COUNCIL on FOREIGN RELATIONS

September 24, 2024

SFS | GEORGETOWN UNIVERSITY Walsh School of Foreign Service

China's New National Security Laws: Risks to American Companies and Conflicts of Interest

Prepared statement by
Dr. Rush Doshi
C.V. Starr Senior Fellow and Director of the China Strategy Initiative, Council on Foreign Relations
Assistant Professor of Security Studies, Georgetown University Walsh School of Foreign Service

Before the
U.S. Senate Committee on Homeland Security and Governmental Affairs
United States Senate
2nd Session, *118th* Congress

Hearing on "Safeguarding the Homeland: Examining Conflicts of Interest in Federal Contracting to Protect America's Future"

Chairman Peters, Ranking Member Paul, distinguished members of the Committee, thank you very much for the opportunity to testify at today's hearing on conflicts of interest in federal contracting.

My remarks will focus on a few items. First, I will discuss how the People's Republic of China's (PRC) geopolitical ambitions and leverage over U.S. companies in the PRC – gained through threatening market access and through a new regime of national security laws – create conflicts of interest. Second, I will discuss how these conflicts might play out in specific sectors, namely the consulting industry. Third, I will examine conflicts in the technology sector given risks to U.S. data, critical infrastructure, and government networks. Fourth, I will offer a few recommendations for U.S. policy to help firms resist PRC pressure and avoid conflicts of interest.

I. The PRC's Geopolitical Ambitions, Leverage over U.S. Companies, and Conflicts of Interest

The PRC uses a variety of forms of leverage, including threats to withhold market access and national security legislation, to pressure U.S. companies to advance PRC objectives. Accordingly, U.S. companies operating in the PRC face a challenging environment that can exacerbate conflicts of interest, particularly

for those companies that might contract with the U.S. government, handle sensitive U.S. government data, or operate sensitive platforms upon which the U.S. government relies.

PRC Objectives

The PRC leadership seeks to restore China to its past position of preeminence, and accordingly, has developed a grand strategy coordinated across multiple instruments of statecraft to displace U.S.-led order. As I argue in *The Long Game: China's Grand Strategy to Displace American Order,* the PRC leadership has made clear its intent to "catch up and surpass" the U.S. technologically; to reduce dependence on the West and increase global dependence on China economically (part of a policy it calls "dual circulation" [双循环]); to be able to defeat U.S. forces in a regional clash militarily while building a global power projection capability; and to reset global norms politically.[1]

Intention must be matched by capability to be taken seriously. On that metric, the PRC is the first U.S. competitor to surpass 70% of U.S. GDP. It is already the world's leading industrial power and exceeds U.S. capability in certain technology sectors, including some military sectors. It fields military forces that some experts believe could defeat the United States in regional conflict. It has also mounted aggressive efforts to develop accesses on U.S. critical infrastructure. Accordingly, the United States faces a situation many believe resembles a new Cold War but from a position that is more tenuous than against past competitors.

A key difference between this competition and the Cold War, however, is that U.S. companies are deeply involved in the PRC economy. In some sectors, and particularly for companies that also work closely with the U.S. government, that activity creates the possibility of conflicts of interest. This is especially true considering (1) PRC threats to deny market access and (2) the PRC's security-focused regulatory regime.

Weaponizing Market Access

An enduring source of PRC leverage over U.S. companies has been access to the PRC market. The promise of market access, and the explicit or implicit threat to withhold it, is a tool the PRC uses to advance various state objectives. For Beijing, these objectives include gaining access to technology, know-how, data, sensitive U.S. government information, or compliance with PRC political positions, among others.

PRC threats to withhold market access have led U.S. companies to take steps that are contrary to their own long-term interests, and at times, to U.S. national interests. The PRC has successfully pressured U.S. companies to transfer intellectual property to China, to engage in joint ventures that ultimately boost PRC capability, to increase investment in China at the expense of the United States or other locations, and even to refrain from complaining about these pressure tactics. PRC officials have directly told U.S. companies in some cases to transfer intellectual property in order to receive market access. In other cases, joint venture partners have stolen intellectual property from U.S. companies and set up their own competitive ventures while trapping the U.S. partner in a now defunct joint venture. Sometimes, when foreign companies have sought recourse for intellectual property theft in foreign courts, they have been punished in China's market through judicial action.

In addition to facing threats to market access, U.S. companies operating in the PRC can also be subject to a variety of other legal and even personal threats. Many companies can be tied up by PRC regulatory actions or costly litigation to coerce acquiescence on items important to the PRC. Foreign executives have sometimes been prohibited from leaving the country under "exit bans." If a court sides with a local

company's litigation against a foreign company, which could occur in a secret hearing, an executive could be "trapped" in the PRC without much notice or resource.

The PRC's credible implicit or explicit threats to withhold market access – or to target the safety of executives – can create conflicts of interest for U.S. firms. The payoff from complying with the PRC's conditions or demands, however, continues to fall. American companies are increasingly vocal about the fact that complying with the PRC's conditions is no guarantee of consistent market access, and the PRC's long game is to replace foreign firms and businesses with PRC alternatives.

New National Security Laws

Second, in addition to restrictions on market access, the PRC's expansive set of new national security laws creates another source of challenges – and conflicts of interest – for the operations of U.S. companies in China. Under this legal regime, the Party can (1) insert Party cells into foreign-owned companies; (2) compel PRC entities and individuals to cooperate with the PRC's intelligence services and keep the fact of that cooperation secret; and (3) access the data of foreign companies.

I'll now turn to discuss each of these three challenges.

1. **Conflicts of Interest from Party Cells in Chinese and Foreign-Owned Companies:** PRC laws, notably the 1993 Company Law, require PRC companies to establish and maintain Chinese Communist Party (CCP) cells. The purpose of a CCP cell is to better align the activities of the company with the PRC's objectives. More than 90% of the PRC's top 500 enterprises have Party cells, according to data from a Party-led body.[2] In 2020, the PRC issued guidelines clarifying the roles of CCP cells. These guidelines indicated that Party cells should play a role in corporate governance, strategic decision-making, and personnel management, and that they could work to revise corporate charters to recognize the leading role of the CCP.[3] Members of Party cells sometimes sit on boards, and boards sometimes consult with Party cells on major decisions. Since 2016, the PRC has increasingly pushed subsidiaries of foreign-owned companies to establish Party cells. The PRC released new requirements in 2018 and 2022 that call for foreign joint ventures that are publicly listed to open Party cells as well as certain foreign-owned financial institutions.[4] HSBC Holdings, for example, set up a CCP cell in 2022 in its investment banking subsidiary in China, with executives reportedly concerned about the optics of potentially exposing strategic decisions and client data to the CCP.[5] "Big Four" accounting firm EY created a CCP cell as well which later required its members to wear Chinese Communist Party badges.[6] Mercedes-Benz reportedly has a party cell in its Chinese joint venture which is involved in management meetings.[7] Most firms do not want to host a Chinese Communist Party cell, but as FBI Director Chris Wray noted in testimony last year, "The CEOs I've talked to are afraid to say something."[8]

2. **Conflicts of Interest from New Laws Mandating Cooperation with PRC Intelligence Agencies**: Several PRC laws force Chinese individuals and entities, including subsidiaries of U.S. companies, to cooperate with PRC intelligence agencies. For example, the 2017 National Intelligence Law (Article 7 and 14) requires Chinese individuals and entities, including subsidiaries of U.S. companies in China, to affirmatively support PRC national intelligence work, comply with demands from PRC intelligence and law enforcement agencies, and "keep the secrets of national intelligence work from becoming public."[9] The Department of Homeland Security warns companies that, under this law, the PRC could require a PRC entity to provide data from a U.S. person or business or compel a company to install backdoors in equipment.[10] The 2021 Counterespionage Law similarly mandates that Chinese nationals cooperate with national security

agencies. It also requires businesses, universities, and other organizations to cooperate with PRC intelligence services to monitor Chinese citizens with access to sensitive information when they travel overseas and to train them in counterespionage.

3. **Conflicts of Interest from New Laws That Allow PRC Access to Networks, Encryption Keys, and Data**: Other pieces of legislation put onerous restrictions on data transfer and provide the PRC access to networks, encryption keys, and data. For example, the 2017 Cybersecurity Law requires that data in undefined critical industries be stored in China and that PRC public security and intelligence agencies be able to conduct spot checks of networks, which could include access to data. The PRC's Cyberspace Administration of China (CAC) can launch "cybersecurity reviews" of U.S. companies at any time to demand virtually anything from data to source code from the targeted company.[11] Regulations issued in 2021 also force companies in China, including foreign companies, to report software vulnerabilities to the PRC government before informing anyone else – allowing the PRC to stockpile these vulnerabilities for offensive advantage.[12] Similarly, the 2020 Encryption Law's Article 31 requires the State Cryptographic Administration (SCA) to have access to commercial cryptography systems for certification purposes, which could allow SCA access to decryption keys and passwords, according to the Department of Homeland Security.[13] In practice, most firms will use PRC-certified encryption rather than compromise the encryption they may rely on in their home markets. While this practice may seem sophisticated, the reality is that it will not provide protection against the PRC government.[14] Encryption aside, the 2021 Data Security Law mandates that any company processing important data is subject to a periodic security review by Chinese officials. It also prohibits the release of any data to a foreign judicial or law enforcement agency – which has at times been interpreted to apply to administrative agencies – without PRC government approval, regardless of where the data originated from. This provision could complicate compliance with a subpoena or regulatory action. The 2023 update to the Counterespionage Law widens covered information beyond "state secrets and intelligence" to include "documents, data, materials or items related to national security and interests." This broad definition creates a legal foundation to gather data from foreign firms and their employees with little justification. It also includes authority to inspect their electronic devices. Additionally, a 2024 update to the state secrets law introduced a new, nebulous concept called "work secrets" defined as information that is not a state secret but "will cause certain adverse effects if leaked.' This could apply to anything the Party-state decides could cause "adverse effects" if leaked.

Implications of Conflicts of Interest

As FBI Director Chris Wray told this committee in 2019, "Chinese law essentially compels Chinese companies and typically compels U.S. companies that are operating in China to have relationships with different kinds of Chinese companies to provide whatever information the government wants whenever it wants."[15] Since 2019, the situation has only deteriorated.

PRC leverage over U.S. companies can undermine U.S. interests and national security in several distinct ways. U.S. companies could (1) inadvertently act as vectors for the PRC to access sensitive information, data, intellectual property, etc.; (2) be caught between mutually exclusive U.S. and PRC demands; and (3) could, in some cases, seek to profit from conflicts.

1. **Vectors for the PRC to Access Sensitive Information:** U.S. companies may inadvertently act as vectors for the PRC government to access U.S. intellectual property, trade secrets, sensitive data, or sensitive networks. Such transfer could occur through the actions of Party cells within U.S. subsidiaries or their partners. It could occur through laws that compel a U.S. subsidiary, employee,

or PRC private sector partner to comply with requests from the PRC intelligence service. It could also occur through the ability of law enforcement and other bodies to outright inspect or seize data as well as their ability to bypass encryption due to the requirement for commercial encryption to be registered with PRC regulators. As a practical matter, this means that sensitive data stored by a U.S. company could be transferred to the PRC without the company's knowledge. It also could mean that, for example, U.S. companies providing cloud services in China with even the very best protections could inadvertently provide access or information relevant for facilitating PRC cyber attack to their local PRC operators, such as network topology or architecture relevant for U.S. operations.

2. **Conflicting and Mutually Irreconcilable Compliance Requirements:** Second, U.S. companies face conflicts between the obligations they have to the U.S. or allied and partner governments and those that they face under PRC law. For example, the PRC's 2021 Anti-Sanction Law and 2023 Foreign Relations Law allows the PRC to punish U.S. companies if they comply with sanctions or legislation the PRC seems discriminatory. Moreover, companies may be unable to comply with Congressional subpoenas or requests by law enforcement or administrative agencies for information relevant to regulations without being out of compliance with PRC laws on data transfer. This, in effect, forces companies to choose whether to be compliant with one system or another.

3. **Profiting from Conflicts of Interest:** U.S. companies may lean into conflicts of interest for financial benefit. For example, a company could conceivably share information or experience gained from working with the U.S. government, including sensitive information U.S. policy or government practices, to support work done with PRC entities.

While the costs and likelihood of these conflicts of interest are growing, the benefits of complying with PRC pressure tactics are clearly falling. Compliance with the PRC's pressure tactics might provide some short-term market access, but the PRC's ultimate objective is to eventually replace these companies with indigenous PRC companies. The "China cycle," as the writer Noah Smith calls it, involves (1) a multinational company setting up in the PRC to access the PRC market; (2) a multinational company complying with terms that effectively result in the transfer of their technology or know-how to PRC companies; (3) the PRC government then helping PRC companies push out the multinational; and (4) the PRC companies then competing with the multinational for market share in other countries, often with some state support.[16]

Increasingly, foreign multinationals and the trade associations that represent them are raising direct concerns publicly. Jens Eskelund, president of the European Chamber of Commerce in China, said in a statement that, "The scope of issues deemed 'sensitive' seems to be constantly expanding, which makes it more difficult for companies to access information necessary for making investment decisions related to their China operations."[17] Similarly, the US-China Business Council wrote in its most recent member survey that, "American companies that conduct business in China continue to encounter systemic challenges around market access and barriers to investment, opaque rules and uneven regulatory enforcement, and rising compliance requirements, particularly around data security and privacy."[18] Meanwhile, the PRC has not taken action to address these concerns. The growing influence and power of the security services has, instead, created additional obstacles. China's Ministry of State Security has published a series of web comics to educate citizens about the national security risks it faces from foreigners. One example included a special investigator going undercover at a consulting firm and demonstrating it was selling sensitive information.[19]

II. The Consulting Industry

Since 2023, the PRC has taken a number of aggressive steps against U.S. consulting and due diligence firms, which heighten already existing conflicts of interest that may be present when these firms conduct work for the U.S. government and for PRC state-affiliated entities.

PRC Crackdowns on Consulting Firms

PRC state media has stressed that the activities of foreign firms must not be contrary to PRC national interests, but this standard remains nebulously defined. Data on macroeconomic trends or the performance of individual companies, often critical to facilitating U.S.-China investment and economic exchange, can now fall within the vague definition of "state secrets," "work secrets," or information that harms China's "national security." This creates wide-ranging vulnerabilities for consulting firms in the PRC that can amplify conflicts of interest.

In 2023, the PRC began taking broad action against foreign consulting firms in the PRC.

- PRC law enforcement raided the offices of Bain & Company. They detained and questioned several employees and seized phones and computers and the data stored on them.[20]
- PRC authorities also raided the offices of international advisory and knowledge services firm Capvision in Beijing, Shenzhen, Shanghai, and Suzhou as part of an investigation into their alleged failure to protect "state secrets." PRC authorities seized devices and even sentenced one of their senior experts who had been kept on retainer to six years in prison.[21] Capvision was forced to acknowledge that it had caused harm to PRC national security.
- The PRC raided the Mintz Group's Beijing offices, closed the branch, and detained five local employees, ultimately fining the company for failing to obtain approval of statistical survey work and then raising the fine the following year.[22] The raids came after the company issued an article on due diligence related to the Uyghur Forced Labor Prevention Act.[23]

Due in part to the crackdown, the *Financial Times* reported last year that U.S. consulting firms are already reducing business in China. Many are struggling to find work, delaying start dates for new employees, and failing to meet revenue projections.[24] The risk and likelihood of conflicts interest from operations in China has increased while the reward has decreased.

Conflicts of Interest for Consulting Firms

In some cases, as this Committee has helped reveal, U.S. consulting firms have provided services to the U.S. government while also consulting for the PRC. McKinsey, for example, has worked on over 60 contracts for the U.S. military and law enforcement over a dozen years in areas including weapons systems, the Defense Department's IT network, shipyard modernization, technology for military services, FBI intelligence gathering, and other projects – some of which require a security clearance.[25] Since 2008, it made more than $850 million in contracts with the U.S. federal government. But it has simultaneously conducted work for PRC state-owned enterprises and private companies, and according to one McKinsey website, for the PRC government as well.[26] McKinsey has indicated it does not "serve clients on issues related to defense, intelligence, justice, or police issues" in the PRC, but a McKinsey-affiliated group reportedly advised the PRC government on its Made in China 2025 industrial policy plan, advocated for civil-military integration, and recommended the PRC push foreign companies out and indigenize their roles in the PRC economy – proposals that harmed U.S. interests. These proposals were evidently directly presented to former Premier Li Kiqiang.[27] It is possible that expertise gained from working with U.S.

industry and the U.S. government could have informed work on a PRC plan that, at its core, seeks "catch up and surpass" the United States in technology. It is not in the national security interests of the United States for companies providing support to U.S. industry to support the PRC's industrial policy efforts to the outcompete the United States, nor is it in the interests of their U.S. clients.

McKinsey is not the only U.S. consulting firm that has served both the U.S. and PRC governments. Bain and Boston Consulting Group also have operations in China. These firms may have protections in place to ensure sensitive U.S. data could not be transferred by the PRC, but it is unclear how sufficient those protections are given the PRC's ability to compromise the data of U.S. companies operating in the PRC and demand compliance from PRC entities and individuals to share that data. Similarly, even if these firms have extensive internal firewalls to ensure special knowledge about U.S. government or corporate strategies would not inadvertently or deliberately be transferred to projects in China, it is unclear whether these are sufficient given the increasingly challenging regulatory environment in the PRC.

The fact that U.S. consulting firms conducting sensitive work for the U.S. government were not previously required to disclose to the U.S. government that they had projects with the PRC creates a serious national security risk. The compliance requirements for consulting firms imposed by the federal government are, in other words, even lower than those for U.S. military personnel or civil servants holding security clearance who would certainly be required to disclose work done for the PRC or other foreign actors.

Moreover, PRC law complicates any compliance with a U.S. subpoena or request for information on their business in the PRC, effectively allowing a foreign power to dictate the terms of U.S. oversight of the relationship between these companies and a foreign power – an untenable position. Together, this suggests the need for a different approach to regulating those companies that have the privilege of providing services to the U.S. government.

III. The Tech Industry – Software, Cloud, and Networks

The conflicts faced by U.S. consulting firms are serious, but those faced by some U.S. technology companies who serve both the U.S. government and the Chinese market are potentially far more consequential. The risks involve not only the transfer of sensitive data but also the compromise of platforms upon which the U.S. government relies, as well as risks to critical infrastructure.

Risks to United States Platforms and Critical Infrastructure

With respect to platforms, for example, the communications of the U.S. government have repeatedly been compromised by PRC cyber actors. Most recently, the PRC targeted Microsoft Exchange Online, which allowed it to compromise 60,000 State Department emails and the account of U.S. Commerce Secretary Gina Raimondo, U.S. Ambassador to China Nicholas Burns, and others. It is still unknown how the PRC was able to do this, and the incursion was first detected by the State Department and not industry.

In addition to these risks, government officials and private sector leaders have increasingly called attention to PRC activity in U.S. critical infrastructure that could pose a direct threat to homeland security. Earlier this year, CISA, NSA, FBI, and Five Eyes partners assessed that, "that People's Republic of China (PRC) state-sponsored cyber actors are seeking to pre-position themselves on IT networks for disruptive or destructive cyberattacks against U.S. critical infrastructure in the event of a major crisis or conflict with the United States," and that a PRC group called "Volt Typhoon" had comprised infrastructure providers in several sectors.[28] At the Munich Security Conference a few weeks later, Deputy National Security Adviser Anne Neuberger explained further that, "For a long time when we all in the industry

talked about cyber security our key focus was theft of data...what has shifted as captured in the Volt Typhoon threat vector is countries pre-positioning in the critical infrastructure of another country." Neuberger explained that "we know it is not for espionage purposes, because when we look at the sectors like water sectors and civilian airport sectors, those have very little intelligence value." She continued, "That is a concern because a potential disruption of critical infrastructure could be used to put pressure on a government during a crisis or could be used to put pressure or try to message to a population during a crisis.[29] As Jen Easterly said to the Select Committee on the CCP, the PRC is ready to "launch destructive cyber-attacks in the event of a major crisis or conflict with the United States," including "the disruption of our gas pipelines; the pollution of our water facilities; the severing of our telecommunications; the crippling of our transportation systems." These steps would be designed to "to incite chaos and panic across our country and deter our ability to marshal military might and citizen will."[30]

The private sector is aware of the problem. As Microsoft CEO Brad Smith explained, "we've seen from China in particular this prepositioning of so-called web shells. Think of it as tunnels into our water system, our electrical grid, into the air traffic control system, the kind of thing that you look at and you say, this is only useful for one thing and…they have it in place in the event of a war or hostilities."[31] In an annual report last year, Microsoft noted it had been tracking some of the relevant threat actors focused on U.S. critical infrastructure for several years.

As Congress develops more advanced conflict of interest guidelines, it may be worth considering the risks posed by U.S. technology companies that do business in the PRC. Companies that support the U.S. government or critical infrastructure in the United States might, through operations in the PRC, inadvertently create vulnerabilities for their operations in the United States that would affect national security, especially as Beijing puts more pressure on these companies.

Conflicts of Interest in The Technology Sector

First, several U.S. technology companies that serve the U.S. government have provided the PRC government the source code of the systems that the U.S. government and most Americans rely on. In 2003, Microsoft allowed China to participate in its Government Security Program which it indicated "provides national governments with controlled access to Microsoft Windows source code."[32] More recently, in 2016, Microsoft launched a "Transparency Center" in China to provide "access to documents and source code" for "Windows, Windows Server, Office, Exchange Server, SQL Server, and SharePoint Server," services upon which the U.S. government also depends.[33] Similarly, in 2015 IBM decided to allow the Chinese government review its source code in a controlled environment.[34] Even when companies do not voluntarily provide such information, they could conceivably be compelled to provide it not as a condition of market access but as part of a regulatory action. For example, the PRC's "cybersecurity review," which was directed against Micron in 2023 in retaliation for U.S. semiconductor export controls, lack due process and can be used to demand sensitive information and to levy heavy penalties.[35] Notably, in this more challenging regulatory environment, both Microsoft and IBM have reduced operations in China. In August 2024, IBM reportedly closed its operations in China, including its China Development Lab and China Systems Lab, in favor of labs in other countries, including India.[36] Similarly, in May 2024, Microsoft asked several hundred employees in China to relocate to other countries as it reduced cloud-computing and AI research.[37]

Second, U.S. cloud service providers that support the U.S. government and that operate in the PRC almost certainly face conflicts given the PRC's regulatory environment. As detailed previously, over the last seven years, the PRC has introduced a National Intelligence Law, Counterespionage Law, Encryption Law, Data Security Law, and updates to its definition of state secrets. This regime gives the PRC the ability to

demand PRC entities and individuals comply with requests from the intelligence services, provide access to encryption keys, insert personnel on site, or outright seize equipment and data. In that regime, the fact that U.S. cloud operators in China are required by the Chinese government to partner with a Chinese operator is concerning. Microsoft, for example, partners with 21 Vianet, to operate Microsoft's cloud services in China, including Azure; Amazon partners with Beijing Sinnet Technology Co., Ltd. (Sinnet) and Amazon Web Services Ningxia Region run by Ningxia Western Cloud Data Technology, Co., Ltd. (NWCD). Others, like Google and Oracle, do not offer services in mainland China.[38] For those that do, the concern is whether their systems in China are adequately firewalled from systems in the United States, or whether compromise of cloud infrastructure in China could be used to compromise U.S. systems. Even with such firewalls, it is conceivable that PRC operating partners could gain important insights into how their U.S. partners provide cloud services to clients in the United States, such as important information about network topology and architecture. More fundamentally, the fact that PRC operators may be operating a PRC cloud with encryption keys provided to the PRC government all under a regime that gives broad authority to PRC intelligence services to embed themselves in the operator suggests data stored in U.S. cloud systems in the PRC is not secure. The idea that the PRC would exploit access to cloud services to gain access to those who use them is not farfetched. PRC Ministry of State Security cyber actors are known to have hacked into technology service providers, gaining access to their clients, which included 5G provider Ericsson and U.S. defense company Huntington Ingalls, among others.[39] Foreign governments have also noted that, in overseas markets, PRC cyber threat actors have sought to compromise cloud service providers. Accordingly, it stands to reason they would do so within China as well.[40]

There are reasons to believe the PRC is focused on gaining advantages from these kinds of entanglements in China. For example, technology companies supporting the U.S. government may be forced to cooperate with China's cybersecurity legislation by providing information on zero-day exploits that the PRC government appears to be promptly weaponizing. Microsoft has publicly accused the PRC of using the country's new vulnerability disclosure requirements to stockpile zero-day exploits. "China's vulnerability reporting regulation went into effect September 2021," it wrote in a 2022 report, "marking a first in the world for a government to require the reporting of vulnerabilities into a government authority for review prior to the vulnerability being shared with the product or service owner." Based on the data, Microsoft concludes that, "the increased use of zero days over the last year from China-based actors likely reflects the first full year of China's vulnerability disclosure requirements for the Chinese security community and a major step in the use of zero-day exploits as a state priority."[41]

Asymmetric Advantages for the PRC

What is particularly concerning is the possibility that the PRC may be learning more about systems on which the U.S. relies while reducing its own reliance on U.S. systems. Conversely, the United States may not be able to gain comparable information about PRC systems. Over time, this creates a structural asymmetric vulnerability. This is not a purely academic consideration. In 2016, President Xi stressed the country's information technology systems needed to be "controllable," with PRC agencies determining foreign software could not meet these standards.[42] This year, *the Wall Street Journal* reported that the PRC issued a guidance – "Document 79" – requiring state-owned enterprises in strategic sectors to replace all foreign IT software by 2027, colloquially known in China as "Delete A" where "A" refers to America.[43] Meanwhile, the PRC seeks to spread its own services around the world.

The PRC is well underway towards reliance on "controllable" systems. For example, even as Microsoft was increasing PRC visibility into its products, the PRC was reducing its reliance on Microsoft products and forcing public service providers and others to switch to the indigenous PRC HarmonyOS system.

During the recent outage related to a Crowdstrike update, PRC public services – in contrast to U.S. services – experienced a "minimal impact." PRC government employees boasted that this "proved that the country has made progress in achieving its goal of 'safe and controllable' computing systems."[44] Accordingly, there are risks that the information shared with the PRC about U.S. technology systems could create asymmetric vulnerabilities. Similarly, although U.S. cloud providers do have some market share in the PRC, that share is small compared to Chinese cloud providers who have successfully increased their market share. Three PRC companies, for example, have 80% market share within the PRC. As with consulting, the benefits from involvement in the PRC marketplace are likely falling while the risks are growing. As Microsoft CEO Brad Smith noted in recent testimony, the PRC accounts for about 1.5% of Microsoft's revenue and the company is scaling down its engineering team in the PRC too. At the same time, the PRC is backing its own cloud providers in foreign markets, and the opportunity for U.S. providers in the market is shrinking while the risks continue to grow.[45]

More broadly, in cloud, the PRC's lead cloud operators - Alibaba, Baidu, and Tencent - all operate in the United States in an environment that is far more permissive than one available to U.S. cloud companies in China. None of these companies, for example, are forced to have a local joint venture partner. Accordingly, the United States has no direct visibility into their networks, topology, or encryption even though the Trump and Biden Administrations have expressed concerns about the security risks posed by PRC cloud companies operating in the United States, including access to data, among other considerations.[46] The fact that the regulatory environment for technology companies in the United States and the PRC is fundamentally not reciprocal provides advantages to the PRC.

IV. Recommendations that Build on Provisions Already Included in the *Time to Choose Act*

U.S. companies face an unenviable position in the PRC. Prudent regulatory action from Congress could help these companies better withstand PRC pressure. Rather than refuse to comply with PRC requests independently, they could – with these steps – instead point to the U.S. government as the reason for their non-compliance, possibly buying them some space with the PRC. In some cases where this approach is not viable, certain U.S. companies may indeed have to choose work with the U.S. government over considerably less lucrative and diminishing opportunity in the PRC market. These provisions below would not affect the vast majority of companies operating in the PRC, but they would affect those upon which the United States government depends.

- **Congress could consider legislation that prohibits, or at a minimum requires disclosure of, Chinese Communist Party cells within foreign companies or their subsidiaries.** Congress could apply this standard to companies listed on public exchanges, as some proposed legislation does. This Committee could consider prohibiting cells in companies contracting with the federal government. A blanket prohibition would allow companies to blame Washington – rather than their own decision-making – for refusing PRC pressure to establish such cells.

- **Congress could consider legislation that prohibits U.S. companies and their subsidiaries from complying with PRC national security laws.** The PRC's recent national security laws – especially the Counterespionage Law, National Intelligence Law, Cybersecurity Law, Encryption Law, and Data Security Law – create a regime that forces companies to take action contrary to their interests and those of their clients, including the U.S. government. Taken together, these laws give the PRC the ability to demand PRC entities and individuals comply with requests from the intelligence services, provide access to encryption keys, insert personnel on site, or outright seize equipment and data. This Committee could prohibit compliance with certain features of PRC

legislation for those companies contracting with the federal government. In the present, companies effectively have no excuse *not* to comply, which only facilitates greater PRC pressure.

- **Congress could consider prohibiting companies that contract with the federal government, especially technology companies, from entering arrangements with PRC entities that could plausibly threaten U.S. national security.** Companies that provide software or cloud services for the U.S. government, for example, could be prohibited from sharing source code with the PRC government or nominally private sector PRC companies. For companies providing cloud services to the U.S. government, a minimum requirement could be disclosure of any arrangements with the PRC and PRC entities, especially if these could conceivably compromise the security of the service provided to the U.S. government. This could be written to specify operation of PRC cloud infrastructure by PRC entities, the provision of encryption keys to PRC regulators, or other such items. In addition to require notification, Congress could also presumptively prohibit such activity at risk of losing U.S. government contracts.

Endnotes

[1] Rush Doshi, *The Long Game: China's Grand Strategy to Displace American Order* (Oxford: Oxford University Press, 2021).

[2] Neil Thomas, "Party Committees in the Private Sector: Rising Presence, Moderate Prevalence," Commentary, Macro Polo, December 16, 2020, https://macropolo.org/party-committees-private-sector-china/?rp=m.

[3] Jérôme Doyon, "Influence without Ownership: the Chinese Communist Party Targets the Private Sector," Expressions, Institut Montaigne, January 26. 2021, https://www.institutmontaigne.org/en/expressions/influence-without-ownership-chinese-communist-party-targets-private-sector.

[4] Dennis Kwok and Sam Goodman, "Chinese Communist Cells in Western Firms?" *Wall Street Journal*, July 11, 2022, https://www.wsj.com/articles/communist-cells-in-western-firms-business-investment-returns-xi-jinping-11657552354.

[5] Patrick, Mulholland, "HSBC Unit Installs Chinese Communist Party Committee," *Telegraph*, July 21, 2022, https://web.archive.org/web/20220728222230/https://www.telegraph.co.uk/business/2022/07/21/hsbc-unit-installs-chinese-communist-party-committee/.

[6] Cheng Leng and Ryan McMorrow, "EY China staff encouraged to wear Communist party badges," *Financial Times*, February 27, 2023, https://www.ft.com/content/cfa55e7d-1294-4c4f-85cc-03c6ec63550a.

[7] Michael Cunningham and Bryan Burack, "Don't Give the CCP Backdoor Influence Over U.S. Companies," Commentary, Heritage Foundation, June 12, 2023, https://www.heritage.org/asia/commentary/dont-give-the-ccp-backdoor-influence-over-us-companies.

[8] Kevin Breuninger and Eamon Javers, "Communist Party Cells Influencing U.S. Companies' China Operations, FBI Director Wray Says." *CNBC*, July 12, 2023, https://www.cnbc.com/2023/07/12/communist-cells-influence-companies-in-china-fbi-director.html.

[9] For more, see U.S. Department of Homeland Security, Office of Strategy, Policy, and Plans and Office of Trade and Economic Security, *Data Security Business Advisory: Risks and Considerations for Businesses Using Data Services and Equipment from Firms Linked to the People's Republic of China*, December 22, 2020, https://www.dhs.gov/publication/data-security-business-advisory, (accessed July 24, 2024).

[10] Ibid.

[11] Lester Ross and Kenneth Zhou," China Launches Cybersecurity Review Against Micron," WilmerHale, April 11, 2023, https://www.wilmerhale.com/insights/client-alerts/20230411-china-launches-cybersecurity-review-against-micron

[12] Dakota Cary and Kristin Del Rosso, "Selight of Hand: How China Weaponizes Software Vulnerabilities," Atlantic Council, September 6, 2023, https://www.atlanticcouncil.org/in-depth-research-reports/report/sleight-of-hand-how-china-weaponizes-software-vulnerability/#few-good-options

[13] For more, see U.S. Department of Homeland Security, Office of Strategy, Policy, and Plans and Office of Trade and Economic Security, *Data Security Business Advisory: Risks and Considerations for Businesses Using Data Services and Equipment from Firms Linked to the People's Republic of China*, December 22, 2020, https://www.dhs.gov/publication/data-security-business-advisory, (accessed July 24, 2024).

[14] "China's New Cryptography Law: Still No Place to Hide," China Law Blog (Blog), Harris Sliwoski, November 7, 2019, https://harris-sliwoski.com/chinalawblog/chinas-new-cryptography-law-still-no-place-to-hide/.

[15] Office of Senator Josh Hawley, "FBI Director: China Can Compel Tech Companies Doing Business In Country To Turn Over Any Information China Wants," press release, November 5, 2019, https://www.hawley.senate.gov/fbi-director-china-can-compel-tech-companies-doing-business-country-turn-over-any-information-china/.

[16] Noah Smith, "Why China is Defeating Tesla,", April 17, 2024, https://www.noahpinion.blog/p/why-china-is-defeating-tesla

[17] Daisuke Wakabayashi, Keith Bradsher, and Claire Fu, "China Expands Scope of 'State Secrets' Law in Security Push," *New York Times*, February 28, 2024, https://www.nytimes.com/2024/02/28/world/asia/china-state-secrets-law.html.

[18] US-China Business Council, *Member Survey*, 2023, 1, https://www.uschina.org/reports/2023-member-survey.

[19] Wakabayashi, Bradsher, and Fu, "China Expands Scope of 'State Secrets' Law in Security Push"; A link to the cartoon is available here https://mp.weixin.qq.com/s/K9QDFFOKTCHUZ-iA5R-zQQ.

[20] Martin Purbrick, "Chinese National Security Laws Hinder Foreign Companies' Operations in China," *China Brief* 23, no. 19 (October 20, 2023): 11-15, https://jamestown.org/program/chinese-national-security-laws-hinder-foreign-companies-operations-in-china/.

[21] Nectar Gan and Juliana Liu, "'Everybody Is Worried': China Raids Offices of Consultancy Firm Capvision In Widening Industry Crackdown," *CNN*, May 9, 2023, https://edition.cnn.com/2023/05/09/business/china-capvision-consultant-industry-crackdown-intl-hnk/index.html.

[22] Daisuke Wakabayashi and Keith Bradsher, "U.S. Consulting Firm Is the Latest Target of a Chinese Crackdown," *New York Times*, April 27, 2023, https://www.nytimes.com/2023/04/27/business/bain-china.html; Chun Han Wong, "China Raises Fines on Mintz Due-Diligence Firm," *Wall Street Journal*, March 12, 2024, https://www.wsj.com/world/china/china-raises-fines-on-mintz-due-diligence-firm-c7486aeb.

[23] Purbrick, "Chinese National Security Laws Hinder Foreign Companies' Operations in China."

[24] Ryan McMorrow, Joe Leahy, Nian Liu, and Eleanor Olcott, "Work Dries Up for US Consultancies In China After National Security Raids," *Financial Times*, July 23, 2024, https://www.ft.com/content/0b869421-10fd-41e7-8280-5d09a224062f.

[25] Dan De Luce and Yasmine Salam, "Advising Both Chinese State Companies and The Pentagon, McKinsey & Co. Comes Under Scrutiny," *NBC News*, November 13, 2024, https://www.nbcnews.com/politics/national-security/advising-both-chinese-state-companies-pentagon-mckinsey-co-comes-under-n1283777.

[26] Stephen Foley, Ryan McMorrow, and Demetri Sevastopulo, "McKinsey website touted its advice to Chinese government ministries," *Financial Times*, February 27, 2024, https://www.ft.com/content/159f27df-5758-4be2-881e-1bf3025bc98b.

[27] De Luce and Salam, "Advising Both Chinese State Companies and The Pentagon, McKinsey & Co. Comes Under Scrutiny."

[28] United States of America, Australian Government, Dominion of Canada, United Kingdom of Great Britain and Northern Ireland, New Zealand, *Joint Cybersecurity Advisory: PRC State-Sponsored Actors Compromise and Maintain Persistent Access to U.S. Critical Infrastructure*, Cybersecurity & Infrastructure Security Agency (US), National Security Agency (US), Department of Justice (US), Department of Energy (US), Environmental Protection Agency (US), Transportation Security Administration (US), Signals Directorate (AUS), Cyber Security Centre (AUS), Communications Security Establishment (CAN), Centre for Cyber Security (CAN), National Cyber Security Centre (NZ), National Cyber Security Centre (UK), AA24-038A, February 7, 2024, https://www.cisa.gov/sites/default/files/2024-03/aa24-038a_csa_prc_state_sponsored_actors_compromise_us_critical_infrastructure_3.pdf.

[29] Anne Neuberger, "MCSC 2024: Fireside Chat: Anne Neuberger," Sicherheitsnetzwerk München, March 11, 2024, YouTube video, https://www.youtube.com/watch?v=WlvcT3aPb2k.

[30] Jen Easterly, "Opening Statement by CISA Director Jen Easterly," Blog, News, Cybersecurity& Infrastructure Security Agency, January 31, 2024, https://www.cisa.gov/news-events/news/opening-statement-cisa-director-jen-easterly.

[31] *A Cascade of Security Failures: Assessing Microsoft Corporation's Cybersecurity Shortfalls and the Implications for Homeland Security*, 118th Congress, 2nd session, 2024, (Statement of Brad Smith, Vice Chairman and President, Microsoft).

[32] Geoffrey Cain has written extensively about these linkages. See also, "Microsoft and China Announce Government Security Program Agreement," Stories, Microsoft, February 28, 2003, https://news.microsoft.com/2003/02/28/microsoft-and-china-announce-government-security-program-agreement/; "China Information Technology Security Certification Center Source Code Review Lab Opened," Stories, Microsoft, September 26, 2003, https://news.microsoft.com/2003/09/26/china-information-technology-security-certification-center-source-code-review-lab-opened/; "Microsoft Gives Chinese Government Access to Windows Source Code," *People's Daily*, March 4, 2003, http://en.people.cn/200303/04/eng20030304_112657.shtml.

[33] Laramillermsft and MicrosoftGuyJFlo, "Transparency Centers," Articles, Microsoft Security, Microsoft, February 2, 2024, https://learn.microsoft.com/en-us/security/engineering/contenttransparencycenters.

[34] Eva Dou, “IBM Allows Chinese Government to Review Source Code,” *Wall Street Journal*, October 16, 2015, https://www.wsj.com/articles/ibm-allows-chinese-government-to-review-source-code-1444989039.

[35] Lester Ross and Kenneth Zhou," China Launches Cybersecurity Review Against Micron," WilmerHale, April 11, 2023, https://www.wilmerhale.com/insights/client-alerts/20230411-china-launches-cybersecurity-review-against-micron

[36] Ivana Saric, "IBM is Latest U.S. Tech Giant to Pull Back from China," Axios, August 26, 2024, https://www.axios.com/2024/08/26/ibm-rd-division-china-us-tech-competition

[37] Ibid.

[38] “Cloud Locations,” Google, https://cloud.google.com/about/locations#asia-pacific; Public Cloud Region Locations, Oracle, https://www.oracle.com/cloud/public-cloud-regions/.

[39] Jack Stubbs, Joseph Menn, and Christopher Bing, "Inside the West's Failed Fight Agianst China's 'Cloud Hopper' Hackers," *Reuters*, June 16, 2019, https://www.reuters.com/investigates/special-report/china-cyber-cloudhopper/

[40] "Cyber threat bulletin: Cyber Centre urges Canadians to be aware of and protect against PRC cyber threat activity," Canadian Centre for Cyber Security, June 3, 2024, https://www.cyber.gc.ca/en/guidance/cyber-threat-bulletin-cyber-centre-urges-canadians-be-aware-and-protect-against-prc-cyber-threat-activity

[41] Microsoft, *Microsoft Digital Defense Report*, Security Insider, Microsoft, 2022, 39-40, https://www.microsoft.com/en-us/security/security-insider/intelligence-reports/microsoft-digital-defense-report-2022.

[42] Rush Doshi, Emily De La Bruyere, Nathan Picarsic, and John Ferguson, "Chinas a 'Cyber Great Power': Beijing's Two Voices in Telecommunications," Brookings Institution, April 2021, https://www.brookings.edu/wp-content/uploads/2021/04/FP_20210405_china_cyber_power.pdf, p. 10.

[43] Liza Lin, "China Intensifies Push to ‘Delete America’ From Its Technology," The Wall Street Journal, March 7, 2024, https://www.wsj.com/world/china/china-technology-software-delete-america-2b8ea89f.

[44] Wency Chen, Coco Feng, and Che Pan, "Microsoft Outage Leaves China Largely Untouched as Tech Self-Sufficiency Campaign Pays Off," South China Morning Post, July 19, 2024, https://www.scmp.com/tech/big-tech/article/3271171/microsoft-outage-leaves-china-largely-untouched-tech-self-sufficiency-campaign-pays

[45] Mark Montgomery and Eric Sayers, “Don’t Let China Take Over the Cloud — US National Security Depends On It,” *Hill*, November 13, 2023, https://thehill.com/opinion/national-security/4307002-dont-let-china-take-over-the-cloud-us-national-security-depends-on-it/.

[46] David McCabe, "China's Cloud Computing Firms Raise Concern for U.S.," New York Times, June 21, 2023, https://www.nytimes.com/2023/06/21/technology/china-cloud-computing-concern.html