on them abiding because it is in a shared interest that has to do generally about signaling or escalation, or other destructive impacts that we can't control.

COMMISSIONER CLEVELAND: Jeff, you have to unmute.

COMMISSIONER FIEDLER: Let me ask the entire panel. Does anyone know if the U.S. Government has a catalog of stolen intellectual property?

I mean, we've been listening to problems of the theft of intellectual property for 20 years now. Do we have a catalog of that?

DR. SEGAL: So, I once heard that there was a NIC study done on the impact of the theft of commercial secrets. That, I assume would have some I don't know if catalog is the right word but some scoping of the technologies and areas.

But I heard it wasn't particularly good and never really was released. And so, there are just so many issues in trying to measure what the impact of a stolen intellectual property is. I would be very surprised if there's any comprehensive overview.

COMMISSIONER FIEDLER: I'm having trouble unmuting here on my computer.

If we're considering impositions of cost to the Chinese, or, let's say the thieves of intellectual property, or the users of intellectual property, and let's just take commercial or industrial theft of intellectual property, that we should impose costs on those companies that are using the stolen property.

I mean, so what I'm hearing is we complain about it but we don't know who's using it? And therefore, we can't impose any costs? I'm not sure I

DR. SEGAL: So, again, I can't speak to what the intelligence agencies know. I suspect they have a number of cases where they do know. I can only speak to what has been publicly released.

In most of those indictments, they sometimes speak who the actor is. They rarely speak who the beneficiary is.

There were some cases for example, Su Bin, who is a hacker that was based in Canada, who was eventually sent to the United States in that case, it was the C7 and transportation planes that were clear kind of identifiers.

It would probably rely on the U.S. being willing to burn some assets. You have to basically, I think, probably show attribution in greater clarity than we have in the past, and we might decide that it's worth it in those instances.

COMMISSIONER FIEDLER: I would just comment that on a manufacturing basis we could see it. We should be able to see it fairly quickly in the company producing a product that competes, dwarfs, puts out of business, the U.S. company whose property was stolen.

I mean, I don't understand why we haven't imposed those kinds of costs on Chinese companies in their use of stolen intellectual property.

DR. SEGAL: So, most of those known cases are not cyber. Or at least the publicly discussed ones. I think you're right, we do have, for example, American Superconductor, where the software was clearly stolen by an insider. The Chinese customer then developed their own competitor, and then cut their contract with American Superconductor.

But that wasn't a cyber-enabled one. It was an internal threat. So, yes, I think we have a couple of cases. Again, there is a big estimate. The Intellectual Property Commission, out of the National Bureau of Asian Research, does a big number every year.

But it's not broken down by China cyber-enabled. So, I think there are probably threads to be pulled, but there are not many

(Simultaneous speaking.)

COMMISSIONER FIEDLER: I'm sure there are. Okay, thank you very much.

DR. SEGAL: Thank you.

CHAIRMAN WONG: Commissioner Friedberg.

COMMISSIONER FRIEDBERG: Yeah, just to follow up on that. For purposes of imposing costs, I supposed you could say it doesn't really matter whether the theft was cyber-enabled or done in some other way, when you see a product that's identical to an American product.

Maybe you have probable cause to impose some kind of punishment. If we're not doing that, it's not clear to me exactly why.

I had a couple of questions on the defensive aspect of this. And I suppose the biggest question is, what can we say about how well the defenses that have been implemented and improved over time have worked.

And, Dr. Schneider, there's a remarkable line in your testimony, where you say, there's no evidence that either DoD or defense industrial-based networks are less vulnerable than they were four years ago.

Either the strategy or the implementation is not working. Could you say a bit more about that? Because obviously, people are trying pretty hard to make it work.

DR. SCHNEIDER: Yes. And that was an intentionally provocative statement I included. And I think part of the problem is there are almost no measures of effectiveness in general in any of these strategies.

So, it's very difficult to hold the DoD's, for example, feet to the fire, when you have no idea what would constitute success and not-success. It's certainly not in the number of intrusions or the scope of data that's being stolen, because that is actually increasing, not decreasing.

And I think what plagues the Department of Defense and probably the government networks more generally, and Dr. Jenkins can speak to, is that there are very byzantine and arcane practices when it comes to baseline information technology.

So, you are not implementing commercial best-practices. You are using very old network architectures and processes, and then you're putting it through the filter of the budget acquisition process where the services are doing kind of their own things, and then DISA, which is at the joint level, is kind of trained to push enterprise-wide solutions.

And then, the CIO's office is trying to put everything on the cloud, and these things just don't speak to each other.

So, we can invest in cyber protection teams over and over again, but we don't actually have that many cyber protection teams. There's only 133 kind of overall teams, and cyber protection teams are just a small percentage of that.

So, the idea that you're going to use a small percentage of the Cyber Mission Force to defend an architecture that's inherently insecure is a problem.

So, I would say we have not invested enough in defense. But the problem's not really cyber command's fault, it's not the fault of the CPTs, the cyber protection teams, it's the fault of the DoD writ-large, which is not invested in IT and baseline network architecture.

COMMISSIONER FRIEDBERG: Okay. But it would seem, logically, if there is no reliable measure of effectiveness for defensive measures, there's no limit to how much money you could spend.

You could spend every dollar in the federal budget and you wouldn't know whether you were doing better or worse.

So, it would seem like that's an important question to address, what kinds of measures might there be, not only for government, but for private actors.

I had a further question for you, Dr. Schneider, regarding the Defending Forward. And obviously there are limits to how much people on the outside know about what exactly this means and what's going on.

But can you tell us anything about who authorizes such operations? Are there rules of engagement? Is there a chain of command?

We heard earlier that in China there seems to be a highly centralized command system. What is the mechanism by which these attacks are authorized in the U.S.?

DR. SCHNEIDER: Yeah, that's a good question, and there's actually been significant change over the last four years.

So, under the Obama Administration, this was actually highly centralized, even at the executive level. And there were very few offensive campaigns of any kind or color that were not approved at that executive level.

Now, under the Trump Administration, a lot of those authorities were actually delegated down to the component command. I think in this case the Cyber Command, but also potentially some of the geographic commands.

And we've heard about some of these offensive operations that are tied to joint task forces. So, some of these Defend Forward operations are part and parcel of joint task forces, for example, against election disinformation.

So, these are occurring at a much lower level. Not down at the operational or tactical level, but definitely held at the functional, or geographic, command level.

CHAIRMAN WONG: Thank you. Commissioner Glas.

VICE CHAIR GLAS: Thank you all for your testimony. I'm going to pass.

CHAIRMAN WONG: We will move to Commissioner Schriver.

COMMISSIONER SCHRIVER: Thank you. And thank you to the witnesses for your
testimony and really expert views. It's really fascinating discussion.

Dr. Segal, I want to just pick out one of your recommendations, because and this is maybe because I bear some scars from something I think is very analogous.

You talked about operator-to-operator dialogue and the potential value of that. And my previous scars, as I said, we tried for years, decades, when it came to maritime security and safety. What we really need is operator-to-operator dialogue.

We need shift drivers to talk to shift drivers. Talk about rules of the road and safety. And of course, we could rarely get it. And when we did, they were so closely supervised by a foreign affairs bureau, senior officers, that they make their scripted opening statements, and then stand down for the rest of the event.

In any event, I just was curious on your recommendation, why you think those could be of value, and why it wouldn't follow form with other attempts to get, quote unquote, the real operators together, which we never seem to be able to do where the PLA is concerned?

DR. SEGAL: Yeah, I feel your pain and I thank you for your service doing it. I included the recommendation with the expectation that it would probably fail.

I think, quite honestly, I had my RA start to put together all of the work done on mil-to-mil discussions during the last 20 years, and all of the barriers that were faced. And several of them were probably written by you. I didn't include the entire footnote because it was so large.

But I think we would probably face the same issue: that the Chinese would either send the wrong people, or not be particularly forthcoming.

But I do think, given the risk, we would want to signal how important it is to us. I think we should be willing to walk away.

Dr. Schneider mentioned that there was this kind of pivot in Chinese thinking around 2013, 2014, where they stopped thinking of us as being so much more vulnerable than they are to these cyberattacks, and we really haven't had any follow-up discussions since that time.

So, perhaps the environment has changed. So, I would be optimistic that maybe we could take advantage of that.

COMMISSIONER SCHRIVER: I appreciate the candid answer there. I want to make just a comment about cost imposition, see if there's any reaction to it.

I think at times we look at cost imposition and we think it has to be on point. You know, cyber for cyber, or very directed at participants in the original maligned behavior.

When we looked at South China Sea incursions, we say, well, the land reclamation, let's target the cement companies that help to build out the islets.

And then we said, no, let's just take them out of RIMPAC. And I think sometimes cost imposition, we need to broaden the understanding of that and not think it's got to be on point, or a cyber problem has to be met with cyber means.

And so, if we broaden out the notion of cost imposition, do you think there are ways we could actually get at curtailing some of this behavior? Or do they just absorb it all?

Because none of these PLA officers are going to face the inside of a U.S. courtroom, as one of the witnesses observed. And a lot of these organizations can melt away and re-form.

Should be broaden the scope of how we think of cost imposition? Would that have any chance of success?

And I realize I'm just throwing out a concept and asking for reaction. So, if anybody has a reaction to that among the panelists, I'd appreciate it.

DR. SCHNEIDER: So, I would agree. I sympathize with concern that a focus on tit-for-tat is unimaginative. I think in general, policymakers really want to do cyber tit-for-tat, and then finding themselves left with very few tools.

Especially, I mean, if you go back to Sony, for example, what is the U.S. going to do in a tit-for-tat? They're going to attack North Korean film? Like, this is ridiculous.

So, I completely agree that we need to have options that are beyond tit-for-tat. What those options are, that has been a struggle for us in terms of imagination.

I think that most people view responses in the economic domain being proportional, at least, to cyber.

But once again, we struggle with linking some of those economic measures with demonstrated changes in cyberspace.

CHAIRMAN WONG: Thank you. We're going to move to Commissioner Scissors.

COMMISSIONER SCISSORS: Thanks. I appreciated Adam's comment about beneficiaries, and also Jeff's skepticism about our ability to get information on them. It's something I've been involved in for about eight years, off and on, with the U.S. government.

There are a number of reasons why we don't focus on beneficiaries. And when we do, we don't have good information.

And I just think there's a very partial, but nonetheless a solution, that would improve things, which is we need to change the incentives for companies, so that it is easier for them to get retaliatory measures imposed against the companies that are benefitting from cybertheft.

We have one big case and example here involving U.S. Steel, where it just turned into a nightmare, the level of proof demanded in U.S. courts was not achievable. Or, if it was achievable, the people who could achieve it wouldn't disclose it, because it would burn U.S. resources.

So, one way to increase the resources available to the U.S. not the U.S. government necessarily, but to the U.S. is to have American companies think, if I find out who benefitted from this cyberattack on my systems, I'm actually going to get a policy response.

And we have the ability, Congress has the ability to make it easier for that to happen. I don't want to spend a lot of time going into detail about that, but it is possible that we can make it easier and give the American government a broader range of options.

It would require legal changes, because our court system seems to think that the Chinese are legitimate actors in all cases, which of course is not true.

Rant over. Question, Dr. Jenkins. If I understood your written testimony correctly, you implied a tradeoff between crisis/wartime cyber and conventional competition cyber for the U.S.

Are you able to talk at all about how the Chinese determine how to deal with this tradeoff? That you can't prepare for everything. There are two different general domains here.

There's a tradeoff to the United States, there's obviously a tradeoff from China. Can you talk a little bit about how the Chinese face that tradeoff?

MR. JENKINS: I'm not sure. That's not really background. Or I may be misunderstanding your question.

I think from the private sector's perspective, there's a limitation to what they can do from a defensive perspective with the resources that they have available to it.

Of course, they could apply more resources to it and get closer and closer and closer to perfect, but nothing's going to get them all the way. They're going to get to a point of diminishing returns at some point.

So, essentially, organizations have to look at themselves and say, what do I do? What's my role in the economy? Am I a target of Chinese intellectual property theft? And then, let me understand what the threat is from the Chinese and adapt my defense in a way that makes it harder for the Chinese to get into my network.

COMMISSIONER SCISSORS: Sorry to interrupt. I think you confused my rant with my question, which is my fault.

The question is not about   the rant involves making it easier for corporations to respond. But the question is about government. So the U.S., in terms of allocating resources, if I understood your testimony correctly, we have a tradeoff between, are we going to compare for a crisis and maybe verging on war, or are we going to compare for the more convention space where there's a lot of cyber activity?

If that's accurate, the Chinese obviously face the same tradeoff. And so, I'm asking about how the Chinese Government sees that basic tradeoff, insofar as you know. That they would emphasize one or the other, or they're going to try to resource their way through both. Whatever their view of the basic tradeoff is.

MR. JENKINS: Yeah, I'm sorry. I don't have much insight into the thinking on what the Chinese Government could do.

I will say, from the U.S. government perspective, there is always a balance in what crisis is on the horizon, where we're going to focus critical infrastructure owners and operators on defending against that.

So, obviously today and for the last few weeks, the U.S. government's focus has been on getting critical infrastructure to pay attention to potential threat from Russian actors.

So, any threat from Chinese actors is falling to the wayside over the last few weeks, at least in terms of U.S. communication to critical infrastructure owners and operators.

So, there's a little bit of a resource limitation on the U.S. government side from that perspective.

DR. SCHNEIDER: If you don't mind, I would say that China does not have some of the mass problems that the U.S. does. So, U.S. has a very limited amount of resources to devote to offensive cyber. We focused on highly specialized expert teams.

The Chinese have an estimate of up to 50,000 hackers. That's just the quantity.

(No audible response.)

DR. SCHNEIDER: It sure does.

COMMISSIONER SCISSORS: Absolutely.

DR. SCHNEIDER: And while military targets are very, very difficult and you need better and more expertise, the sheer number of potential hackers that they have means that they might not have to make as much of these choices as the United States does.

There's also, we have to delegate responsibility. We have laws about who can do what in the United States, between Title 10 and Title 50, and Title 32.

I'm not a China expert. To my knowledge though, that does not translate in the PLA.

COMMISSIONER SCISSORS: Thank you.

DR. SEGAL: I would just add that looking at the urgency that China has been acting domestically since 2017   let's say since Xi first said that national security is cybersecurity, and Cybersecurity Law, the Data Protection Law, the PIPL, the building out of the CAC's regulatory impacts, all of the things that earlier panels talked about, about regulating hackers and interactions with the MSS   all of that suggests to me that they are worried on both fronts, both a destructive and disruptive attack and something that would be coercive, and more broadly, the whole range of cyber threats.

CHAIRMAN WONG: We'll move to Commissioner Wessel.

COMMISSIONER WESSEL: Thank you all for your testimony today. I'd like to go to supply chain issues. And over the years, some of us on the Commission have looked deeply into that and at one point found out that the DFAR did not allow procurement officers to look at the country sourcing products in terms of their procurement decisions, unless it was for a munitions list item.

So, a Bradley fighting vehicle, etc., we determined that Lenovo computers, which at that point had been identified as having some risks, were being purchased up at Tobyhanna, which was our C4ISR equipment depot.

Fast-forward to a couple of years ago, I think it was 2019, the DoD Inspector General identified tens of millions of dollars of procurement of Chinese-sourced items again, including Lenovo and otherwise where there were beaconing allegations in the past, etc.

It seems to be we have an electronic hygiene problem, in addition to a question about doctrine and intent, that we're enhancing Chinese capabilities through potentially ill-advised sourcing and procurement decisions.

If the witnesses could give us any thoughts they have on that and whether enough attention is being given to sort of the fox-in-the-henhouse issue. Adam?

DR. SEGAL: Yes, there is definitely the vulnerability and threat. I can't remember when it was. The Defense Science Board did a study as well of sourcing of chips and how many of them were counterfeit and sourced in China, or other places that they shouldn't have. So, I think clearly a threat.

I guess my feeling about these things right now are that those types of attacks are actually pretty difficult. The MSS would have to be pretty certain that it could guarantee that the device ended up someplace that it wanted it to be.

And they're getting in so easily in all the other ways, that I don't see that as being a huge threat compared to spear phishing and all the other things. Finding vulnerabilities in supply chain through software, as opposed to making sure that the device is in a place that they want to be.

So, I think it is a risk. I think it's definitely a long-term threat and there clearly are going to be vulnerabilities.

I just think, given their ability to enter through all the other ways we know about, it's probably not heavily relied on.

DR. SCHNEIDER: So, I would disagree a little bit with Dr. Segal. And I think it's because we're coming at it from slightly different perspectives.

I think that for the Department of Defense a supply chain vulnerability is the worst possible vulnerability. It's actually extremely difficult to attack individual weapons systems with cyber, partly because we have relatively archaic software within these systems. Right?

So, all these methods that the Chinese use to get into kind of modern infrastructure are actually relatively difficult for U.S. weapons, since we're talking a lot of '90s technology.

What is more concerning, and this is what would keep me up at night, is if we have inadvertently allowed for a supply chain vulnerability within like an avionics suite of an entire fleet of a type of aircraft.

That's extremely difficult to deal with. And that's the kismet. That is the vulnerability you want as a military. I mean, those are the types of investments that only really great State actors can make.

So, for me, if I was most concerned about threat vulnerabilities, I would be very concerned about supply chain vulnerabilities within, specifically, the U.S. Strategic Force.

COMMISSIONER WESSEL: Neil, any thoughts?

MR. JENKINS: I think I fall somewhere in between my two panelists on this. I think organizations within critical infrastructure are constantly dealing with supply chain issues not necessarily knowing where their products that they buy and that are a part of their infrastructure necessarily come from, where they're sourced from.

There are mitigations you can take to try and correct that. If you're buying things that may be on a watch list or something that you would be concerned about, you should be finding ways to mitigate, or cordon those off from important parts of your network.

You may not want the Lenovo laptops, for example, to be connected to your backup systems, for example.

There are other things and other mitigations that can be in place, like software build materials, to have a better understanding of what software and what pieces of equipment are in your infrastructure, so that if you do find out that there's a danger there, you can take care of them easily.

But I think at the end of the day it's a risk, but it's a very difficult risk to completely and totally understand and mitigate.

COMMISSIONER WESSEL: Thank you. There is another round, I have other questions. Thank you.

CHAIRMAN WONG: Well, we'll definitely have another round. So, now it's to me. My question is for Dr. Schneider. I was taking note of the part of your written testimony on how the U.S. military has trouble attracting and retaining cyber talent.

And I'm just curious, what are the drivers behind that difficulty? Is it simply that we don't pay enough money? Is there not a culture of military service among engineers and developers? Is it we have a recruitment process that's ill-fitted to this community? Is it lack of promotion possibilities if you are a cyber operator? I'm just curious what are the drivers?

DR. SCHNEIDER: I mean it's, unfortunately, a mixture of all of the above. Right? Some of these are cultural issues

Each one of the services, for example, has a different physical fitness component. Not all of our best cybersecurity folks are actually able to meet some of those physical fitness requirements.

And, anecdotally, when I was an intelligence commander, I unfortunately had to lose some of my most talented SIGINT professionals, because they couldn't pass the Air Force fitness test.

So, there are some cultural phenomena. Also, the services are not necessarily set up for this as its own, what you would call an MOS, a military kind of identifier.

And so, each one of the Armed Services is experimenting with, well what do we call these people? Are they information operators? Are they cyberspace operators?

And then, there is a problem with the enlisted officer divide, a lot of the really high talent.

So, let's say I'm an executive director at JP Morgan Chase and I want to hire the best cybersecurity people.

They're not 18-year-olds that are kind of prodigies. These are generally people with master's degrees, PhDs from top universities from all over the world.

So, am I going to take that person, and then like throw them into an enlisted corps? Are they going to start as a lieutenant?

I mean, there is kind of and this has always been a problem about a lack of convergence between the way the military thinks about talent and the way talent is used in the civilian side.

It's also just really difficult to bring people into the military these days, whether it's because of, have they smoked pot before?

Do they have too many foreign relatives or foreign friends? It's very difficult to get people through the security clearance process now.

And, okay, we say we want to bring you in, and then you have to wait one to two to three years to get through the security clearance to actually be commissioned.

These are all deterrents. And then, another deterrent is that a lot of the cybersecurity, if it's offensive cyber, that's really cool and sexy and fun.

But if you're working on defensive cybersecurity in the United States, you are like a decade behind what's happening in industry. So, you're not being challenged with new tools and new skill sets.

You're having to learn, how do I pledge together what is the DoDIN the Department of Defense Information Network? And that's a very different type of skill set than what we're seeing of your coming out of Google, for example.

CHAIRMAN WONG: So, we've had prior testimony earlier today about the efforts that the Chinese have made to reorganize their cyber personnel.

The implication I'm hearing from you and from the prior testimony, is that they've done a better job than us at reorienting their personnel structure to prosecute cyber?

DR. SCHNEIDER: I mean, this may be true. I think we focused on very, very we've focused on fitting cyber within the realms of how we already understand military talent.

And part of that is because of the way we do authorities. I can't use my smart civilian that works at NSA to conduct an offensive cyber operation, because these are different authorities. You know, Title 10 versus Title 50.

So, we actually have an extraordinary civilian base that we can draw from within the United States. But that civilian base cannot work on a variety of different operations.

I mean, we can talk for hours about the problems with the civilian workforce and how difficult it is to bring the civilian workforce in, despite a series of Congressional changes to how we hire people in Department of Defense.

So, the military has very unique problems to bringing in talent. The civilian workforce also has problems.

CHAIRMAN WONG: Thank you. We'll now move back to Commissioner Bartholomew, if you have a question.

COMMISSIONER BARTHOLOMEW: Yes, a couple of them. One is I should know the answers to this one but I don't are the people that the Department of Justice has indicted, are they placed on Interpol's Red Notice list?

DR. SEGAL: I don't know.

COMMISSIONER BARTHOLOMEW: It was just as I was listening to, I just thought, well, right. If you're not on some sort of list like that, then what are essentially the sanctions against you?

All right then, I'll switch gears. I was very interested, Dr. Jenkins, in how you were talking about the private sector working together with government to address some of these issues. And I noticed that you said you can make sure that the information that they share is not FOIAble, or anything like that.

But my question there is, how do you manage the fact that a collaboration might have competitors together, and they might see a vulnerability in somebody else's system as a competitive advantage for them? How do you manage that kind of dynamic?

MR. JENKINS: Yes, thank you. So, there are a couple of ways to handle this. I think one of the most promising ways that doesn't require any kind of legislation or regulation, is just that cybersecurity people, whether they be in the private sector or in the government, really have an ethos of sharing and getting stuff to each other and working together.

That's changed a lot over the last decade, especially within the private sector. We were in an area where everybody's information was closely held. The intelligence that they had was closely held.

But over time we've gotten to a point where companies in the private sector that do cybersecurity understand that what they see, they see because they're on a specific set of networks. They see their slice of the environment.

And the only way they can see a broader slice of the environment is by sharing more information. So, you see that in public reporting, you see that in blogs coming out, you see that in sharing communities, like the one I work with at the Cyber Threat Alliance, you see that in closed sharing communities, where communities get together.

Legislatively, the Cybersecurity and Information Act of 2015 also put in place protections for antitrust. So, if organizations are sharing information on technical indicators or defensive measures for cybersecurity purposes, that can't be used for antitrust issues.

So, while your specific example of talking about vulnerabilities may not fit into that and may be something that is of concern, when companies get together and talk about the indicators that they're seeing and the defensive measures that they're putting into place, they shouldn't be concerned about that infringing on any kind of antitrust or triggering any kind of antitrust concerns.

COMMISSIONER BARTHOLOMEW: Thank you. That still doesn't get to the fact that they might be providing information that gives somebody else a competitive advantage, right? It's just the nature of the business that we have here.

I'm also, like several of my colleagues, really struggling with this idea of imposition of costs and what we can actually do that would dissuade the Chinese government from doing the activities that it's doing.

When I think about commercial espionage, for example, by the time we figured out sometimes the theft of trade secrets, the damage has already been done.

On things like biotechnology, they're avoiding having to pay R&D costs by stealing the R&D that has been done by our companies, sometimes underwritten by the federal government.

So, I just really am, like Randy I guess, really struggling with, what kind of imposition of costs do we have that would dissuade them from even trying to do this?

Otherwise, it's what the proverbial shutting the barn door after the horse has gotten out. Anyone?

(Simultaneous speaking.)

DR. SEGAL: I don't think we're ever going to dissuade them. Sorry.

DR. SCHNEIDER: No, go ahead.

DR. SEGAL: Sorry, Jackie.

DR. SCHNEIDER: Well, I would venture to say that we focus too much about dissuading or deterring, and not enough about degrading.

Cost imposition is important, but we in the United States sometimes forget just making things harder is also good. And there has not been a lot of investment in making it harder for the Chinese to be successful.

And I don't mean that like, I want to change your behavior. I mean, let's just make it harder. And those are investments in defense, in resiliency and in counter-cyber operations.

COMMISSIONER BARTHOLOMEW: Dr. Segal?

DR. SEGAL: Yes. So, I mean, clearly we have a tool to inflict pain on China. If we look at Huawei and semiconductor controls, we have done significant damage to Huawei.

So, I think it is possible at a pace. But I basically agree with Dr. Schneider's points, which I think is, given the vast benefit that China has taken from this, there's no way we can do it at scale to truly impose enough cost.

And so, then we're really talking about degrading, either through disruption of the operations, or just making it so much harder for them to actually steal the material.

COMMISSIONER BARTHOLOMEW: Great. Thank you.

CHAIRMAN WONG: Now, we're going to move into our second round of questioning. I think Commissioner Wessel was the one who explicitly asked for it, so I will start with him.

COMMISSIONER WESSEL: Thank you, Mr. Chair. I want to briefly tag the issue that Derek had raised earlier, about U.S. Steel and what was the Section 337 case which is before the International Trade Commission that gives authority to actually confiscate goods produced through the violation of intellectual property rights at the border.

So, it's a rather effective mechanism when it's allowed to operate. The problem in that case was that the original information was obtained through law enforcement and intelligence sources, and our legal system limits the ability of taking that information and applying it in another judicial setting.

If our witnesses could provide any thoughts about that, that'd be helpful. It may be something we want to look at, but that really created a tremendous problem.

And when we look at attribution sets and other issues we've raised today, and how proof of IP violations might be obtained, if we can never apply them in a commercial setting on behalf of a U.S. company, the effectiveness of our mechanisms may be diminished. Thoughts? Adam or others?

DR. SEGAL: So, yeah, I'm not familiar with the specific legalities of it, but it strikes me that either the question is, perhaps, closer cooperation with some of the private sector firms, who then can release the data without the same regards over the intel problem in separate jurisdictions, but I think there is the balance that I think was raised in Adam Kozy's testimony earlier about the costs and benefits of attribution.

And so, are we burning some techniques that are incredibly useful for other reasons for the pursuit of these commercial court cases? That I think would probably have to be made on a case-by-case decision.

COMMISSIONER WESSEL: Okay. That may be something that we want to look into more. Separately, with the Putin/Xi meeting recently and what we all have seen publicly as to Russian capabilities, do any of the witnesses have thoughts about what China may be learning from Russia?

Are you aware of any cooperative cyber training, cyber sharing of techniques, mechanisms, tools, etc.?

DR. SEGAL: So everything in the public domain, so in 2015 if I remember correctly, China and Russia signed what everybody called the Non-Aggression Pact in Cyberspace. And then, the Chinese turned around and started hacking Russian defense industries.

So, it was not a non-hacking pact. But most of the public evidence on cooperation, after that agreement, has been about information and Internet control, so helping the Russians build out their version of The Great Firewall.

There has been, I think, some learning came up earlier on information operations, but the Chinese have not adopted Russian methods. But I think they have learned by watching.

I would be very surprised if we would see very close cooperation on the offensive or the intelligence side on cyber between China and Russia, just given the lack of trust between the two intelligence agencies, and the fact that they both continue hacking each other. So, I would suspect to see it mainly in Internet control areas.

COMMISSIONER WESSEL: Other witnesses' thoughts?

MR. JENKINS: I would just add, I think that Dr. Segal's right. I think most of the learning that we've seen from the Chinese, in terms of what the Russians are doing, has been in the information operations space, trying to influence various politics in other countries.

And I would note too that from recent reporting, it's pretty clear that any kind of pact that they have may not be foolproof. There's been some instances of some ransomware from people in Russian space affecting Chinese businesses. So, they're not exactly best friends in terms of cyber activities.

COMMISSIONER WESSEL: Thank you.

CHAIRMAN WONG: Are there any other Commissioners with a second set of questions? Aaron? I see your hand there.

COMMISSIONER FRIEDBERG: Thank you. This is a question for Dr. Jenkins, or two questions.

If I understood you correctly, the recommendation in the Cyber Solarium Report is that critical industries and critical infrastructure have to demonstrate, or to propose that they need to demonstrate, that they've achieved a certain level of cybersecurity. Is that correct?

MR. JENKINS: So, yes, that recommendation is specific to the systematically important critical infrastructure.

So, identifying what infrastructure is the most important of our critical infrastructure, then taking the organizations that own that infrastructure and requiring them to essentially work in the private-public partnership.

As a part of that requirement, the proposal would give them some extra liability protection. It would ensure that the U.S. Government is providing them with additional assistance.

That could come from instant response teams, it could come from threat-hunting teams, from any of the various agencies. And in exchange for those carrots, the stick would be they have to certify their security on a routine basis, to ensure that they're doing everything that they can to protect their network. So, that would be the idea of the tradeoff there.

COMMISSIONER FRIEDBERG: And is there some mechanism through which the government would audit or assess whether in fact these companies were doing enough?

MR. JENKINS: Yes, there would have to be that. It's not clear from the Solarium Report exactly what they see that regulatory regime looking like. We would want to make sure that it's not simply a compliance regime where they're just checking a bunch of boxes.

We would want to make sure that there are some other things in place, like allowing U.S. government systems to at least scan their Internet-facing systems for vulnerabilities, those kinds of things in place so it's not just a compliance regime.

But those are things that would need to be worked out in the legislation.

COMMISSIONER FRIEDBERG: And do you know what the status of the legislation for implementing that proposal is at this point?

MR. JENKINS: I believe that the Solarium provided a draft legislation or a legislative proposal for that, but I'm not exactly sure where that stands in terms of implementation.

COMMISSIONER FRIEDBERG: Do you know if there are any proposals for doing something that would be less rigorous but perhaps broader, either requiring or allowing companies in a whole array of sectors to demonstrate, to go through some process by which they would demonstrate the adequacy of their cyber defenses, and perhaps receiving some kind of benefit for doing that, whether it's a tax break or some change in their liability? Is there any thought of doing that on a broader basis?

MR. JENKINS: I believe some of the closest things to what you're referring to now would be in some of the industries that are already regulated within the U.S., and then we're looking at attaching additional cybersecurity-specific regulations to them.

I think what immediately comes to mind would be the oil and natural gas companies, TSA – Transportation Security Administration which is their sector risk management agency. They have recently provided additional guidelines and requirements that oil and natural gas companies and pipeline companies have to follow.

And so, those types of security requirements in those types of sectors, that's where we're seeing that most right now.

COMMISSIONER FRIEDBERG: Thank you.

CHAIRMAN WONG: Any other Commissioners with another round of questions? Well, seeing none, I think we can close up shop a couple of minutes early.

But I want to thank this panel and all of our other panelists today for some very good testimony, very good recommendations. We have a lot to think about in an area with great and growing import for our national security, our economic competitiveness, and a lot of recommendations for us to consider for our report to Congress at the end of the year.

Our next hearing is March 17, where we will discuss and consider China's energy policies. But until then, we are adjourned for today. Thank you.

(Whereupon, the above-entitled matter went off the record at 2:45 p.m.)