
C4ADS
innovation for peace
PARTY CAPITAL
A BLUEPRINT FOR NATIONAL SECURITY
DUE DILIGENCE ON CHINA

ABOUT C4ADS

C4ADS (www.c4ads.org) is a 501(c)(3) nonprofit organization dedicated to data-driven analysis and evidence-based reporting of conflict and security issues worldwide. We seek to alleviate the analytical burden carried by public sector institutions by applying manpower, depth, and rigor to questions of conflict and security. Our approach leverages nontraditional investigative techniques and emerging analytical technologies. We recognize the value of working on the ground in the field, capturing local knowledge, and collecting original data to inform our analysis. At the same time, we employ cutting edge technology to manage and analyze that data. The result is an innovative analytical approach to conflict prevention and mitigation.

LEGAL DISCLAIMER

The mention of any individual, company, organization, or other entity in this report does not imply the violation of any law or international agreement, and should not be construed as such.

ABOUT THE AUTHOR

Jason Arterburn is Program Director for the Counterproliferation Cell at C4ADS, where he leads a team in using open source data to expose and investigate national security threats in China, North Korea, Iran, Russia, and Pakistan. Jason has testified to the U.S.-China Economic & Security Review Commission on the role of publicly available data in addressing threats from China. His analysis has also been cited by the Congressional Executive Commission on China and the United Nations Panel of Experts on North Korea, and has informed front page stories in the New York Times, Wall Street Journal, and Washington Post.

Jason earned a bachelor's degree in economics and interdisciplinary security studies from the University of Alabama, where he was awarded the Harry S. Truman and David L. Boren Scholarships, and a master's degree in China studies from Peking University, where he was a Yenching Scholar. Prior to C4ADS, Jason studied at Tsinghua University as a Blakemore Freeman Fellow in the Inter-University Program for Chinese Language Studies. He speaks Mandarin.

ACKNOWLEDGEMENTS

The author would like to thank all those who provided data, insights, and guidance during this project. The author would like to particularly thank the many C4ADS analysts and consultants who supported one or more aspects of the creation of this report, particularly Varun Vira, Thomas Ewing, Coby Goldberg, Irina Bukharin, Tim Doner, Anna Wheeler, and Tingting Naggiar.

The author would also like to thank the many experts who provided input and feedback in the drafting process, including but not limited to Meg Rithmire, F. Warren McFarlan Associate Professor at Harvard Business School; James Mulvenon, Director of Intelligence Integration at SOS International; Catherine Aiken, Acting Director of Data Science at Georgetown's Center for Security and Emerging Technology (CSET); Jude Blanchette, Freeman Chair in China Studies at the Center for Strategic and International Studies (CSIS); Martijn Rasser, Senior Fellow and Director of the Technology and National Security Program at the Center for a New American Security (CNAS); and Nate Sibley, Research Fellow at the Hudson Institute.

OUR TECH PARTNERS

C4ADS would also like to thank its technology partners, whose software and systems are integral to the integrity and quality of our research and analysis.

COVER ART

Cover illustration by Weitong Mai

TABLE OF CONTENTS

EXECUTIVE SUMMARY

China's commercial system exposes the United States to systemic national security risks that require new approaches for threat identification and response. In the absence of formal market protections, Chinese commercial actors operate with the threat of "exposure, incrimination[,] and, by extension, the coercive power of the party-state."[1] When Chinese companies pursue globalization, they expose the international community to "national security externalities" [2] of the party-state's involvement in China's domestic economy, which lacks the neutrality, due process, and clear legal delineation of state-business relations in market-oriented liberal democracies.

Policymakers internationally have achieved broad consensus about the urgency of mitigating the national security risks of exposure to China's commercial system, and observers have paid significant attention to changes in China's political economy under General Secretary Xi Jinping. However, comparatively less work has connected the most recent scholarship on Chinese state-business relations to those national security policy concerns. Additionally, while groups like the House Permanent Select Committee on Intelligence have highlighted the need for nontraditional intelligence consumers like state governments and university administrators to gain access to information about threats from China, there remains relatively limited discussion about how to achieve broader stakeholder engagement.

This report presents a systematic analysis of Chinese state-business relations to develop a novel, operational framework for national security due diligence in China's commercial sector. To do so, we draw not only on the most recent scholarship in international political economy but also on original analysis of high-scale, low-cost data from publicly available sources.

Key findings are as follows:

The Chinese party-state engages with commercial actors through networks that are exceedingly complex, diversified, and politicized. We analyze public disclosures from 70,000+ Chinese companies, universities, and civil society organizations to demonstrate that the party-state engages with commercial actors through commercial, financial, academic, social, and political mechanisms that are both similar to and distinct from state-business relations in market-oriented liberal democracies.

Party-state interactions with the commercial sector leave an extensive data footprint in publicly available sources. We develop a novel framework for assessing national security risks related to Chinese commercial actors that considers party-state equity or financing, political exposure, industry sensitivity, market structure, and goal compatibility between the commercial actor and the party-state.

High-scale data integration produces actionable information on national security risks related to technology competition, corruption, threat finance, and political interference. We operationalize our risk framework to identify high-risk networks in China's military-industrial complex and financial institutions with case studies in quantum technology, organized crime, and political lobbying in the United States.

Based on these findings, we recommend that the U.S. government and its allies invest more significantly in developing a national security due diligence capability on China that leverages publicly available information, which can facilitate effective multilateral policy responses with timeliness and precision.

DEFINITIONS

ACFIC	All-China Federation of Industry and Commerce
ASPI	Australian Strategic Policy Institute
CCP	Chinese Communist Party
CPPCC	Chinese People's Political Consultative Conference
FARA	Foreign Agents Registration Act
FCC	Federal Communications Commission
GGIF	Government-Guided Investment Fund
IPO	Initial Public Offering
MCF	Military-Civil Fusion
MIIT	Ministry of Industry and Information Technology
MOST	Ministry of Science and Technology
NPC	National People's Congress
NS-CMIC	Non-SDN Chinese Military-Industrial Complex Company
PAI	Publicly Available Information
PEP	Politically Exposed Person
PLA	People's Liberation Army
R&D	Research and Development
RCAs	Relatives and Close Associates
SASAC	State-owned Assets Supervision and Administration Commission
SDN	Specially Designated National
SOE	State-owned Enterprise
STAR Market	Shanghai Stock Exchange Science and Technology Innovation Board
UFWD	United Front Work Department

A COMPLEX, DIVERSIFIED, AND POLITICIZED COMMERCIAL SYSTEM

There is a clear and justifiable alarm around the Chinese party-state's use of its economy to pursue national security objectives. Yet it remains difficult to assess the relationships between commercial actors and the party-state and, in turn, the potential national security risks that a firm's behavior could pose.

On November 3, 2020, General Secretary Xi Jinping blocked what was slated to be the largest initial public offering in the world.[3] [4] Jack Ma, the second-richest man in China whose Ant Group has propelled significant transformations to China's digital economy, was poised to list his company on the Shanghai and Hong Kong stock exchanges with an estimated value of more than $34 billion. In an effort to save the initial public offering (IPO) as Ma's relationship with Beijing grew strained, he told regulators that they could "take any of the platforms Ant [Group] has as long as the country needs it."[5]

Xi Jinping's decision to block one of the largest and most successful Chinese companies stunned many observers as a new milestone in the Chinese Communist Party's (CCP's) effort to coerce the private sector into operating in its image, an endeavor that took on a new intensity in 2020. This attempt to reassert Party primacy in the private sector also coincided with new policy guidance from the CCP, which called in September 2020 for reinvigorated United Front Work in the private sector "to better focus the wisdom and strength of private businesspeople on the goal and mission to realize the great rejuvenation of the Chinese nation."[6] The policy's stated goal is to "build a backbone team of private business people that is dependable and usable in key moments,"[7] and as Jack Ma's blocked IPO made clear, the CCP would pursue it not just through soft appeals to patriotism but also through coercive regulatory measures.[8]

Ant Group's turbulent bout with Chinese regulators lays bare a major challenge facing policymakers in the United States and its allies: how to assess the relationship of a commercial actor to the Chinese party-state and, by extension, how to determine the national security risks that the company could pose. If a private company with Ant Group's stature and political leverage could be so arbitrarily subjected to party-state coercion and capture, then so too could any other Chinese commercial actor engaged in the global economy. But the Party's latest efforts to reassert itself in the private sector suggest a more nuanced reality: that from the Party's view, there is still insufficient Party influence or control over commercial actors, many of whom could ultimately endanger the interests of the party-state or ruling class through the wealth and power that they generate.

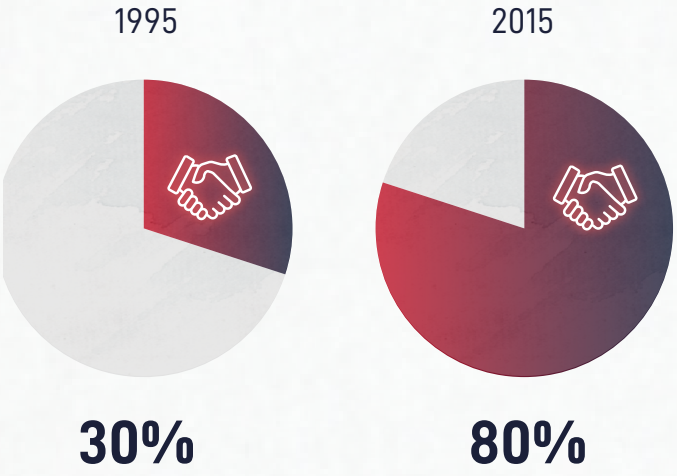
These subnational networks of business leaders and local government officials have emerged in a system that has been described as "regionally decentralized authoritarianism," in which powerful local governments have been responsible for the growth of private firms in the absence of strong protections for private property rights.[9] Bai et al. (2019) argue that those partnerships between local governments and private firms "almost always [take] the form of special deals" resembling collusion, and that because collusion has been growth-enhancing over the last three decades, it has become embedded as an informal yet durable institution in China's commercial system.[10] Recent scholarship suggests that universities and academic institutions have also turned to a different form of "special deals" in order to secure their own legal and economic protections. In considering the relationship of universities to the party-state's authoritarian system, Elizabeth Perry (2019) argues that Chinese professors exhibit "patterns of educated acquiescence," making concessions to the party-state on certain academic freedoms in exchange for privileges or benefits conferred by the state. While Perry's work focuses primarily on scholarship in the humanities in the context of political liberalization, she describes an intentional effort by the Chinese party-state to "win over their intelligentsia" by extending "an attractive package of privileges and benefits (social, prestige, political influence, material goods, and the like)," which ultimately "structures academic activities in ways that promote [the party-state's] interests by directing intellectual production into officially approved and remunerated outlets."[11] From companies to universities, the most recent academic scholarship is consistent in its assessments that Chinese commercial actors maintain complex relationships to the party-state that can neither be generalized as omnipotent party-state control nor delineated through simple distinctions like state-owned or private.

Whatever their status, Chinese firms globalize the risks of arbitrary and excessive party-state encroachment when they turn to international markets for investment and commercial partnerships. The task at hand for policymakers, then, is to determine the precise relationship of a given Chinese commercial actor to the party-state, and to assess the national security risks that such a relationship could pose—either if the firm were to become an instrument of economic statecraft, or if the firm were to expose its international partners to the collateral damage of arbitrary Chinese party-state encroachment. But doing either is a significant challenge for three core reasons.

First, China's commercial system is exceedingly complex. In fact, according to one study, the average size of the largest 100 conglomerates in China increased from 500 companies in 1995 to more than 15,000 companies in 2015.[12] Among the top 1,000 conglomerates, the share of subsidiaries that are joint ventures with other firms has increased from 30% to 80%.[13]

Average size of the largest 100 conglomerates in China

Growth in share of joint ventures among subsidiaries of Chinese conglomerates



Source: Bai, Hsieh, and Song (2019)

Second, Chinese commercial actors are extremely diversified in their operations. For example, China Poly Group, a state-owned conglomerate whose subsidiary Poly Technologies is on the U.S. Department of Commerce Entity List for weapons proliferation, also trades in art and antiquities via its subsidiary Poly Culture and maintains one of the largest art auction houses in the world.[14]

Third, China's commercial environment is highly politicized, with party-state proximity having a quantifiable impact on capital accumulation. Bai et al. (2020) assess that while the share of privately held capital in China's economy has increased by 14.4% from 2000 to 2019, private entrepreneurs with no state connections have seen a decrease in their holdings over the same period.[15] The degree of politicization and absence of market protections has led scholars like Meg Rithmire and Hao Chen (2021) to conclude that extortion is a central feature of Chinese business systems, as commercial actors "obtain business resources such as state assets, land, credit, or prestige" only by "manipulat[ing] a combination of political relationships, corporate governance institutions, and the tools of financial capitalism."[16]

The net result is that, as Jude Blanchette notes, "the analytical frameworks that many of us are using to understand China's economy are stuck in past paradigms that view 'state' and 'market' as standing in tension. In reality, China's sui generis CCP Inc. system is creating an entirely new political-economic order, and one that is already leaving a deep impression on the global order."[17] This report demonstrates a way forward—using high-scale data integration to produce actionable information about the relationship of Chinese companies to the party-state, and in turn make evidence-based assessments about the national security risks that those commercial actors could pose.

THE PARTY-STATE'S TOOLKIT FOR ECONOMIC STATECRAFT

To determine the potential national security risks of Chinese commercial activity, it is first necessary to understand how Chinese commercial actors interact with the party-state and when they could be subject to its coercive power.

China's party-state cannot control every commercial actor. When it seeks to do so, however, it has a range of both legal and extralegal mechanisms to induce and compel commercial actors toward its policy preferences, which are both similar to and distinct from mechanisms for state-business relations in countries like the United States. When Chinese commercial actors pursue globalization, they expose the international community to externalities of inconsistent, unpredictable, and at times excessive party-state involvement in the domestic economy, which may impinge on national security interests even in the absence of directed efforts at economic statecraft.

There are a number of ways in which the Chinese party-state engages with the commercial system:

Commercial
Using state-owned enterprises (SOEs) and their vast networks of subsidiaries to advance desired policy objectives at home and abroad, and regulators with broad authorities (e.g. standards process and product certifications) to tilt the commercial environment for favored enterprises.

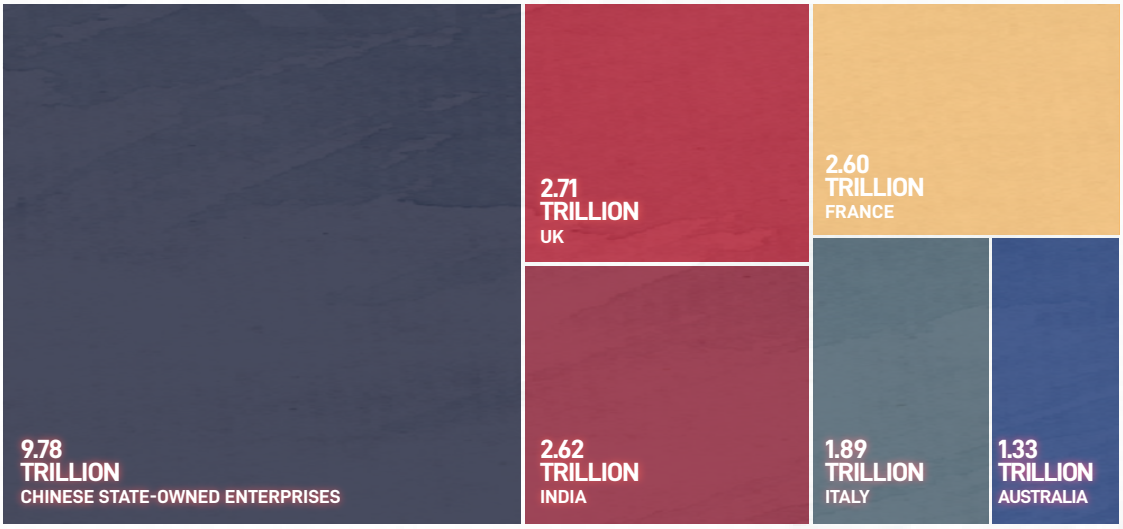
Financial
Gatekeeping access to capital through state-owned financial institutions, government-guided investment funds, and strict capital controls.

Academic
Encouraging universities to use massive investment vehicles and other financial inducements to attract talent, acquire technology, and commercialize it domestically.

Social
Conferring prestige to business elites through membership in formal political institutions that incentivize alignment with party-state priorities.

Political
Mobilizing political committees and industrial associations as extralegal mechanisms for corporate governance and oversight, and using expansive laws (e.g. cybersecurity, counterespionage, counterterrorism, anti-sanction) to threaten and compel the party-state's policy line through the legal system.

商业 Commercial



Estimated share of global GDP production by Chinese SOEs and similarly sized countries (in USD)

Estimate about SOE GPD share: Baston, A. (2021, February 16). Confronting Chinese State Capitalism [Video, timestamp 30:13]. Center for Strategic and International Studies. https://www.csis.org/events/confronting-chinese-state-capitalism
Source: World Bank (2020)"

The most direct form of Chinese party-state involvement in the economy is through its ownership and management of SOEs at the central, provincial, and local levels. China's SOEs direct capital toward key sectors and spearhead investments both at home and abroad,[18] and by one estimate, China's SOEs collectively produce 4.5% of global GDP, which is greater than the GDP of the United Kingdom.[19] State-owned enterprises are also enormously complex, often holding equity stakes in thousands of companies through layered investment networks that include other state-owned enterprises, publicly traded companies, privately held companies, and joint ventures with other businesses. For central SOEs (i.e. those owned and managed by national authorities), the Chinese Communist Party (CCP) directly controls executive leadership appointments and promotion and in some cases will appoint foreign nationals to SOE boards.[20] [21] Wendy Leutert (2020) notes that Xi Jinping has further institutionalized CCP control over central SOEs by increasing dual appointments for SOE executives to concurrent positions in CCP leadership to "constrain managerial independence by bringing SOE leadership into the political realm of the CCP,"[22] and by increasing the incidence of personnel rotation among SOE leadership as a means of reducing the risk of "departmentalization," i.e. the risk of specific actors becoming too entrenched in interests other than those of the CCP.[23]

While central SOEs may be easy to classify as an agent of the state, it is less clear what precisely the national security significance of a minority equity stake in a subordinate company may ultimately be. Relatedly, while some subsidiaries of defense SOEs may be easy to classify as Non-SDN Chinese Military-Industrial Complex Companies[24] (NS-CMICs) or military end users,[25] it is less clear whether a subsidiary operating in an entirely different industry with a minority equity stake should also be classified as such given the commercial diversity of China's largest state-owned conglomerates.

金融 Financial

To advance its industrial policy, the party-state directly engages in domestic and foreign capital markets through state-owned banks, state-owned asset management companies, sovereign wealth funds, and, more recently, government-guided investment funds (GGIFs). China's policy banks, sovereign wealth funds, and state-run investment vehicles may help to make acquisitions and prepare for listing on stock exchanges. China's monetary policy broadly restricts capital flows internationally, and by gatekeeping access to financial markets domestically and abroad, China's party-state has a mechanism through which to protect companies that support its political or policy objectives.

Government-guided investment funds drive capital toward companies that support the party-state's policy goals, including those that later integrate with global financial markets through investment from abroad or IPOs on international stock exchanges. To do so, central and local government entities establish investment funds with a defined purpose aligned with party-state policy objectives and solicit additional capital investments from private investors. Those funds then direct capital toward companies and projects that support the party-state's development objectives. As of the first quarter of 2020, a leading Chinese third-party aggregator of private capital markets data estimated that 1,741 GGIFs were operating in China.[26] Unlike venture capital funds in the United States, only 27% of GGIFs are designed to support startups and early-stage innovation.[27] [28] Instead, 62% of GGIFs are "industry funds" created to support the growth of targeted strategic industries.[29] For example, following a government push for "indigenous innovation" for "core technologies,"[30] the number of registered companies working in semiconductors increased by 52% between 2018 and 2020, and the volume of investment increased by more than 800% over the same period.[31] [32]

Recent developments in financial markets allow Chinese companies—including those that directly support China's military and strategic technology sectors—to access significant sources of domestic and foreign capital. For example, in July 2019, the Shanghai Stock Exchange launched the Science and Technology Innovation Board ("STAR Market"), which provided Chinese technology companies in priority sectors such as artificial intelligence, semiconductors, and biotechnology a faster and easier regulatory path to launching and pricing IPOs. The STAR Market is now one of the most valuable stock markets in Asia and has provided a significant boost to Chinese technology companies, including companies that are unprofitable or would otherwise be unable to go public on other Chinese exchanges.[33]

Beyond the STAR Market, Chinese companies associated with China's military-industrial complex (either through commercial partnerships or equity) may also list on stock exchanges in Shenzhen and Hong Kong, which creates exposure to U.S. financial markets and investors. A July 2020 report from the U.S. Securities and Exchange Commission's Division of Economic and Risk Analysis found that at least five Chinese companies exposed to U.S. investors via the MSCI China A Index are on either the U.S. Department of Commerce's Entity List or designated by the Federal Communications Commissions (FCC) as a "national security threat."[34] A November 2020 report from RWR Advisory Group similarly found that more than 100 subsidiaries of companies that the U.S. Department of Defense designated for associations to the People's Liberation Army (PLA) are exposed to U.S. investors through various popular indexes such as the MSCI Emerging Markets Index and the FTSE All-World Index.[35]

How GGIFs, SOEs, and the STAR Market work together to develop Chinese technology companies

Alongside more traditional fiscal policy mechanisms, the Chinese party-state uses financial market tools to direct private capital toward party-state industrial policy objectives. Perhaps the clearest case is China's semiconductor industry.[36] One apparent GGIF alone, the China Integrated Circuit Industry Investment Fund, has made investments in 63 different companies in the industry since 2014.[37] By providing cheap capital that enables semiconductor companies to make investments in research and expansion, the party-state also helps these companies access broader sources of capital. China's most successful semiconductor company, Semiconductor Manufacturing International Corporation (SMIC), was able to go public on Shanghai's STAR Market in July 2020, in large part thanks to significant capital injections that it had previously received from the aforementioned China Integrated Circuit Industry Investment Fund, a state-owned telecommunications company (Datang Telecom Group), and a state-owned sovereign wealth fund founded to operate in global rather than domestic markets (CNIC Corporation).[38] [39] In other words, by drawing on capital from multiple state-backed sources—a GGIF, an SOE, and a sovereign wealth fund—SMIC, which the U.S. Department of the Treasury has named a Non-SDN Chinese Military-Industrial Complex Company,[40] was able to gain the stability it needed to access public capital through an IPO. By injecting public capital into private capital markets, China's party-state has helped the number of semiconductor companies to grow fivefold since 2014.[41] [42]

How the Semiconductor Manufacturing International Corporation began trading publicly

学术 Academic

China's party-state directly participates in domestic and international research and development (R&D) through universities, their holding companies, and talent recruitment programs. Chinese universities may expose the United States to national security risk through what scholar Elizabeth Perry has described as "patterns of educated acquiescence," through which universities buttress the party-state's authoritarian system by making political concessions in exchange for benefits that the state provides.[43] While Perry's work is primarily focused on scholarship in the humanities in the context of political liberalization, she describes an intentional effort by the Chinese party-state to "win over their intelligentsia" by extending "an attractive package of privileges and benefits (social, prestige, political influence, material goods, and the like)."[44] While connections between the state and academia are certainly neither direct nor unique to China, the party-state's systems of incentives must be properly understood in order to design effective disclosure requirements that would protect the integrity of research partnerships, particularly in sensitive fields like emerging technologies.

Some universities like the Seven Sons of National Defense (国防七子) emerge directly from China's military-industrial complex and therefore can be easily characterized as a national security risk. However, other universities may support China's military R&D programs in less straightforward ways.[45] For example, the Australia Strategic Policy Institute has identified and profiled more than 100 Chinese universities that work to varying degrees with China's military-industrial complex, e.g., through technology innovation parks or partnerships with state laboratories.[46]

With party-state encouragement, Chinese universities operate holding companies that make significant investments and acquisitions domestically and overseas, and create financial incentives for professors to hold simultaneous positions at companies that commercialize technologies developed through their research. In fact, Chinese corporate records indicate that 79 universities identified for associations with China's military-industrial complex have direct or indirect investments in more than 20,000 companies, some of which make investments in technology parks and collaborative research activities abroad.[47] Moreover, these universities regularly create financial incentives for professors to hold simultaneous positions at companies that commercialize technologies developed through their research, a policy pursued by the CCP since the 1980s.[48] [49]

Recent national and local policy initiatives have spurred on the growth of these university-backed commercial networks by encouraging a range of new financial incentives for professors that successfully commercialize technology. For example, one recent policy initiative encouraged universities to provide professors with greater proportions of "post-transfer income" that companies generate by commercializing technology.[50] Another recent policy effort encouraged companies to offer professors equity backed by their patents and technology.[51] Chinese professors, who may collaborate or hold adjunct research positions internationally, may also hold concurrent positions at technology companies, which may be technically legal in the local country's disclosure requirements but not always immediately disclosed in international collaboration or exchanges.

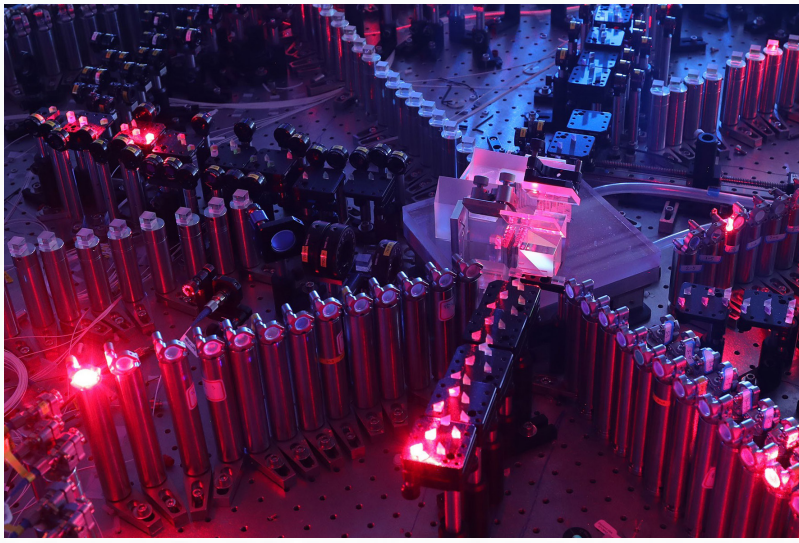
The Chinese government also coordinates global talent recruitment programs that target Chinese and foreign nationals for professional opportunities at Chinese universities and companies in priority sectors ranging from agriculture to biotechnology.[52] As Jeffrey Stoff notes in China's Quest for Foreign Technology, "China's talent recruitment programs, of which there are hundreds, are run at national, provincial, municipal, and even institutional levels, and are woven into government and [Chinese Communist Party] organs, SOEs, defense research and academic institutions, national laboratories, 'private' industry, domestic and overseas 'NGOs,' and global diaspora

organizations."[53] China's talent programs do not necessarily constitute illegal activity, and recent criminal prosecutions against Asian American academics in the United States have sparked debate about how current tools for addressing illicit technology transfers may risk prosecutorial overreach and racial profiling.[54]

社会 Social

China's party-state incorporates business elites into the political system and vice versa through various institutions (like the Chinese People's Political Consultative Conference) that create "politically exposed businesses." At the national level, the CCP appoints prominent members of society to five-year term seats on either the National People's Congress (NPC), China's national legislature; or the Chinese People's Political Consultative Conference (CPPCC), a political advisory body. There are about 2,000 to 3,000 members on each body at any given time. The NPC and CPPCC are consultative in nature, meeting just once annually for an in-person plenary session. As such, members do not discharge formal state functions, which is the basis for most international definitions for politically exposed persons (PEPs).[55] Similarly, their relationship to the party-state is not one of a patron to a client that would require registration as a foreign agent under the Foreign Agents Registration Act (FARA).[56] However, membership in either of these bodies is indicative of the CCP's awareness of a particular individual and desire to align their activities with CCP priorities, which may present a comparatively higher risk of bribery, corruption, and/or extortion through their proximity to state power.

Certain groups within these consultative bodies are designed specifically to capture business elites. For example, at the national level, the China People's Political Consultative Conference has a constituent committee that functions as a national chamber of commerce, the All-China Federation of Industry and Commerce (ACFIC). The CCP's United Front Work Department, which promotes



A research team including Chinese quantum physicist Pan Jianwei announced in December 2020 that it had established a quantum computer prototype, marking China's first milestone on the path to full-scale quantum computing. Credit: Xinhua via Getty

Party interests by building relationships with elites in China, the Chinese diaspora, and other influential figures abroad, established ACFIC in 1953 to promote the Party's interests among industrialists in China, and was revived in 1979 to implement the party-state's vision of economic reform and opening via both state-owned and private enterprises.[57]

Today, ACFIC functions as a formal institutional channel for private companies to lobby the government within the party-state apparatus. Research on successful policy proposals from ACFIC between 2009 and 2016 indicates that private business leaders' "policy influence stems from their political embeddedness rather than any efforts that challenge the party-state."[58] One previous study found that for 95 of the top 100 private firms and 8 of the top 10 internet companies, the founder or de facto controller was currently or formerly part of the NPC or the CPPCC.[59] Public records and Mandarin-language news reporting indicate that some members of ACFIC leadership and on ACFIC subcommittees also have familial connections to CCP elites, worked previously for the PLA, or participate in ACFIC in their capacity with the Ministry of Public Security, United Front Work Department, or other government organizations.

政治

Political

The Chinese party-state manages industrial associations and party committees as a means of extralegal corporate governance and industry coordination that national security practitioners abroad may not be able to measure easily. State-owned enterprises, publicly-listed companies, and banks are legally required to have party committees, which are intended to influence companies toward CCP policy priorities.[60] While private companies are not necessarily required to have such committees, the number of those that do is growing. According to an analysis of ACFIC survey data by the Paulson Institute, 48.3% of private firms in China have party committees.[61] On average, there has been a 2.1% increase in the number of private firms with reported party committees during Xi Jinping's tenure, which will likely continue to rise given the CCP's recent emphasis on expanding the Party in the 'private sector.'[62] The survey data also indicates that party organizations are more common at larger companies.[63] The China Securities Regulatory Commission requires that all companies listed on Chinese stock exchanges establish Party committees and provide the "necessary conditions" for Party activities.[64]

Industrial associations emerged from supervising ministries that were dissolved but have retained many of the institutional functions of their predecessor organizations, including but not limited to addressing foreign anti-dumping charges, coordinating trade fairs, mediating trade disputes, and others.[65] [66] While the United States and its allies have also promoted industry alliances and chambers of commerce to develop industry, Chinese industrial associations and industry alliances differ in the extent to which the Chinese party-state asserts control over them as an extralegal corporate governance mechanism. In fact, in September 2020, the CCP issued new guidance on strengthening its role in the private sector, calling for the United Front Work Department to strengthen Party leadership of private industry by bringing private entrepreneurs into ACFIC and industrial associations.[67] Milhaupt and Zheng (2015) further note that China's extralegal involvement in the commercial sector via industrial associations differs from state participation in other countries because they enforce rules without the clear legal delineation or neutrality that would protect a company's market operations from excessive or inconsistent state encroachment.[68]

The All-China Federation of Industry and Commerce directly oversees 31 industrial associations in fields such as agriculture, energy, cosmetics, and real estate.[69] Beyond ACFIC-directed industrial associations, the Chinese party-state has also promoted the development of industry alliances in other strategic sectors to realize its industrial policy goals. In an analysis of one example—the Artificial Intelligence Industry Alliance—researchers at the Center for Security & Emerging Technology found that SOEs occupied a disproportionate number of leadership positions in the industrial association given the composition of its membership.[70]

In cases where corporate behavior fails to conform to the interests of the party-state, Chinese regulators can wield an increasingly broad range of expansive national security laws to compel the party-state's policy line through the legal system. In recent years, the National People's Congress has passed a blizzard of national security laws related to cybersecurity, counterespionage, counterterrorism, anti-sanction, and data sharing, which codify formerly extralegal mechanisms for party-state intervention in the economy and leave Chinese companies under the constant threat of legal action should the party-state so choose.[71] In her book on the party-state's use of antitrust law to regulate Chinese companies, Angela Zhang (2021) quotes one anonymous Chinese businessman in saying that "the law in China does not have only a few grey areas: it is one big grey area. The authorities can tolerate a practice for years then round people up on an arbitrary basis."[72] When faced with the threat of such action from the party-state, enterprises are expected to fold. Zhang (2021) also quotes a former

director-general of the National Development and Reform Commission's [NDRC's] antitrust subdivision, who stated on television that "regardless of whether your company is the subject of an investigation, if you give yourself up voluntarily and cooperate, you can receive a lesser punishment or avoid it altogether."[73] NDRC officials have warned foreign firms against using China's legal system to resist regulatory action, imposing higher fines as punishment on those who attempt legal resistance.[74]

In sum, China's party-state apparatus interacts with companies in a networked corporate environment to support its policy objectives through formal and informal mechanisms. These include appointing and managing leadership at SOEs, gatekeeping access to financial and capital markets, managing universities with significant commercial activities, co-opting private sector executives in formal political institutions, and coordinating enterprise through industry associations, party committees, and regulatory policy. While those mechanisms do not guarantee full control over companies, they provide a range of tools to coerce or induce companies toward the party-state's policy objectives in ways that are both similar to and distinct from mechanisms for state-business relations in countries like the United States. In order to characterize the relationship of a commercial actor to the Chinese party-state, national security practitioners must take a networked approach that considers the many complexities of ownership and control in China's political economy.

Liang Wengen, vice president of All-China Federation of Industry and Commerce and chairman of Sany Group, gives a speech on stage during China Top 500 Private Enterprises Summit 2019 on August 22, 2019 in Xining, Qinghai Province of China. Credit: VCG/VCG via Getty Images

THE PARTY-STATE'S DATA FOOTPRINT

Party-state interactions with the commercial sector leave an extensive data footprint in publicly available sources, which can help identify national security risks.

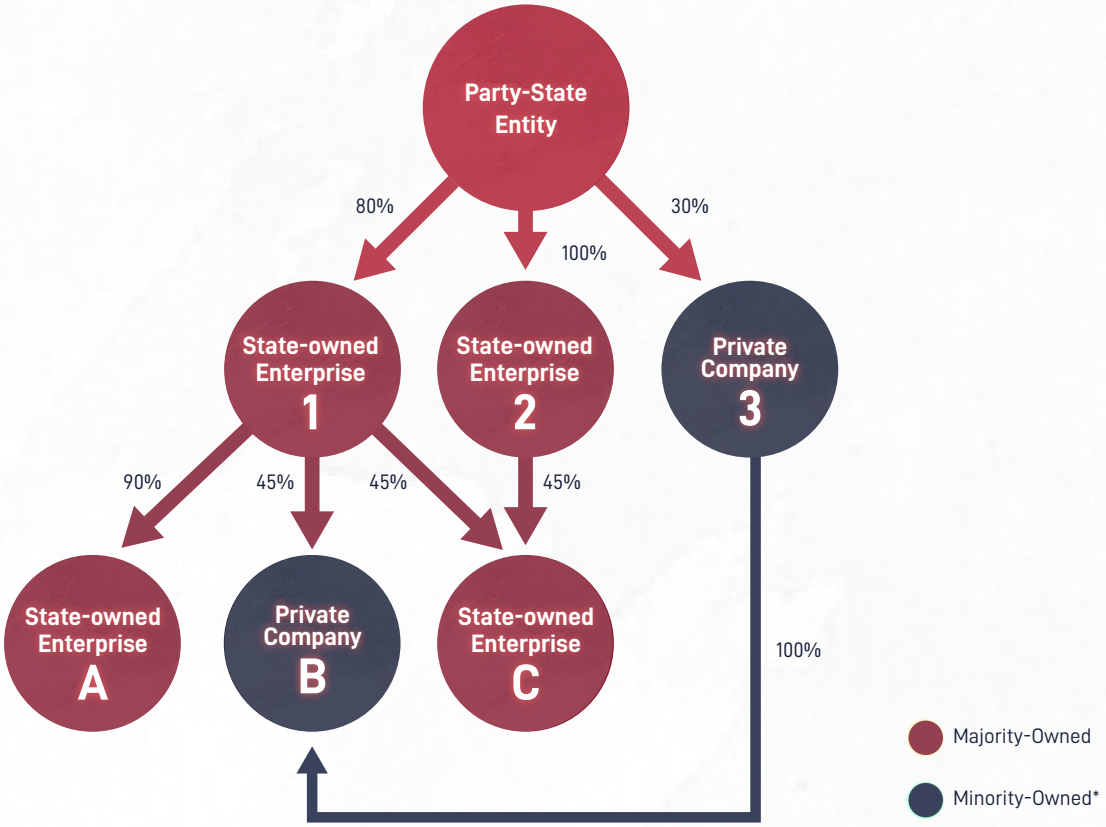
Party-state networks leave an extensive data footprint in their interactions with the commercial sector. To support assessments of national security risk, C4ADS developed a framework to connect available data to possible indicators that a commercial actor may advance Chinese state interests through the course of its normal profit-seeking activities or as the result of party-state coercion. In doing so, we integrated conceptual frameworks about Chinese state-business relations developed by such scholars as William Norris (2016) and Meg Rithmire (2021), emphasizing indicators that can be assessed with the breadth of publicly available information sources.[75] While indicators may not be entirely mutually exclusive, each contains elements that help contextualize the relationship of a commercial actor to the party-state, which in turn can help assess the possibility that a commercial actor could become an instrument of Chinese economic statecraft. As such, the framework should support analysis across a range of national security issues that relate to party-state involvement in the commercial sector like technology competition, corruption, threat finance, and political inference.

INDICATOR	OBSERVABLE FEATURES	LOW VALUE	HIGH VALUE
Party-state equity	Shareholders, shareholdings, and other control relationships	No party-state equity	Wholly state-owned
Political exposure	Director/shareholder affiliations (with political bodies or elite families), firm size	No exposure	National champion
Industry sensitivity	Political campaigns, national strategic planning documents, cooperation with CCP talent programs	Not sensitive	Strategic priority
Market structure[76]	Number of firms, market share, pricing power	Highly competitive	Concentrated
Goal compatibility[77]	Profit motive, state defines goals, mutual exclusivity of state and actor goals	Divergent goals ("crony capital"[78])	Convergent goals ("tactical capital"[79])

Policymakers can collect evidence for each of these indicators from a variety of publicly available sources:

- Corporate registries and other datasets that describe corporate structure, investors, employees and ultimate beneficial ownership;
- Property and land registries that indicate the ownership of physical assets at key facilities;
- Asset registries, such as those for property, vessels, and aircraft;
- Tender data that details government contracts, the companies supporting military technological development, and the capabilities that the Chinese party-state solicits from private enterprise;
- Academic publications, conference proceedings, details of masters and doctoral theses, lists of staff at institutions, science and technology awards, fellowship programs, and other academic-related datasets, which can provide information about possible international exposure to China's military R&D enterprise;
- Entity-level trade data, which includes the organizations involved in the transfer of goods, the nature of the shipment, and the method of transportation;
- Financial records and investment disclosures that indicate the parties involved in mergers and acquisitions or cross-border greenfield investments;
- Venture capital data that indicates the source of funds and financing in key technological sectors;
- Satellite imagery available through commercial providers;
- Signal data for vessel and aircraft positions;
- Domain registration records and web traffic data;
- Data containing selectors used by individuals, including phone numbers, social media accounts, physical addresses, and more; and
- Databases for known PEPs and leadership in China's political institutions.

Party-State Equity



How party-state entities accrue majority equity stakes through layers of companies

*Note: Minority-owned companies may take on one of many structures including but not limited to privately held and publicly traded.

Equity ownership analysis provides critical information about the financial relationship of a company to the party-state.[80] Chinese corporate records are free and publicly available and contain information about shareholders, the size of their equity stakes, and more. When collected at scale, corporate records can therefore provide information about the party-state's cumulative equity stake in a subsidiary company, the distance between a party-state entity and a 'private' company in the network, and the nature and identity of majority shareholders. If the Chinese party-state has a majority interest in the company, U.S. law classifies those enterprises as a "foreign instrumentality," for which U.S. law has clear predicate offenses for national security threats like economic espionage.[81] In many cases, however, classifying a company as a foreign instrumentality may require a more significant investigation, as the party-state's majority stake may only be the result of equity accumulated through several layers of companies and investment pathways.[82]

Political Exposure

A commercial actor's political exposure may provide invaluable information about the extent to which the company is on the party-state's radar. Public lists of Chinese officials, Mandarin-language news reporting, social media, and other forms of publicly available information can help contextualize the relationship of a company to political elites. As a result, assessments can include whether the company's shareholders, directors, or officers concurrently hold leadership positions in the CCP, official state institutions, the company's party committee, or Chinese industrial associations.

Information on entities and individuals can be gleaned from a number of publicly available sources. For example, Chinese government agencies publish the names of officials at the national, provincial, and local levels with pictures and information about their backgrounds. Resumes for public officials often include educational background, previous positions, and other information that provide rich personally identifiable information about key figures. Membership lists are also public for the CPPCC, NPC, and their provincial equivalents but do not always contain the personally identifiable information required to disambiguate a person's identity across multiple data sources. In many cases, investigators can use Mandarin-language news reporting, social media, judicial records, and social network analysis techniques to draw high-confidence inferences in the course of investigations. Third-party due diligence providers like Refinitiv and Dow Jones also build lists of politically exposed persons and their relatives and close associates (RCAs) to support financial crime investigations. Beyond specific people, companies may also advertise their relationships to public officials and industrial associations on their websites. Similarly, local governments or industrial associations may post news stories about activities between local leaders and companies, such as establishing new technology parks or special agreements for investment. For universities, this may include professors who are affiliated with key state laboratories or recipients of major awards from the Ministry of Science and Technology, Ministry of Industry and Information Technology, or United Front Work Department organizations that sponsor or support talent recruitment and technology transfer efforts.

Together, these lists can help determine the extent to which commercial actors may be exposed to the party-state apparatus. While basic CCP membership may be a weak signal given the ubiquity of the Party and the range of incentives that may exist for membership, business leaders who participate in the CPPCC and its equivalents (which exists at all levels of government in China) may have more significant political and legal exposure to the party-state that could create national security externalities in their commercial or academic activities abroad. CPPCC membership is a more reliable risk signal, as it is an invite-only institution designed to connect the Party with private businesses. Similarly, regulators may also look into an individual's participation in the National People's Congress or role in leadership positions within the Party or its constituent committees as a proxy for political exposure.

Industry Sensitivity

An industry's sensitivity can broadly indicate party-state regulators' interest in a given company and suggest how the latter may fit into the CCP's stated policy objectives. The level of sensitivity may also indicate how easily government regulators can achieve unity in enforcing a specific policy line—an essential but not always guaranteed precondition for enforcement in China's highly fragmented system.[83] Policymakers and investors should pay particular attention to the party-state's acknowledged policy priorities such as Made in China 2025, which may create national security risks across certain sectors of the Chinese economy.

In some cases, industry sensitivity may be immediately clear. For example, China has identified specific technologies like semiconductors and biotechnology as priorities for investment and development. However, other industries, such as real estate development, may have specific national security or regulatory salience in China that could expose the company or its executives to extortion risk and, in turn, create national security risks abroad.[84] For example, at the outset of the COVID-19 outbreak, Australian news media cited whistleblowers in reporting that Chinese property developers directed employees at their Australian subsidiaries to pause normal business operations and source personal protective equipment (PPE) for company-sponsored charter flights back to China amid significant PPE shortages for Australian healthcare workers, exacerbating fears in Australia about the country's PPE supply.[85] While other sectors like gambling may not directly intersect with core U.S. national security interests, they are also industries with particularly significant regulatory exposure in China that may subject business executives to an outsize risk of extortion by the party-state.

A man visits a booth of Semiconductor Manufacturing International Corporation (SMIC), at China International Semiconductor Expo (IC China 2020) in Shanghai. Credit: Aly Song/Reuters

Within a given industry, policymakers may look for other data points to characterize the extent to which a given company or university is coordinated with the party-state and its policy priorities. For example, if a company participates in state-sponsored talent programs, the company may formally coordinate activities with the relevant party-state offices responsible for organizing and funding those activities. In some cases, companies indicate participation in talent programs on their websites to advertise the quality of their employees, while in other cases, public resume information (e.g., on professional social media platforms like LinkedIn) can allow investigators to connect talent program award recipients to specific employers.

Market Structure

Relatedly, policymakers should consider the market in which the commercial actor primarily operates, which may have varying degrees of dependence on access to the Chinese mainland. For many companies, market operations and key customers may be available in corporate disclosure documents (e.g., to boards of directors) or other forms of economic data, such as bill of lading-level trade data, cross-border investment records, securities filings, and capital market data. In addition, company websites often include overseas operating locations, which may also be accessible through general internet searches or corporate registries in third jurisdictions. Less obvious forms of data, like the aircraft travel of corporate jets or executives that can be tracked with Automatic Dependent Surveillance-Broadcast (ADS-B) data, may also provide information about a company's growth strategy and impending investment deals.[86] Together, these documents can provide insights into the extent to which a company is dependent on the Chinese market for its current operations or future growth strategy and, as such, the extent to which a company may face commercial and financial incentives to comply with party-state policy priorities.

Similarly, if the company is authorized to produce military equipment or dangerous materials or regularly bids on procurement tenders for the military, it may have commercial dependencies on China's military-industrial complex, which can be assessed through a more thorough investigation of commercial partners and market share. Additionally, Chinese companies listed on domestic exchanges—particularly under concept stocks dedicated to national policy priorities like "military-civil fusion" or on dedicated exchanges like China's technology-focused STAR Market—indicate strong commercial success on technology products that are priorities for the party-state. Their prominence in fields aligned with the party-state's interest may prompt additional scrutiny for their lower-profile subsidiary companies, joint ventures with other Chinese firms (e.g., Chinese defense SOEs), or research partnerships with defense universities or key state laboratories.

Norris (2016) notes that the relative number of resources or expertise between the state regulators and companies has also been a key factor in cases when the Chinese party-state has instrumentalized companies toward its policy objectives. In other words, the Chinese party-state cannot manipulate a firm as easily when the number of companies under its purview or the degree of technical expertise required for oversight and regulation is high. At the sectoral level, U.S. policymakers and regulators should therefore consider the relationship of specific segments of China's economy to the authorities responsible for overseeing it as one variable among several in assessing the risk that a company may be co-opted to advance policy initiatives.

Goal Compatibility

Finally, policymakers should consider the extent to which a company's commercial goals align with the party-state's policy goals, which they can determine from a mix of corporate disclosures, executive statements, Chinese policy documents, and qualitative assessments about the specific people and companies in a given network (e.g., what we know about them and their relationships to Chinese political factions from derogatory reporting, judicial records, or other sources).[87] If a company's normal profit-seeking behavior advances the party-state's national security objectives, the party-state may simply seek to enable the company's commercial success rather than directly control it as a "foreign instrumentality," which may introduce new complexities in establishing a predicate offense required for certain policy responses for risk mitigation.[88] [89] An assessment of a firm's commercial goals and potential alignment with party-state interests may require more qualitative analysis and assessment, proceeding from an understanding of China's stated policy priorities (e.g., Made in China 2025), the commercial actor's primary business activities as declared in corporate registry filings and on its website, and the political relationships of business executives to party-state elites.

When considered together, these data sources can help contextualize the relationships of commercial actors to the party-state and—at the point of interaction with the United States or other places—help policymakers place entities on a gradient of national security risk given the capabilities and intent of the party-state and the company or university. Through high-scale data collection and integration around those indicators, national security practitioners can proactively identify where risk is most acute and develop tailored policy responses.[90]

The closing session of the National People's Congress at the Great Hall of the People on March 11, 2021 in Beijing, China. Credit: Kevin Frayer

A BIG DATA MODEL FOR RISK IDENTIFICATION AT SCALE

A scalable, repeatable process for identifying high-risk Chinese entities with a high degree of fidelity is a critical requirement for U.S. national security efforts to combat national security threats from China's economy.

C4ADS developed a beta big data model to apply the above framework to three threat areas: technology competition, corruption, threat finance, and political interference. This approach demonstrates not only the challenge but also the feasibility of using high-scale data integration and enhanced due diligence as a critical lever in the U.S. policy toolkit to identify and mitigate national security risks from China's commercial and academic ecosystem.[91] In each case, we applied a relatively straightforward three-step process.

Step 1: Build Baseline Data

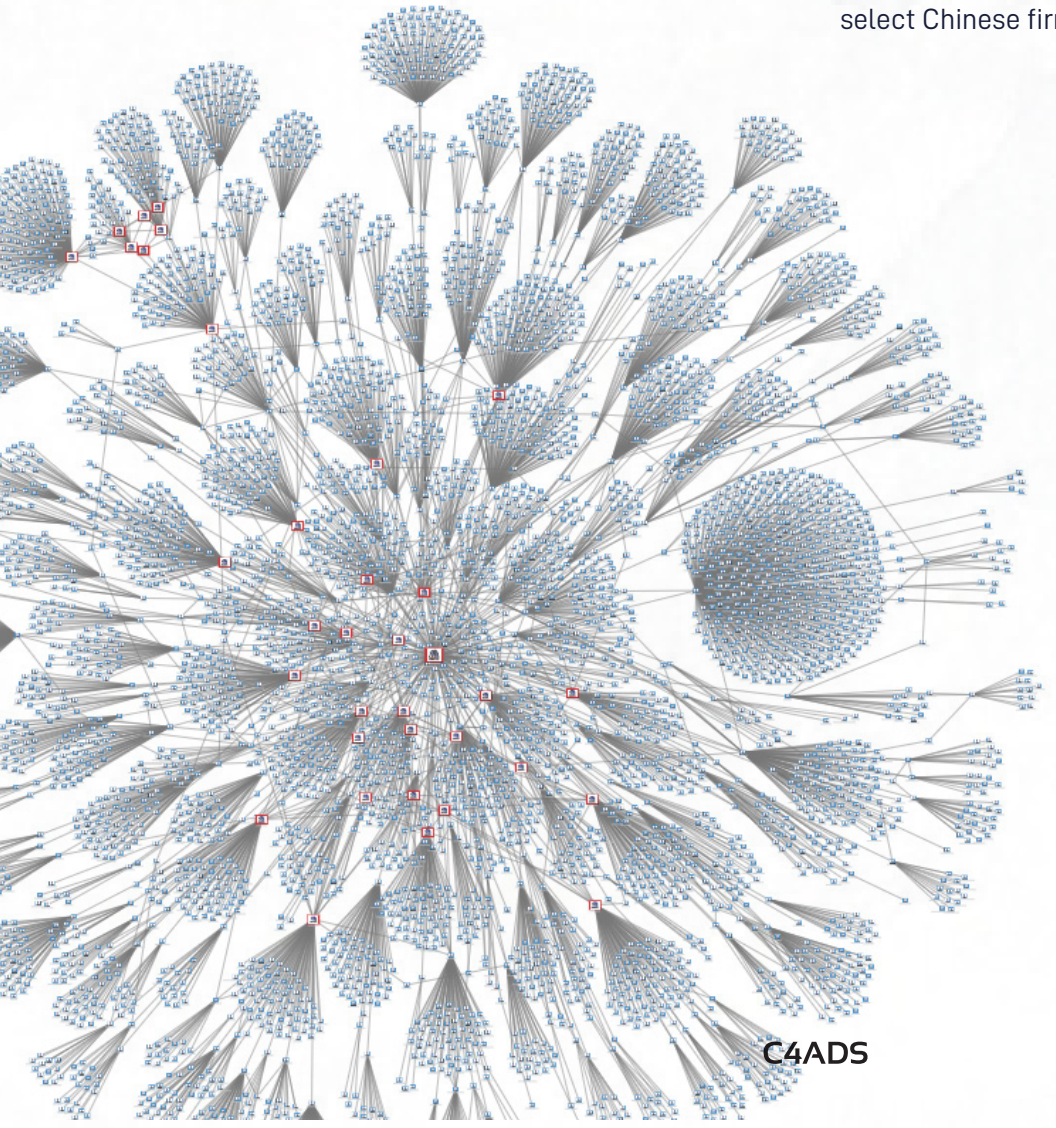
Our first step was to collect baseline data across the segments of China's commercial and academic system where we know the party-state to be involved, as explored in the above section, **The Party-State's Toolkit for Economic Statecraft**. Below, we outline data collected in the beta phase of our project, which we intend to expand in the future.

Commercial

Using corporate registry filings, we mapped subsidiaries of the State-owned Assets Supervision and Administration Commission (SASAC) within five degrees using Chinese corporate registry filings. This identified approximately 34,000 companies with around 8,000 affiliated shareholders and directors. Future work will expand to include provincial- and local SOEs.

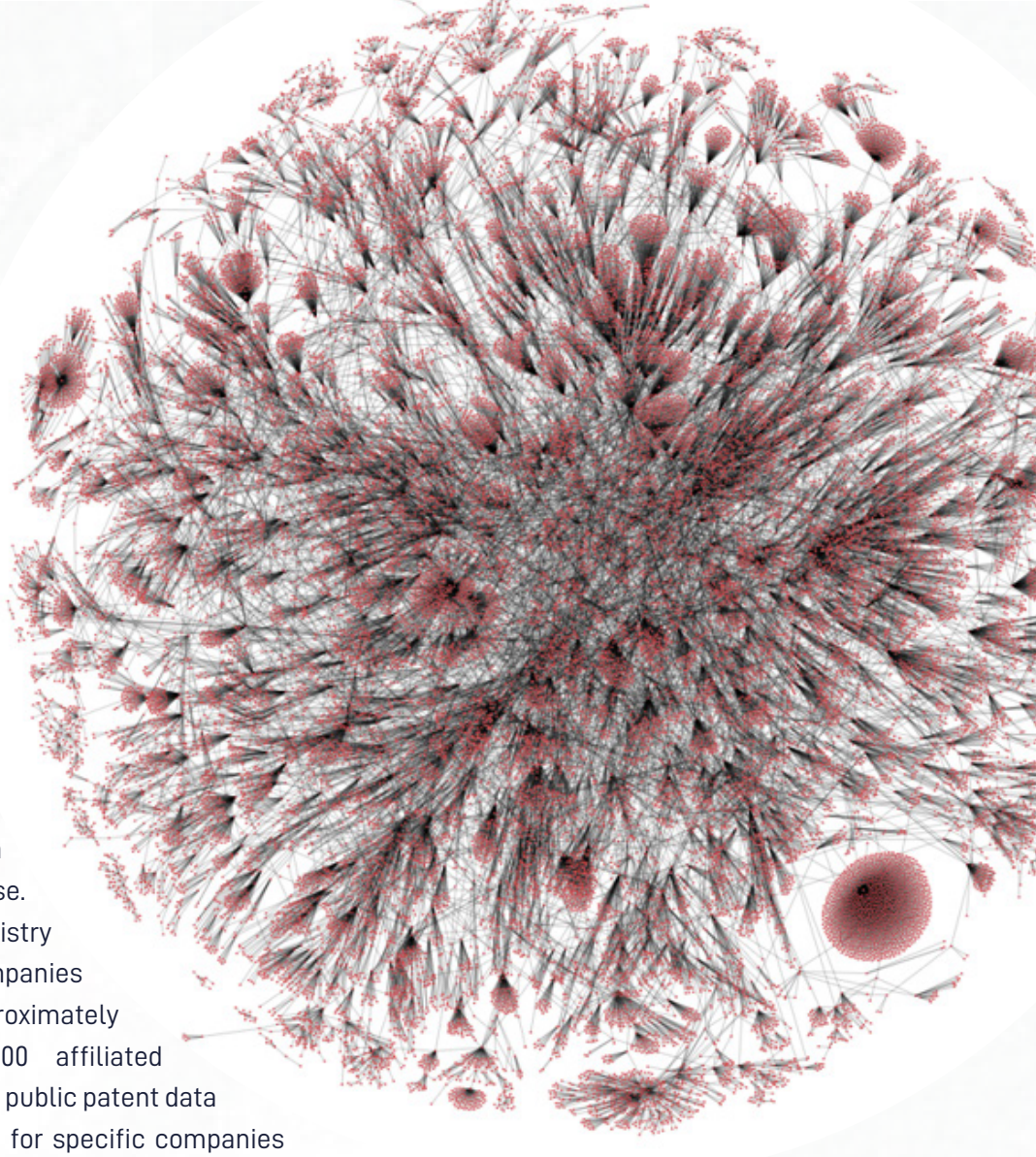
Financial

We identified government-guided investment funds from a third-party aggregator of capital markets data. We also used public corporate disclosures to map ownership for companies listed on Chinese stock exchanges, including information about their key personnel. We also used corporate registry filings to map Chinese state-owned financial institutions (e.g., banks, sovereign wealth funds, asset management companies, and authorized junkets in Macau), and built a database of private equity and venture capital investments by select Chinese firms both domestically and abroad.



Subsidiaries of the State-owned Assets Supervision and Administration Commission

ANALYSIS POWERED BY Palantir



Subsidiaries of investment companies
for China's defense universities

ANALYSIS POWERED BY
Palantir

Academic

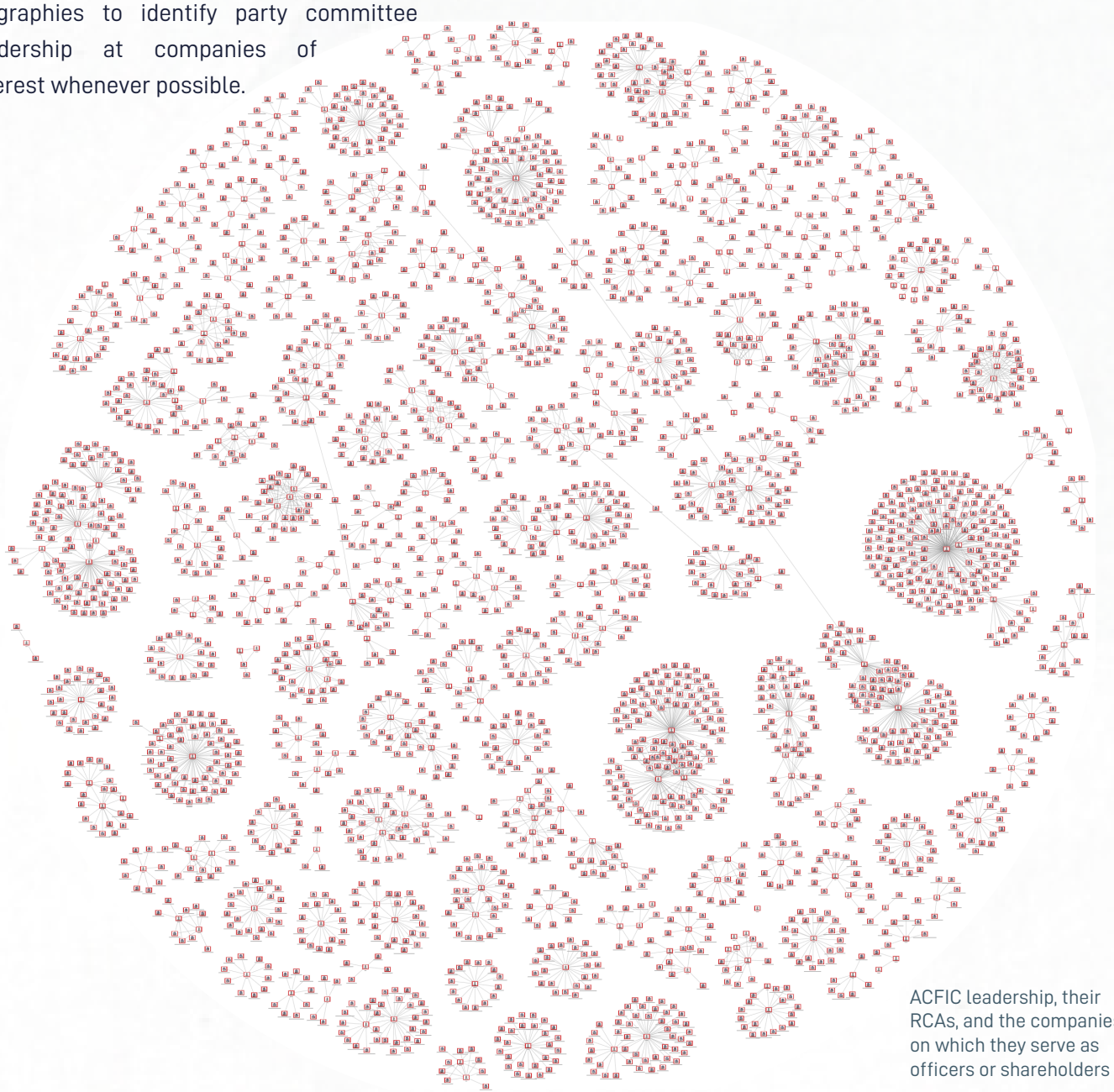
We referenced the Chinese Defense Universities Tracker[92] from the Australian Strategic Policy Institute to identify 115 universities affiliated with China's defense or intelligence enterprise. We then used Chinese corporate registry filings to identify their subsidiary companies within five degrees, which identified approximately 29,000 companies and roughly 6,000 affiliated shareholders and directors. We compiled public patent data and academic bibliographic information for specific companies and research sectors of interest to identify research collaborations between key state laboratories, defense universities, defense contractors, and other previously unidentified companies.

Social

We built a dataset of Chinese politicians and their career information using public Chinese government résumé information for public officials. We also compiled membership lists for China's national- and provincial-level Political Consultative Conferences, which includes approximately 26,000 people. Using Chinese judicial filings and academic reporting, we built a dataset of Chinese organized crime figures. For membership at select organizations of interest, like ACFIC, we also used social media, news reporting, and state media to identify relatives and close associates, a key feature of investigations into politically exposed persons. Where possible, we also used corporate registry information to add information on their affiliated companies, previous affiliations to the military or China's national security apparatus, and other kinds of relationships to the party-state.

Political

We built a dataset of industrial associations under the control of the ACFIC; civil society organizations registered formally to the United Front Work Department; and civil society organizations registered to the CCP. While party committee information is not always public, we used new reporting or company biographies to identify party committee leadership at companies of interest whenever possible.



ACFIC leadership, their RCAs, and the companies on which they serve as officers or shareholders

ANALYSIS POWERED BY Palantir

Step 2: Layer Risk Indicators

As a second step, we applied our risk signals from the previous seciton, **The Party-State's Data Footprint** to identify companies, investors, and universities that may represent an outsize national security risk, which would later be validated by subject matter experts in each core issue area. These indicators can be adjusted over time with new insights and provide a scalable, replicable methodology to dramatically reduce the time required for discovery. In the beta phase of our project, we applied this method to three core national security issues: technology competition, corruption, threat finance, and political interference.

Technology Competition

Goal: To identify companies and academics that work closely with party-state institutions to transfer and commercialize critical technologies of significant national security consequence.

China's science and technology ambitions require that technology be transferred not only from abroad but also from research laboratories into the economy. While Chinese universities file a significant number of patents, they have an extremely low rate of commercialization. To improve commercialization rates, the Chinese government has created policies that allow Chinese universities to invest in companies their faculty start in order to commercialize technology they patent through university affiliations.[93] Given this context, we expect to see a particular risk of international financial exposure to China's military-industrial complex in private or publicly traded companies that work closely with Chinese SOEs, government-guided investment funds, sovereign wealth funds, and defense unversities to develop technologies aligned with strategic policy objectives.

To conduct this analysis, we used Palantir Foundry to process and model the data from Chinese corporate registry filings. This includes bulk machine translations for data fields like "business scope," which allow

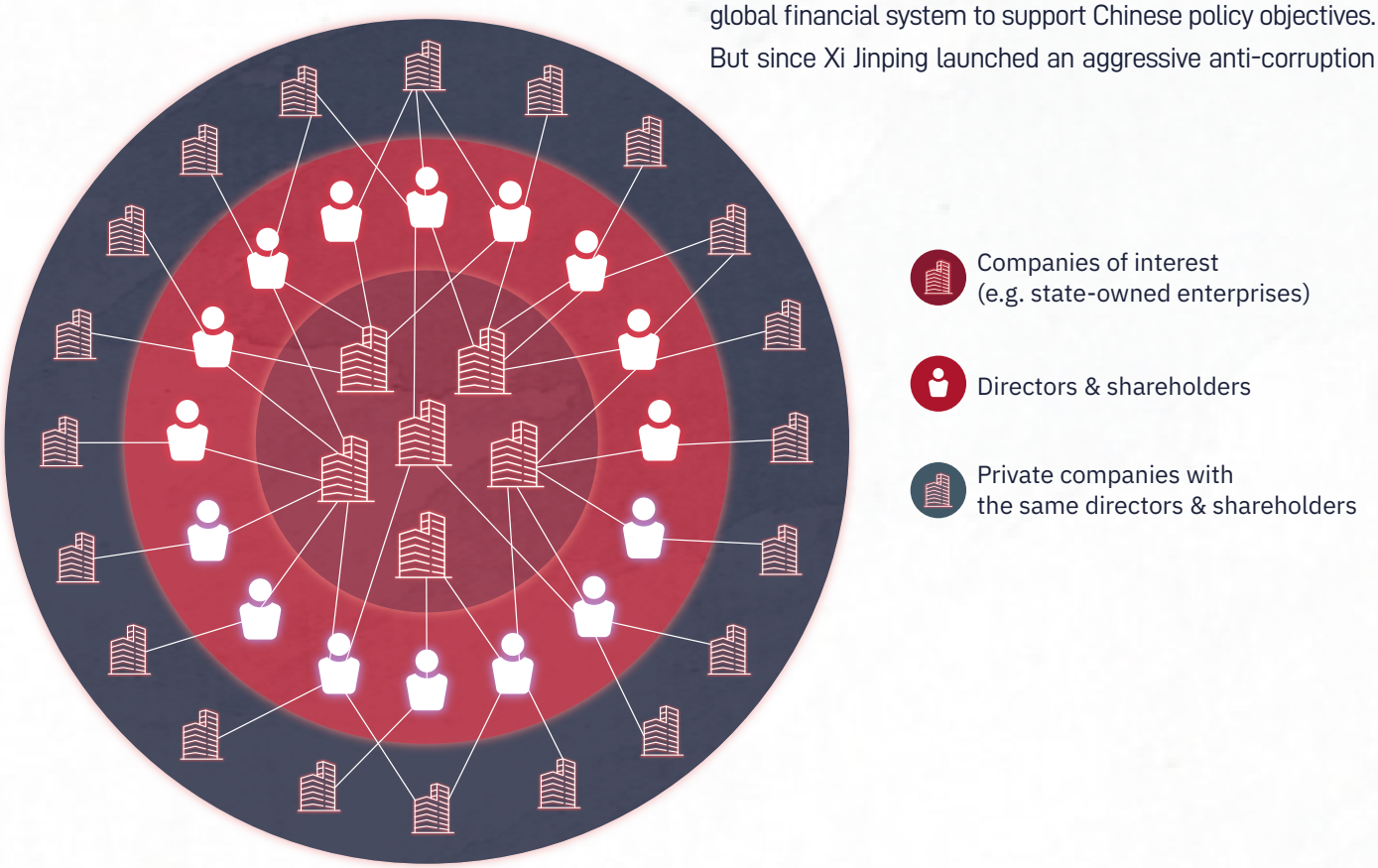
INDICATOR	OBSERVABLE FEATURES
Party-state equity	Companies or universities in which the party-state holds significant equity stakes directly or indirectly.
Political exposure	Company directors or shareholders have simultaneous appointments in Chinese prominent political organizations or key state laboratories.
Industry sensitivity	Work in sectors aligned with state national industrial policy priorities like semiconductors, quantum computing, and artificial intelligence.
Market structure	Dependencies on the Chinese market or Chinese government customers for its commercial success.
Goal compatibility	Profit-seeking activities aligned with party-state national security objectives

for keyword searches on industries of interest like "semiconductors" or "quantum technology." We also enriched the data to record any given company's distance from the original entity of interest, e.g., SASAC or the defense universities, to support questions about the nature of co-investment given network position. Then, we used Palantir Foundry to integrate the data and identify all companies in which both SASAC and the defense universities hold equity stakes, which may represent a higher risk of exposure to China's industrial policy objectives. We similarly identified all company directors and shareholders who hold a position both at subsidiary companies of SASAC and at subsidiary companies of defense universities, which may represent "special investors"[94] with significant proximity to the party-state and party-state capital. As a final step, we screened these datasets against proprietary datasets of Chinese inbound and outbound investment, venture capital flows, procurement tenders, political bodies, academic bibliographic information, lists of personnel at key state laboratories, and other relevant datasets.

Corruption and Threat Finance

Goal: To identify figures in Chinese organized crime or corruption that could use their global financial capacity to advance Chinese national security objectives abroad.

Policymakers have expressed increasing concern that the Chinese party-state may use corruption as an instrument of national power to advance its national security objectives abroad. This may include bribing corrupt foreign officials in support of projects like the Belt and Road Initiative or working with Chinese business elites to launder funds through the global financial system to support Chinese policy objectives. But since Xi Jinping launched an aggressive anti-corruption



Depiction of analytic process to identify co-investments by state-owned enterprises and defense universities

campaign in 2013, we are not interested in determining corruption in the generic sense but specifically corruption that the party-state enables or allows to proceed without consequence, which may indicate some degree of party-state endorsement or complicity.

It is important to emphasize that corruption without consequence in China may not necessarily mean that the party-state has endorsed or supported the corruption. Instead, it could be the result of a corrupt faction that is protected from consequences through "mutual endangerment" with ruling factions, where both sides "hold one another hostage with mutually incriminating information" in "webs of interlocking and competing loyalties."[95] In this sense, closeness to the CCP does not necessarily indicate loyalty or support and instead is a matter of self-preservation and protection. Rather, we treat the confluence of prominence in both criminal enterprises and formal state institutions as an indicator of significant legal and political exposure that could create national security externalities through an individual's international commercial and financial dealings.[96]

To this end, we identified political and organized crime figures with significant financial interests in exposed industries. More specifically, we used Palantir Foundry to analyze people who participate formally in state political bodies like the Party Congress, People's Congress, or Political Consultative Conference at the national and provincial levels. We then identified the intersection between Chinese elites in the political system and our dataset of Chinese officials involved in organized crime or corruption cases. We also used Chinese, Hong Kong, and Macanese judicial filings to map directors and shareholders of Chinese financial institutions, including but not limited to major state-owned banks, sovereign wealth funds, Macanese casinos, and licensed junket operators.[97] We then cross-referenced those individuals identified in association with organized crime and corruption in the region. By identifying individuals with substantial influence over key state-owned financial institutions, exposure to the political apparatus through formal participation in prestigious political bodies, and substantial holdings in both licit and illicit financial systems, we identified individuals who could pose an outsize threat to U.S. national security interests if they leveraged their global financial capacity to support Chinese party-state policy objectives. As a final step, we used Palantir Gotham, a social network analysis tool, to visualize the data and conduct deep-dive investigations.

INDICATOR	OBSERVABLE FEATURES
Party-state equity	Joint ventures with state-owned enterprises or Party elites.
Political exposure	Participation in prominent Chinese political institutions like the CPPCC, NPC, or its provincial and local equivalents.
Industry sensitivity	A significant financial stake in industries that are subject to strict oversight and regulation in mainland China.
Market structure	Dependencies on the Chinese market or Chinese government customers for its commercial success.
Goal compatibility	Profit-seeking activities aligned with party-state national security objectives.

Political Interference

Goal: To identify where Chinese business elites with significant domestic political exposure may participate in political donations and lobbying in the United States.

Chinese business elites with significant domestic political exposure may participate in legal lobbying activities in the United States or abroad with commercial incentives to expand market access. However, in some cases, Chinese business executives may also hold undisclosed, simultaneous appointments in Chinese political institutions, which are neither formal positions in government nor characterized by a patron-client relationship that would require disclosure under FARA. As a result, by allowing multinational corporations to participate in political donations and lobbying without robust disclosure requirements, the United States and other liberal democracies may allow Chinese business elites with a significant risk of bribery, corruption, or extortion inadvertent access and influence in democratic processes.

To identify high-risk networks, we first built a dataset of people who participate formally in state political bodies like the Party Congress, People's Congress, or Political Consultative Conference at the national and provincial levels, and also identified their affiliated companies. We also built membership lists for China's industrial associations and chambers of commerce, which have an explicit coordination function with the party-state apparatus. Where possible, we also supplemented these lists with data on Chinese business elites who have attained foreign citizenship through citizenship-by-investment schemes, which confer visa-free travel for individuals who make investments in countries over a certain threshold.

Next, we processed and modeled public voter records from the U.S. Federal Election Commission that provide information on contributions to political campaigns above a certain threshold. Using our list of political exposed persons and affiliates of multinational companies, we developed fuzzy matching techniques[98] to screen for English and Romanized names against election data, and selected matches above a certain statistical threshold for analyst validation and targeted investigation. As a final step, we used Palantir Gotham to visualize the data and conduct deep-dive investigations. In particular, we focused on people and companies whose commercial activities may support Chinese industries like military satellite communications that undermine U.S. national security interests, even if political lobbying activities are legal under current U.S. law.

INDICATOR	OBSERVABLE FEATURES
Party-state equity	Chinese companies with party-state equity, their shareholders, or their directors made political donations or participated in lobbying.
Political exposure	Companies have a significant proportion of directors or shareholders with simultaneous appointments in Chinese social or political organizations.
Industry sensitivity	Companies have a network position proximate to state-owned enterprises or national champions, and had business activities directly related to stated Chinese national security priorities.
Market structure	Dependencies on the Chinese market or Chinese government customers for its commercial success.
Goal compatibility	Profit-seeking activities aligned with party-state national security objectives.

Step 3: Surface High-Risk Networks for Investigation

Through high-scale data integration and a deductive analytic process, we are able to identify networks of people, companies, universities, and civil society organizations that not only have significant, multidimensional connections to the party-state but also maintain robust engagement with the United States and its allies.

The subsections below provide case studies that demonstrate outputs identified through our approach when applied to technology competition, corruption/threat finance, and political interference. By using publicly available information as data sources of first resort, we are able to develop a high-fidelity understanding of networks that operate in areas of significant national security consequence without the restrictions of classification that may otherwise impede the dissemination of analysis beyond a limited group of stakeholders.

Technology Competition: Defense Laboratories, Quantum, and Financial Markets

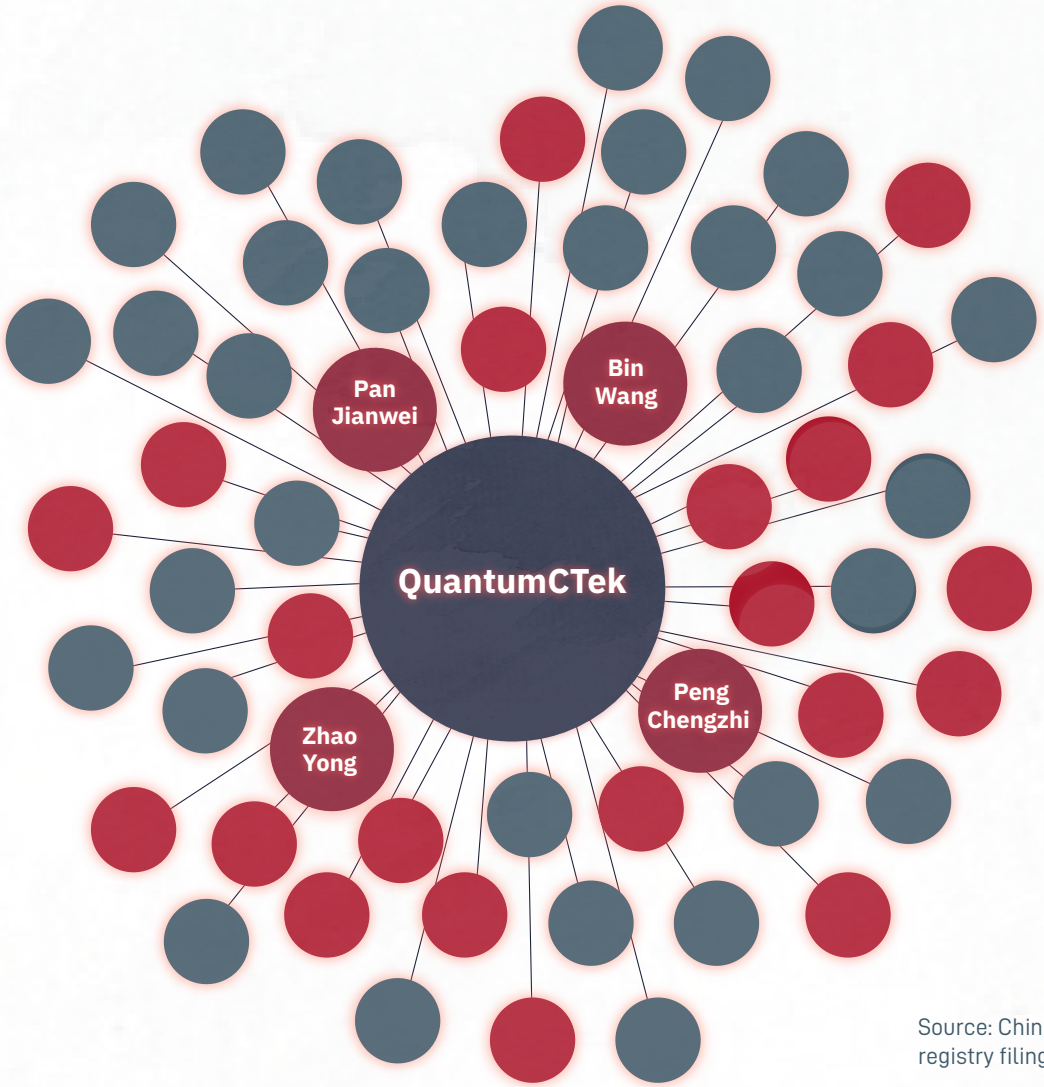
Chinese sovereign wealth funds work with university holding companies to support professors' technology ventures that advance science and technology policy objectives. Professors sometimes hold equity stakes at those ventures through their research and develop significant personal wealth through the success of state-preferred firms. Those firms then benefit from accelerated access to private capital markets through listing on the STAR Market, and can then direct their capital toward other state-backed technology companies in the Chinese market, including those listed by the U.S. government as NS-CMICs or SDNs.

QuantumCTek is a publicly traded quantum communications company listed on the STAR Market.[99] Peng Chengzhi, listed as the company's board chairman and legal representative in Chinese corproate registry filings, is a professor at the University of Science and Technology of China (USTC) and an affiliate of the Quantum Information and Quantum Science Frontier Collaborative Innovation Center (量子信息与量子科技前沿协同创新中心; hereafter "Quantum Center"), one of China's leading laboratories for quantum science.[100] [101] Pan Jianwei, the Quantum Center's director, is listed as a shareholder in the company. Zhao Yong and Wang Bing, two affiliates at the Quantum Center, are also listed as shareholders of the company.[102] [103]

QuantumCTek's directors and shareholders have led some of China's highest profile and most ambitious science experiments. For example, Pan Jianwei, the Quantum Center's director, led China's Micius technology program, which established the first international quantum communications network.[104] The U.S. Office of the Director of National Intelligence and the Departments of Defense, Homeland Security, and State have classified quantum communications as a dual-use technology that, in the hands of adversaries, comprises a "long-range emerging threat" of "high national security consequence."[105] In China's 14th Five-Year Plan, a national-level strategic planning document, Chinese policymakers identified quantum information technologies as a priority for continued development to serve the nation's strategic needs.[106]

Chinese corporate registry filings indicate that Chinese sovereign wealth funds and a university-owned asset management company provided QuantumCTek with seed funding before the company was profitable, and retain some of the largest equity stakes in the company today.[107] According to investment data compiled by Pitchbook, QuantumCTek received its first round of pre-IPO funding from USTC Asset Management Co., the holding company for Peng's and Pan's university, and its second round from CAS Holdings, a sovereign wealth fund operated by the Chinese Academy of Sciences.[108]

After the company became profitable, QuantumCTek received funding from several venture capital companies, including those with private capital.[109] With initial seed funding from a university holding company and a state-owned sovereign wealth fund, QuantumCTek successfully executed a public offering on the Shanghai STAR Market in July 2020.[110] When the company listed, the value of its shares reportedly rose more than 1,000%, with the value of Pan's equity reportedly increasing by more than $34 million.[111]



Source: Chinese corporate registry filings

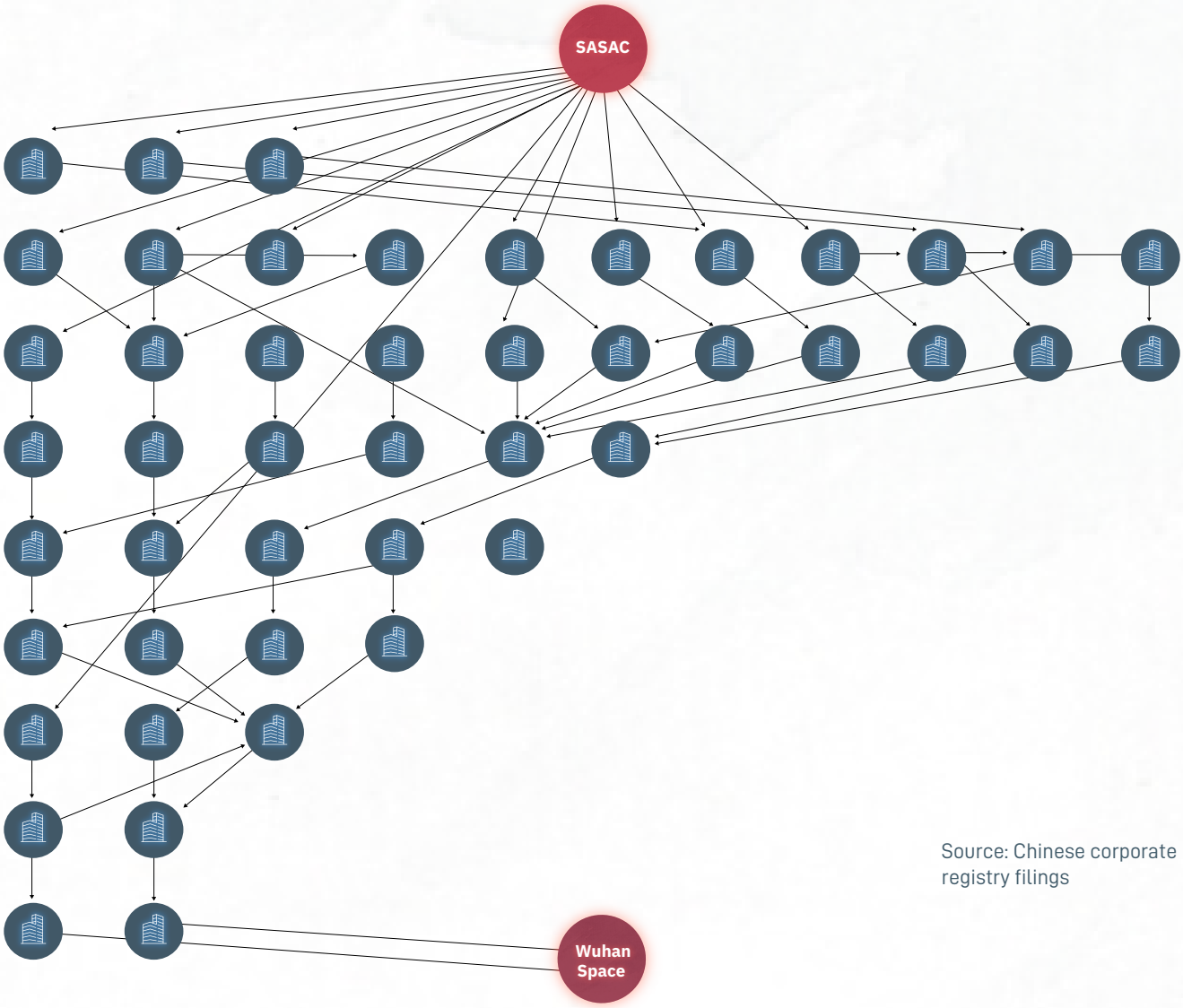
Investor/Investee Companies

Defense Lab Researcher & Director or Shareholder

Director or Shareholder

As QuantumCTek gains expand access to private capital from public trading on the STAR Market, it apparently also maintains investments in other Chinese technology companies, including those that the U.S. government has designated as NS-CMICs or SDNs.[112] Chinse corporate registry filings indicate that QuantumCTek is invested broadly in domestic Chinese companies that are involved in research, development, and commercialization of quantum communications technology, quantum semiconductors, quantum computing, and related technologies. For example, QuantumCTek reportedly holds a 40% stake in Wuhan Space Sanjiang Quantum Communication Co., Ltd. (武汉航天三江量子通信有限公司; "Wuhan Space"), a limited liability company involved in the research, development, and sale of quantum communications technology.[113] Wuhan Space is a subsidiary of the state-owned defense conglomerate China Aerospace Science and Industry Corporation (CASIC), which the U.S. Department of the Treasury classified as an NS-CMIC in June 2021.[114] The State-owned Assets Supervision and Administration Commission (SASAC), which oversees China's national

Investment Pathways from SASAC to Wuhan Space



Source: Chinese corporate registry filings

SOEs, is, according to Chinese corporate registry filings, the company's ultimate beneficial owner, controlling 42% of Wuhan Space's stake through more than 10 investment pathways that are four layers or greater in depth.[115]

Beyond SOEs, QuantumCTek also appearts to have significant investments in the subsidiary of a privately held Chinese company that the United States has classified as a national security threat.[116] QuantumCTek reportedly holds a 34% stake in Nanjing Yiteteng Information Technology Co., Ltd. (南京易科腾信息技术有限公司), a privately held quantum computing company.[117] Chinese corporate registry filings indicate that Nanjing Yiteteng's ultimate beneficial owner is Hou Weigui, the founder of the Chinese telecommunications company ZTE Corporation. In June 2020, the FCC issued an order determining that ZTE poses a national security threat to the security and integrity of the nation's communications networks and communications supply chain because of their size, their close ties to the Chinese government, and the security flaws identified in their equipment," prohibiting the U.S. government from using certain funds to purchase ZTE products for use in the U.S. telecommunications infrastructure.[118] Zhao Yong, the Associate Director of the Quantum Center and a shareholder at QuantumCTek, is listed in corporate documents as serving on Nanjing Yiteteng's board of directors.[119]

The QuantumCTek case illustrates how publicly available information can help identify how the Chinese party-state coordinates sovereign wealth funds, universities, and capital markets to direct significant state capital toward preferred technology ventures, enriching professors and researchers in the process. It also provides a means by which to identify the privately-held and publicly-traded firms that the Chinese party-state has preferred to advance its science and technology ambitions, which can help policymakers in risk identification and response.

Corruption and Threat Finance: Organized Crime, Kleptocracy, and China's Belt and Road Initiative

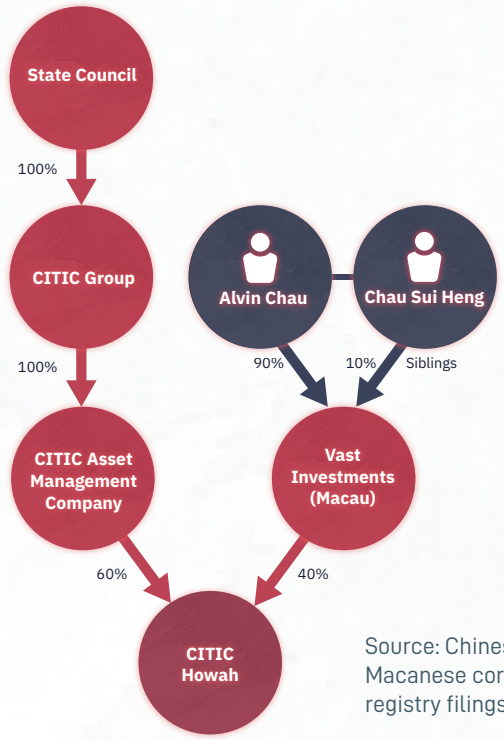
Prominent Chinese organized crime figures serve in formal Chinese political institutions and support Chinese foreign policy objectives while simultaneously using their international commercial enterprises for money laundering. Some of Macau's most significant junket operators, which reportedly have extensive connections to regional organized crime networks, participate in political institutions in mainland China, enter joint ventures with Chinese state-owned financial institutions, and launder funds for Chinese leadership through their corporate presence abroad

In December 2019, Alvin Chau, a Macanese gaming magnate reportedly associated with the 14K Triads,[120] acquired a significant stake in a Chinese state-owned asset management company alongside the CITIC, one of China's largest state-owned investment companies.[121] In 2007, Chau founded SunCity Group.[122] Today, SunCity Group is the largest junket operator in Macau, reportedly boasting a VIP market share of 45%.[123] To put this figure in context, in 2019, the Macau government reported MOP$135.2 billion (nearly US$17 billion) in VIP baccarat revenues, the primary data point for VIP-junket operations.[124]

Today, SunCity is a diversified conglomerate known for its "integrated entertainment" model, incorporating non-gaming services in its clubs such as travel, food and beverage, and non-gaming entertainment.[125] Some news reports have framed SunCity's expansion beyond gaming as an effort to soften SunCity's image from regulators who scrutinize casinos and junkets for links to organized crime and illicit finance.[126]

Chinese corporate registry filings indicate that in December 2019, Alvin Chau acquired a near-40% stake in a joint venture with the Chinese state-owned

CITIC Howah Ownership Structure



Source: Chinese and Macanese corporate registry filings

asset management company CITIC via a company he controls in Macau, and was appointed deputy director of the board. The joint venture, CITIC Howah Asset Management Co. Ltd. (中信浩华资产管理有限公司; "CITIC Howah") is ultimately owned by the State Council, the chief administrative authority in China, via a controlling 60% stake.[127] According to its website, CITIC Howah's three main business lines are distressed assets investment, asset management, and brokering the sales of state-owned assets,[128] and it has a controlling stake in at least 23 financial institutions across mainland China.[129] Macanese corporate registry filings indicate that Alvin Chau and his older sister jointly own the Macau-domiciled investment company that holds CITIC Howah's remaining 40% stake.[130] However, this investment was not Chau's first foray into political exposure in mainland China: in 2013, he was appointed

to the Guangdong provincial committee of the CPPCC for a five-year term.[131]

Four months before acquiring his stake in the CITIC Howah, Chau was expelled from Australia for his extensive organized crime connections.[132] In August 2019, amid a multi-year money laundering probe, Australia's Home Affairs Department expelled Chau from the country for his connections to organized crime, which are well documented in publicly available information sources.[133] According to a leaked report from the Hong Kong Jockey Club, which holds a monopoly on gambling in Hong Kong, Chau was believed to be (or was formerly) a member of the 14K triads, and other "SunCity key personalities have demonstrated links to numerous triad societies and organized crime figures."[134] In particular, Chau is said to have started in the junket industry under Wan Kuok-koi (尹國駒), aka Broken Tooth Koi ("Wan"), a figurehead in Macau's 14K triad syndicate, and maintained a relationship with him before Wan's release from a Chinese prison in December 2012.[135] Notably, following his release from prison, Wan launched multiple commercial ventures in Sihanoukville, Cambodia, where Chau also has business interests.[136] In December 2020, the U.S. Department of the Treasury's Office of Foreign Assets Control (OFAC) designated Wan for bribery, corruption, and graft in Cambodia and Palau, where he allegedly met with public officials under his title as a member of the CPPCC while establishing front companies for 14K triad operations.[137] A preliminary investigation found no evidence that Wan and Chau had joint business ventures in Cambodia.[138]

Chau has substantial commercial partnerships worldwide with individuals investigated for corruption and organized crime, including in U.S. allied countries.[139] For example, following Chau's expulsion from Australia, Cheng Ting Kong (鄭丁港), who appears on Macanese registry filings alongside Chau as a SunCity Group shareholder, reportedly continued to operate SunCity's junkets at the Crown Melbourne, a casino at which high net-worth Chinese individuals, including Xi Jinping's cousin, were investigated for laundering significant amounts of money.[140] Australian media outlet The Age cited financial records indicating that SunCity's bank accounts in Macau moved at least AU$500 million into and out of Australia through its private room at the Crown Casino.[141] In November 2016, the Australian government reportedly added Cheng to the Australia Priority Organization Target list, which has been described as containing the "top tier of groups involved in serious and organized criminal activity causing harm to the Australian community."[142] In his capacity as chairman of the publicly traded company Sun International Holdings, a horse breeding and racing company based in Hong Kong, Cheng reportedly acquired an AU$75 million stake in Australia's horse racing industry.[143] Corporate registry filings further indicate that Cheng and his wife Yeung So Mui (楊素梅) have substantial diversified business interests in such sectors as entertainment, energy, technology, and property development not only in East Asia but also in Australia and Canada.

Additionally, in 2018, SunCity Group entered into a partnership with Golden Sun Sky Entertainment Co., Ltd. ("Golden Sun") to develop a US$360 million casino in Sihanoukville, Cambodia.[144] Golden Sun was reportedly part of Chinese investment group Yunnan Jingcheng Group Co., Ltd. (云南景成集团有限公司) ("Yunnan Jincheng"), chaired by Dong Lecheng (董勒成) at the time of its partnership with SunCity.[145] One of the richest men in Yunnan Province, Dong is involved in the real estate development, aviation, and leisure businesses.[146] Dong has made statements at corporate events saying that Yunnan Jingcheng will cooperate with the local Yunnan governments in various social projects.[147] According to a Caixin report, Dong was investigated in 2014 by the Kunming People's Procuratorate for bribery and had been operating casinos across the Chinese border in Myanmar.[148]

In Hoiana, Vietnam, SunCity partners with Gold Yield Enterprises, a company reportedly controlled by the Cheng Yu-tung family (via Chow Tai Fook Enterprises).[149]The Cheng family is one of Hong Kong's wealthiest families,[150] and in 2012, *The New York Times* reported that Cheng Yu-tung had personal business ties with former Chinese premier Wen Jiabao that were used to expropriate the Wen family's wealth.[151] Other reporting indicates that Chau and SunCity have pursued business ventures in such countries as Russia,[152] Japan,[153] the Philippines, and the Isle of Man.[154]

In a July 2020 video, Chau said that SunCity Group has a "wholehearted devotion to the motherland" amidst swirling rumors about the company's solvency and relationship with regulators.[155] Given the extensive reports of Alvin Chau's involvement with not only organized crime and corruption but also centrally owned party-state financial institutions, his reported relationship to the Chinese party-state cannot be easily characterized as one of traditional patron-client relations nor one of mutual trust. Instead, the relationship might be described as one of "mutual endangerment," in which all parties "hold one another hostage with mutually incriminating information" but are ultimately protected through "webs of interlocking and competing loyalties."[156] Regardless of Chau's relationship to China's party-state, he and his companies would likely demonstrate an outsize financial crime risk to U.S. allies around the world and demonstrate the potential for serious national security threats to emerge from China's commercial system, not necessarily from Chinese economic statecraft but instead the systems of collusion that are endemic in the economy.

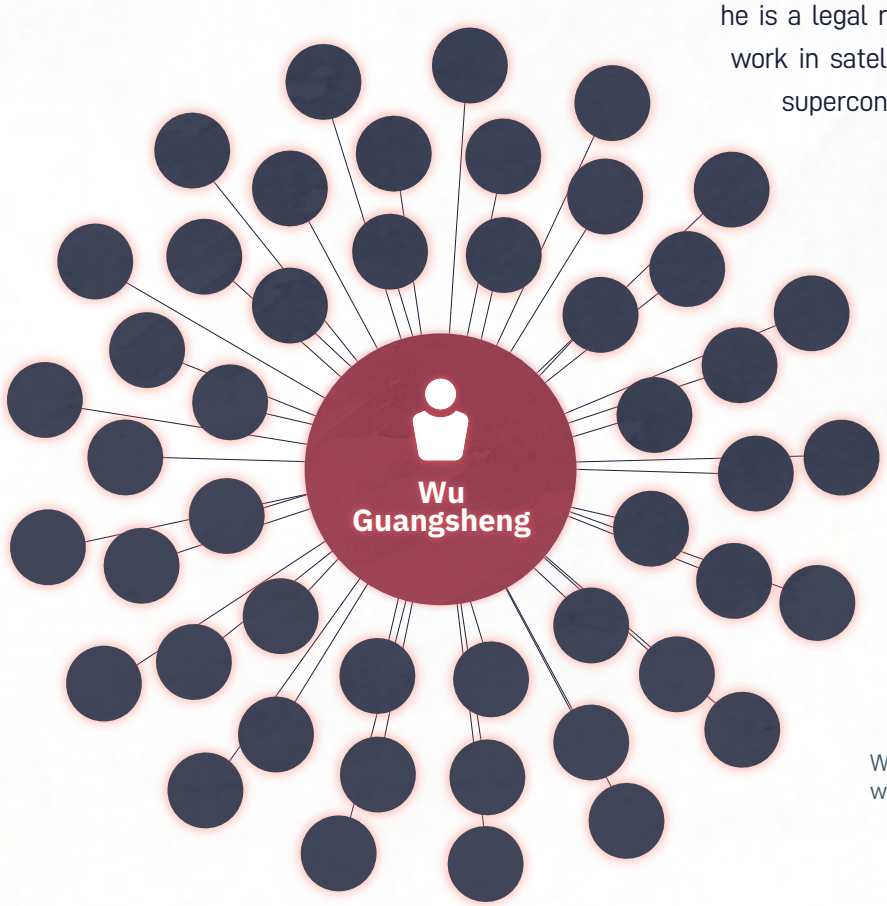
Alvin Chau (left) and Dong Lecheng (right) signing agreement for casino project in Sihanoukville, Cambodia (taken September 2018)[157]

Political Interference: PLA-affiliated Satellite Companies Lobbying in the United States

Many Chinese business elites lobby legally in the United States in their capacity as business leaders, including for companies related to China's military-industrial complex, even though they also serve in prominent Chinese political institutions.

In June 2020, *The Wall Street Journal* reported that Wu Guangsheng (吴光胜), the chairman of a publicly traded Chinese satellite technology company that develops technology with the PLA, attended Republican strategy meetings and met directly with then-President Donald J. Trump and then-Secretary of the Treasury Steve Mnuchin.[158] He did so alongside lobbyists and researchers who made donations to Trump's re-election campaign and were not registered as foreign agents with the Department of Justice under FARA.[159]

Wu Guangsheng's company is prominent in China's military-industrial complex. Chinese corporate registry filings indicate that Wu Guangsheng is the founder, chairman, and general manager of Huaxun Fangzhou Co., Ltd. (华讯方舟股份有限公司; "Huaxun Fangzhou"), a publicly traded satellite company listed on the Shenzhen stock exchange as a "military-civil fusion concept stock" (军民融合概念股票).[160] Chinese corporate registry filings also indicate that SASAC holds a minority equity stake in the company via its direct subsidiary China Hi-Tech Group Co., Ltd. (中国恒天集团有限公司), a textile equipment manufacturer. According to Huaxun Fangzhou's stock disclosures and news reports, more than 90% of its business revenue is estimated to come from the military telecommunication and satellite products it develops.[161] [162] Beyond Huaxun Fangzhou, Wu Guangsheng is an officer or shareholder of 47 companies, and for 36, he is a legal representative.[163] Those companies primarily work in satellite, computing, microelectronics, batteries, superconductors, and other technology.[164]

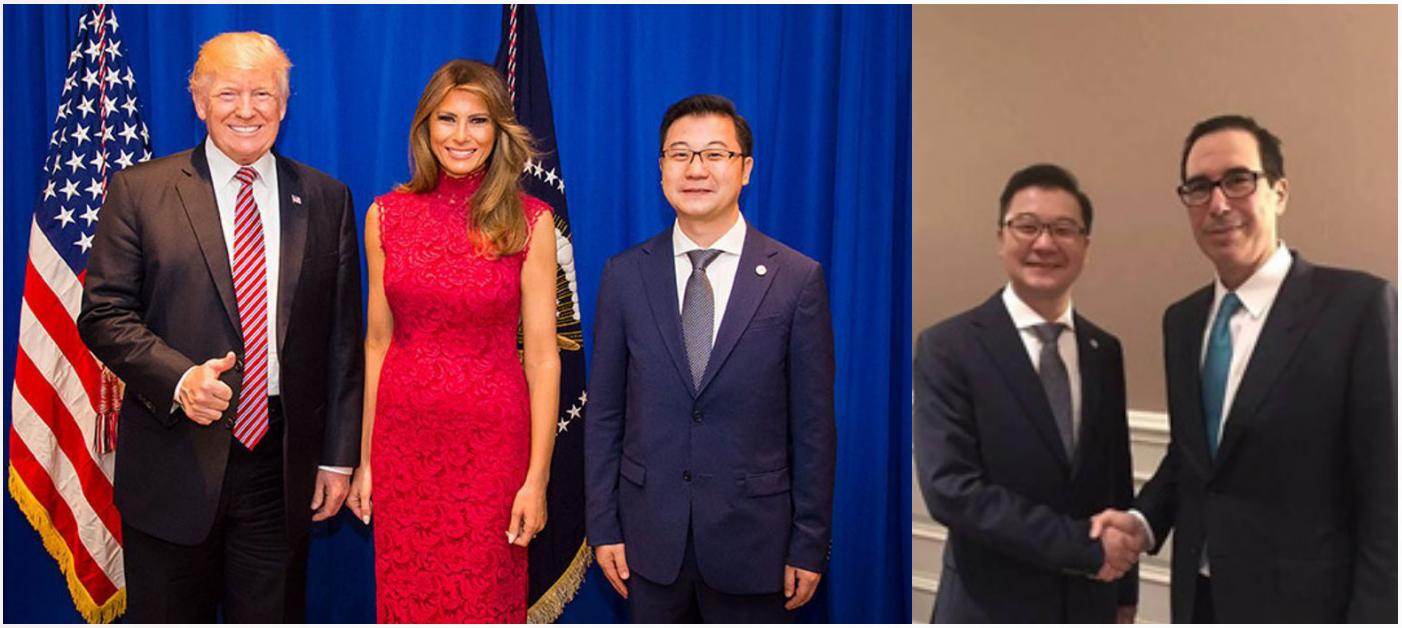


Wu Guangsheng and companies for which he is a director or shareholder

Wu Guangsheng maintains several concurrent leadership positions in political, social, and academic associations directly affiliated with the party-state.[165] Since 2017, Wu Guangsheng has served as a member of the Executive Committee of the All-China Federation of Industry and Commerce, which is subordinate to the United Front Work Department and connects the party-state with private enterprise.[166] He is also a deputy director of ACFIC's Young Entrepreneur Subcommittee.[167] At the same time, Wu is also a representative in the city-level Shenzhen People's Congress as a member of the CCP.[168] [169] In 2019, he was recognized in the People's Daily in the "Fifth Cohort of National Private Sector Outstanding Builders of Socialism with Chinese Characteristics."[170]

Wu Guangsheng's companies have commercial and academic exposure to the United States and its allies.[171] Huaxun Fangzhou's website indicates that it works directly with a range of American technology companies and Chinese companies that work with China's military, including not only state-owned defense contractors but also publicly traded companies like ZTE that the FCC has classified as national security threats.[172] Huaxun Fangzhou operates academic centers that collaborate with Chinese defense universities and universities abroad.[173] For example, in 2014, Huaxun Fangzhou established a research institute with Tianjin University, the Chinese Academy of Sciences, and several other universities with the stated goal of "promoting the commercialization of international and domestic terahertz technology," which has applications in high-bandwidth communications, ultrahigh-resolution imaging, and remote sensing.[174] On its website, the institute lists as partners not only Chinese defense universities like the Harbin Institute of Technology but also foreign universities like the United Kingdom's University of Liverpool and Canada's University of Waterloo.[175] The company's center hosts biannual conferences on terahertz batteries that bring leading experts on the technology from the United States, Germany, Japan, South Korea, Israel, and other countries to events with the leadership of major Chinese state-owned defense conglomerates.[176] The company's website includes profiles of visits by researchers not

Commercial partners as listed on Huaxun Fangzhou's website



Wu Guangsheng with former President Donald J. Trump (Source: Wall Street Journal) and former Treasury Secretary Steven Mnuchin (Source: Huaxun Fangzhou WeChat account).

only from the United Kingdom and Germany but also from the PLA and state-owned defense contractors.[177] [178]

Despite these extensive connections to China's political institutions and military-industrial complex, Wu Guangsheng has also been politically active in the United States through his role as CEO of Huaxun Fangzhou.[179] In June 2020, *The Wall Street Journal* reported that Wu Guangsheng achieved access to U.S. politicians, including then-U.S. President Donald J. Trump.[180] Wu Guangsheng also reportedly met with senior Republican National Committee members Ronna Romney, Elliot Broidy, Shawn Steel, and then-Secretary of the Treasury Steven Mnuchin, according to an article published on Huaxun's social media.[181] *The Wall Street Journal* reported that the dinner was "a Republican National Committee leadership meeting in San Diego and an invite-only gathering where GOP leaders discussed re-election campaign strategies and other issues." [182]

Because Chinese business elites may participate in political institutions that confer prestige and exposure, they may inadvertently expose the United States and other liberal democracies to national security risks through their otherwise legal lobbying activities.[183]

CONCLUDING DISCUSSION AND RECOMMENDATIONS

It is possible to proactively identify national security threats from China's economy through high-scale integration of publicly available information, which can produce outputs with the timeliness and granularity required to be actionable by law enforcement and civil regulators.

China's political economy poses systemic national security risks to the United States and other market-oriented liberal democracies. In order to properly identify and mitigate national security risk, policymakers must be attentive to the formal and informal mechanisms through which the party-state exerts control or influence over commercial actors, which are both similar to and distinct from state-business relations in market-oriented liberal democracies. National security practitioners will continue to face challenges in identifying and mitigating national security threats in China's economy because its commercial systems are complex, diversified, and politicized. However, publicly available information can provide a substantial amount of detailed material to help policymakers assess the relationship of a commercial actor to the party-state and, in turn, develop policy responses tailored to specific risks on a case-by-case basis.

While this report demonstrates the significant potential of using open source information to respond to threats from China, recent events also highlight the potential risks of doing so without the proper ethical or conceptual frameworks. For example, in a June 2021 trial against a former University of Tennessee at Knoxville associate professor Anming Hu, federal agents admitted to falsely accusing Hu of being a Chinese spy based on a "rough translation" of a Mandarin-language flier identified in a Google search, which began a multiyear economic espionage probe.[184] Evidence presented in the trial showed that university administrators struggled to explain disclosure policies to Dr. Hu, and what federal agents may have perceived as intentional omissions from his academic record may have, in fact, been the result of unclear disclosure policies and reporting requirements related to conflicts of interest and Chinese technology transfer.[185] The case highlights the many complexities about using open source information into the intelligence enterprise, particularly as it relates to national security threats from China.

The first is that while open source information may be low-cost and easy to access, the methods for its use and exploitation are not necessarily straightforward. This report demonstrates how useful it can be, but its adoption must be accompanied by rigorous analytic standards, many of which may be unaddressed by compliance frameworks designed primarily for classified information.

The second is that investigations on threats from China require subject matter expertise, which includes both the discernment and linguistic skills to not only find relevant data but also set it in its appropriate context. The data used in this report is predominantly from Mandarin-language sources. While new technology platforms dramatically reduce the technical threshold required for subject matter experts to access and exploit data, they must understand the proper political and technological context to create an analytically rigorous product.

The third is that the long-term success of efforts to counter national security threats from China requires credibility and confidence in the process and approach. Universities and other stakeholders who have traditionally been outside the national security enterprise may reasonably struggle to understand or implement new national security policies related to threats from China, even in good faith efforts to comply. Because publicly available information is free from classification restrictions, it can form the basis of analysis that helps law enforcement and civil regulators more easily show their work and operate from a common understanding with a significant amount of granularity and fidelity. As government efforts to counter threats from China are increasingly subject to public scrutiny, a more effective use of unclassified sources can be a powerful tool to build confidence and facilitate collaboration between the diverse range of stakeholders necessary for protecting and advancing the national interest.

The report's findings inform the following more specific recommendations for law enforcement and civil regulators:

Develop analytic capability, technical systems, and procurement processes that support more effective use of publicly available information (PAI) in the national security enterprise, and improve access to threat assessments for nontraditional consumers of intelligence like state and local governments.

In September 2020, following a two-year review of the U.S. intelligence community's competencies and readiness with respect to China, the House Permanent Select Committee for Intelligence (HPSCI) found that "the United States' intelligence community has not sufficiently adapted to a changing geopolitical and technological environment increasingly shaped by a rising China."[186] Among its unclassified findings, HPSCI stressed that the importance of nontraditional customers receiving intelligence products related to China and the "indispensable" value that open source intelligence can play for a target whose threats to the United States transcend traditional "hard" national security questions like military capabilities.[187] As this report demonstrates, PAI can inform actionable analytic products that are easily disseminated to a wide range of stakeholders—including those outside the federal government like universities or financial institutions on the frontlines of engagement with China. In developing an analytic capability with PAI, policymakers should be attentive to datasets that are beyond the traditional collection taxonomies around which many elements of the intelligence community are organized. Given the broadening range of relevant PAI sources and the expanding group of stakeholders who need access to analysis derived from it, future policy-oriented research and writing should continue to reimagine how the intelligence enterprise should relate to open source information in today's threat and technology environments.

Support joint fusion centers with the Five Eyes and allied counterparts that share resource burdens, promote collaborative analysis, and facilitate coordinated multilateral responses.

China's party-state interacts with the commercial environment in a networked fashion through people, companies, political institutions, and civil society organizations that are transnational in their activities. By developing fusion centers for analysis and information sharing with Five Eyes counterparts, the United States could draw from the complementary expertise, access, and resources of international partners who may have not only critical information related to a key piece of threat network operations but also more capacity to act against a given threat actor. Data management and analysis systems now exist with the security, privacy, and access controls required to collaborate within and across government and industry, even when participants face different compliance obligations or may wish to incorporate sensitive or protected information into portions of their analysis and assessment. By developing new approaches for unclassified data collection, management, and analysis in coordination with allies, the United States and partners can more quickly develop best practices, share resource burdens related to start-up costs and engineering, and facilitate multilateral coordination in policy responses informed from a common operating picture about the nature of the threat.

Develop a national data strategy that coordinates domestic data management reforms with national security concerns related to China.

The United States and its allies should ensure that any domestic efforts to improve data management within the domestic government seize opportunities to improve interoperability with Chinese data sources. For example, the 2020 National Defense Authorization Act mandated that the U.S. government establish a national beneficial ownership registry to consolidate and standardize information about corporate ownership that is currently managed on a state-by-state basis. The relatively straightforward clerical change of requiring that China-domiciled companies with subsidiaries in the United States also include in U.S. corporate disclosures their Chinese name (and unique corporate identifiers in China's commercial registry like the Uniform Social Credit Code) would dramatically improve investigators' ability to conduct due diligence investigations that leverage the full breadth of available sources from Chinese public records. As the U.S. government and allies more broadly reform their approaches to data management and integration, they should ensure that those efforts do not miss opportunities to protect U.S. national security interests against threats from China. This is relevant not only to how data is recorded but also to how data architectures for different government agencies are designed, i.e., with interoperability in mind.

Avoid broad generalizations in threat assessments and policy design.

China's political economy is complex and requires careful attention to how the party-state engages with commercial actors. If policymakers and observers do not appreciate those complexities, they risk producing threat assessments that overstate loose notions of "CCP malign influence" and understate more fundamental vulnerabilities that rules-based, market-oriented systems face in extensive commercial engagements with China's "special deals" economy. In some cases, such as responses to the COVID-19 pandemic or climate change, it is in our national interest to cooperate and collaborate with China. By overemphasizing the extent to which the CCP exerts control over companies, universities, and people in China, we reduce the likelihood that we will be able to seize those opportunities, not only to cooperate on issues of shared concern but also to pursue economic statecraft that changes incentives on commercial behavior divergent from or directly adverse to U.S. interests (like the production of opioid precursors or the use of forced labor in Xinjiang). Additionally, we may distract ourselves from the policy solutions that could more effectively and durably shore up the United States against threats from China, such as increasing transparency in beneficial ownership records for U.S.-domiciled companies, restricting dark money in politics, or combatting racial animus towards the Chinese diaspora (and reinforce our liberal democratic values in the process).[188] These types of policy solutions could inform an affirmative policy agenda that unites the United States and its allies around a shared vision for the future instead of a punitive one that centers solely on countering China.

Invest in Chinese language and area studies in the United States.

Over the longer-term, the United States and its allies need to ensure they have the available expertise required to support the national security mission against threats from China. Doing so will require expanded investments in language and area studies programs within the United States and in programs that attract and retain talent within the U.S. government and policymaking community.

As China's economy continues to grow and globalize, policymakers and regulators in the United States and allied countries will continue to face challenges not only in appraising where the potential costs of engagement with Chinese business systems may outweigh the benefits but also in responding to an ever-broadening range of commercial activities through which China's party-state may conduct economic statecraft. In recent years alone, policymakers in the United States have articulated concerns on issues as diverse as technology transfers that erode U.S. economic and military advantages; illicit financial flows that undermine multilateral efforts in nonproliferation, counterterrorism, and counternarcotics; the deployment of fishing vessels and sand dredgers to assert territorial claims and deplete the global commons; market distortion through noncompetitive economic behavior; and international exposure to China's grievous human rights abuses in Xinjiang and around the world. Over longer time horizons, leaders have expressed strong concerns about constraining choice in certain industries or democratic policies, like facilitating dark money flows, influencing international standard-setting bodies, or changing public opinion. Fundamentally, these risks boil down to whether the party-state can successfully make a commercial actor, university, or civil society organization act in accordance with its interests and policies. As national security concerns continue to expand into spaces outside the traditional intelligence aperture, practitioners will benefit from adopting publicly available information—an analytical tool that can provide timely, actionable insights with high fidelity at a fraction of the cost of more exquisite collection assets.

ENDNOTES

1 Rithmire, M., and Chen, H. (2021). The Emergence of Mafia-like Business Systems in China. Harvard Business School Working Paper, 21-098. https://www.hbs.edu/ris/Publication%20Files/21-098_8bddf731-212d-4939-a3ca-0d708d53c7d3.pdf

2 Norris, W. J. (2016). Chinese Economic Statecraft: Commercial Actors, Grand Strategy, and State Control (1st ed.). Cornell University Press

3 Yang, J. & Wei, L. (2020, November 12). China's President Xi Jinping personally scuttled Jack Ma's Ant IPO. The Wall Street Journal. https://www.wsj.com/articles/china-president-xi-jinping-halted-jack-ma-ant-ipo-11605203556

4 Xie, Y. S., & Yang, J. (2020, October 26). Ant Group to raise more than $34 billion in record IPO. The Wall Street Journal. https://www.wsj.com/articles/ant-group-to-raise-more-than-34-billion-in-record-ipo-11603712848?mod=article_inline

5 Wei, L. (2020, December 20). Jack Ma makes Ant offer to placate Chinese regulators. The Wall Street Journal. https://www.wsj.com/articles/jack-ma-makes-ant-offer-to-placate-chinese-regulators-11608479629?mod=hp_lead_pos4

6 《关于加强新时代民营经济统战工作的意见 Opinion on Strengthening the United Front Work of the Private Economy in the New Era》. Link: http://www.gov.cn/zhengce/2020-09/15/content_5543685.htm

7 "打造一支关键时刻靠得住、用得上的民营经济人士骨干队伍." Translation by Bill Bishop in Sinocism.

8 Subsequent reporting also indicated that Ant Group's IPO would have enriched Xi's political rivals, suggesting that the decision to block it also had a personal calculus outside any national security concerns. See Yang, J. & Wei, L. (2020, November 12).

9 Xu, Chenggang, "The Fundamental Institutions of China's Reforms and Development," Journal of Economic Literature, 2011, 49 (4), 1076–1151.

10 While collusion between governments and private enterprise is common in countries without formal market institutions, Bai, Hsieh, and Song (2019) assess that China's "special deals" system is distinct because of the unusually high administrative capacity of the state that makes special deals broadly available. See Bai, C.-E., Hsieh, C.-T., & Song, Z. M. (2019). Special Deals with Chinese Characteristics. University of Chicago, Becker Friedman Institute for Economics Working Paper, 2019–74, 1–48. https://doi.org/10.2139/ssrn.3391506

11 Perry (2019), pp. 2.

12 Bai, Hsieh, and Song (2019) , pp. 22-23

13 Ibid.

14 For an example of China Poly Group's complex relationship with the Chinese state, see Palmer, A. W. (2018, August 16). The Great Chinese Art Heist. GQ, August 2018. https://www.gq.com/story/the-great-chinese-art-heist

15 Bai, C.-E., Hsieh, C.-T., Song, Z. M., & Wang, X. (2020). Special Deals from Special Investors: The Rise of State-Connected Private Owners in China. National Bureau of Economic Research, Working Paper 28170. https://doi.org/10.3386/w28170

16 Rithmire, M., and Chen, H. (2021).

17 Blanchette, J. (2020, December 1). From "China Inc." to "CCP Inc.": A New Paradigm for Chinese State Capitalism. China Leadership Monitor. https://www.prcleader.org/blanchette

18 In some cases, the Chinese government has attempted to use international investments from its SOEs as political leverage to pressure policymakers in third countries to accept investments or partnerships for other national champions (like Huawei). For example, see Millard, R. (2020, June 13). Boris Johnson faces losing billions if he bans Huawei in the UK. The Telegraph. https://www.telegraph.co.uk/business/2020/06/13/boris-johnson-faces-losing-billions-bans-huawei-uk/

19 Baston, A. (2021, February 16). Confronting Chinese State Capitalism [Video, timestamp 30:13]. Center for Strategic and International Studies. https://www.csis.org/events/confronting-chinese-state-capitalism

20 Leutert, W. (2020). State-Owned Enterprises in Contemporary China. Indiana University Working Paper. https://static1.squarespace.com/static/578f7e4ac534a5c08c478743/t/5e781bb364f35a2e28936903/1584929716451/State-Owned+Enterprises+in+Contemporary+China_Leutert+%28*Accepted+Version%29+.pdf

21 de Graaff, N. (2019). China Inc. goes global. Transnational and national networks of China's globalizing business elite. Review of International Political Economy, 27(2), 208–233. https://doi.org/10.1080/09692290.2019.1675741

22 Leutert, W. (2020). p. 8.

23 Leutert, W. (2018). Firm Control: Governing the State-owned Economy Under Xi Jinping. China Perspectives, 2018(1–2), 27–36. https://doi.org/10.4000/chinaperspectives.7605

24 U.S. Department of the Treasury (2020, June 3). Issuance of Executive Order Addressing the Threat from Securities Investments that Finance Certain Companies of the People's Republic of China & related FAQs; Introduction of Non-SDN Chinese Military-Industrial Complex Companies List. https://home.treasury.gov/policy-issues/financial-sanctions/recent-actions/20210603

25 U.S. Department of Commerce Bureau of Industry and Security. Military End User (MEU) List. https://www.bis.doc.gov/index.php/policy-guidance/lists-of-parties-of-concern/1770

26 Chinese third-party aggregator of private capital markets data

27 Chinese third-party aggregator of private capital markets data

28 Pan, F., Zhang, F., and Wu, F. (2020). State-led Financialization in China: The Case of the Government-guided Investment Fund. The China Quarterly, 1–24. https://doi.org/10.1017/s0305741020000880

29 Chinese third-party aggregator of private capital markets data

30 习近平：自主创新推进网络强国建设-新华网. (2018, April 21). Xinhuanet. http://www.xinhuanet.com/politics/2018-04/21/c_1122719810.htm

31 Chinese third-party Chinese corporate registry aggregator and Ma, R. [@ruima] (2021, February 26). More on semiconductors in China: Number of semiconductor companies registered in China from 2000-2020. Investment was just $1Bn in 2018, grew 6x in 2019, just 1H 2020 was $8.4Bn, the highest of any sector. [Tweet] Twitter. https://twitter.com/ruima/status/1365359788029145088

32 Rui Ma, a technology entrepreneur who first noted these trends, attributes to a combination of government capital, the STAR Market, talent recruitment, and other preferential policies. Ma R. (2021, February 26)

33 Tan, C.K. (2020, July 17). Shanghai's STAR market brings in new dawn for Chinese tech. Nikkei Asia. https://asia.nikkei.com/Business/Business-Spotlight/Shanghai-s-STAR-market-brings-in-new-dawn-for-Chinese-tech

34 U.S. Securities and Exchange Commission. (2020, July). U.S. Investors' Exposure to Domestic Chinese Issuers. https://www.sec.gov/files/US-Investors-Exposure-to-Domestic-Chinese-Issuers_2020.07.06.pdf

35 RWR Advisory Group, LLC. (2020, August). Publicly Traded Chinese Military Companies (and Affiliates) as Designated by the U.S. Department of Defense. https://www.rwradvisory.com/wp-content/uploads/2020/11/RWR_Pentagon-List_Affiliates.pdf

36 氪的朋友们. (2021, January 18). 2020年国内半导体行业投资金额超1400亿元，为史上最多一年_详细解读_最新资讯_热点事件_36氪. 36kr.Com. https://www.36kr.com/p/1059953231336069

37 Chinese third-party aggregator of private capital markets data

38 State ownership assessed from Chinese corporate registry filings.

39 Semiconductor Manufacturing International Corporation. (2020). Semiconductor Manufacturing International Corporation: Annual Report 2019. http://www.smics.com/uploads/e_00981ar-20200418.pdf

40 U.S. Department of the Treasury (2020, June 3).

41 中国半导体行业会不会迎来整合潮? | 新年展望. (2021, January 29). Finance.Sina.Com.Cn. https://finance.sina.com.cn/roll/2021-01-29/doc-ikftssap1761247.shtml?cref=cj

42 However, these capital injections may also undermine state objectives by inducing fraud and corruption by opportunistic executives, as with Wuhan Hongxin Semiconductor Manufacturing. In this sense, the significant direction of government capital toward companies may produce a mix of relationships between businesses and the party-state apparatus, with different implications for U.S. national security. For more information, see Kevin Xu profiled the case of Wuhan Hongxin Semiconductor Manufacturing, describing it as China's "semiconductor Theranos." See Xu, K. (2021, March 4). China's "Semiconductor Theranos": HSMC. Interconnected. https://interconnected.blog/chinas-semiconductor-theranos-hsmc/

43 Perry, E. J. (2019). Educated acquiescence: how academia sustains authoritarianism in China. Theory and Society, 49(1), 1–22. https://doi.org/10.1007/s11186-019-09373-1

44 Perry (2019), pp. 2.

45 As James Mulvenon notes, civilian universities relate to the party-state apparatus in ways that do not reflect the same relationship as in the United States with the Department of Education. For example, the Chinese Ministry of Education appoints university leaders and approves budgets. For a greater exploration of these ideas, see Mulvenon, J. (2020). China's Quest for Foreign Technology. pp. 301-302 (W. C. Hannas and D. K. Tatlow, Eds.). Routledge.

46 Chinese Defence Universities Tracker—Home. Chinese Defence Universities Tracker. https://unitracker.aspi.org.au/

47 The 79 universities were selected from ASPI's Defence University tracker as civilian universities with purported ties to China's military. For more information on C4ADS's selection and identification process, see Goldberg, C. (2021). Open Gates:

Technology Transfer from Chinese Universities to the Defense Industry Through Joint Ventures. https://static1.squarespace.com/static/566ef8b4d8af107232d5358a/t/60d9d5837ca3d8345a0d42c5/1624888707802/Open+Gates_Final.pdf.

48 Li, Wenli and Liu Qiang. "Chinese Higher Education Finance: Changes over Time and Perspectives to the Future." Procedia - Social and Behavioral Sciences, vol. 77, 22 Apr. 2013, https://doi.org/10.1016/j.sbspro.2013.03.095.

49 Zou, Yonghua and Wanxia Zhao. "Anatomy of Tsinghua University Science Park in China: institutional evolution and assessment." The Journal of Technology Transfer, vol. 39, issue 5, May 2012, https://doi.org/10.1007/s10961-013-9314-y.

50 "以科技成果作价投资实施转化的，应当从作价投资取得的股份或者出资比例中提取不低于50%的比例用于奖励" http://www.gov.cn/zhengce/content/2016-03/02/content_5048192.htm

51 Ministry of Education of the People's Republic of China (2020). 教育部 国家知识产权局 科技部 关于提升高等学校专利质量 促进转化运用的若干意见. http://www.moe.gov.cn/srcsite/A16/s7062/202002/t20200221_422861.html

52 CSET maintains an expansive database of known Talent Recruitment Programs. For more information, see Weinstein, E. Chinese Talent Program Tracker. Center for Security and Emerging Technology. https://chinatalenttracker.cset.tech/

53 China's Quest for Foreign Technology. p. 39 (W. C. Hannas and D. K. Tatlow, Eds.)

54 Redden, E. (2021, March 2). Reconsidering the 'China Initiative': Criminal initiative targeting scholars who allegedly hid Chinese. Inside Higher Ed. https://www.insidehighered.com/news/2021/03/02/criminal-initiative-targeting-scholars-who-allegedly-hid-chinese-funding-and

55 "A politically exposed person (PEP) is defined by the Financial Action Task Force (FATF) as an individual who is or has been entrusted with a prominent public function. Due to their position and influence, it is recognised [sic] that many PEPs are in positions that potentially can be abused for the purpose of committing money laundering (ML) offences and related predicate offences, including corruption and bribery, as well as conducting activity related to terrorist financing (TF)." For more information, see Financial Action Task Force (2013, June). Politically Exposed Persons (Recommendations 12 and 22). https://www.fatf-gafi.org/media/fatf/documents/recommendations/Guidance-PEP-Rec12-22.pdf

56 Frequently Asked Questions. (n.d.). U.S. Department of Justice. https://www.wsj.com/articles/trial-of-scientist-accused-of-hiding-china-work-goes-to-jury-11623696796

57 Huang, D. and Chen, M. (2020). Business Lobbying within the Party-State: Embedding Lobbying and Political Co-optation in China. The China Journal, 83, 105–128. https://doi.org/10.1086/705933

58 Huang, D. and Chen, M. (2020)

59 Milhaupt, C. J. and Zheng, W. (2015). Beyond Ownership: State Capitalism and the Chinese Firm. The Georgetown Law Journal, 103(665), 665–722. https://scholarship.law.ufl.edu/cgi/viewcontent.cgi?article=1693&context=facultypub

60 See Article 19, COMPANIES LAW OF THE PEOPLE'S REPUBLIC OF CHINA ORDER OF THE PRESIDENT OF THE PEOPLE'S REPUBLIC OF CHINA No. 42. (2005, October). International Labor Organization. https://www.ilo.org/dyn/natlex/docs/ELECTRONIC/92643/108008/F-186401967/CHN92643%20Eng.pdf

61 Thomas, N. (2020, December 16). Party Committees in the Private Sector: Rising Presence, Moderate Prevalence. MacroPolo. https://macropolo.org/party-committees-private-sector-china/?rp=e

62 Thomas, N. (2020, December 16)

63 Ibid

64 Blanchette, J. (2019, April 23). Against Atrophy: Party Organisations in Private Firms. Made in China Journal. https://madeinchinajournal.com/2019/04/18/against-atrophy-party-organisations-in-private-firms/

65 For background on industrial associations and their relationship to the Chinese party-state, see Milhaupt, C. J. and Zheng, W. (2015), p. 686

66 Cogan, B. M. (2011, September 6). In Re Vitamin C Antitrust Litigation, 810 F. Supp. 2d 522 (E.D.N.Y 2011). CourtListener. https://www.courtlistener.com/opinion/2147703/in-re-vitamin-c-antitrust-litigation/?q=cites%3A184756

67 Opinion on Strengthening the United Front Work of the Private Economy in the New Era. (2020, September 15). Gov.Cn. http://www.gov.cn/zhengce/2020-09/15/content_5543685.htm

68 Milhaupt, C. J., and Zheng, W. (2015), p. 685

69 All-China Federation of Industry and Commerce. Acfic.Org.Cn. http://www.acfic.org.cn/zzjg_327/

70 Luong, N. and Arnold, Z. (2021, May). China's Artificial Intelligence Industry Alliance: Understanding China's AI Strategy Through Industry Alliances. CSET Data Brief. https://cset.georgetown.edu/wp-content/uploads/CSET-Chinas-Artificial-Intelligence-Industry-Alliance-1.pdf

71 In 2021, Chinese regulators have been particularly involved against technology companies. For example, in July 2021, the Cyberspace Administration of China launched a data security investigation against Didi Global, a ride-sharing service in China that is publicly traded on U.S. stock exchanges. Chinese regulators required that Didi's mobile app be removed from app stores and blocked the company from adding new users, which drastically affected the business. The company is now considering going private. For more information, see https://www.wsj.com/articles/didi-global-considers-going-private-to-placate-china-and-compensate-investors-11627551071

72 Chinese Antitrust Exceptionalism p 83

73 Chinese Antitrust Exceptionalism p 81

74 Chinese Antitrust Exceptionalism p 82

75 Norris, W. J. (2016). Chinese Economic Statecraft: Commercial Actors, Grand Strategy, and State Control (1st ed.). Cornell University Press and Rithmire, M. (2019, June, Revised 2021, January). Going Out or Opting Out? Capital, Political Vulnerability, and the State in China's Outward Investment Harvard Business School Working Paper, 20-009.

76 Norris, W. J. (2016).

77 Rithmire, M. (2019, June, Revised 2021, January)

78 Rithmire, M. (2019, June, Revised 2021, January)

79 Rithmire, M. (2019, June, Revised 2021, January)

80 Norris, W. J. (2016) describes "reporting relationship" as a key variable to assess in understanding how well the Chinese party-state may be able to co-opt a company to pursue its policy objectives. While related in some respects, we emphasize here a financial relationship because it may indicate formal mechanisms of reporting and control between the CCP and a company, and because equity stakes are visible in most corporate disclosure documents available to investors. I include extralegal mechanisms for reporting between companies and the CCP under the "political exposure" variable.

81 Definition: foreign instrumentality from 18 USC § 1839(1) | LII / Legal Information Institute. (2016). Economic espionage: https://www.law.cornell.edu/uscode/text/18/1831

82 Previous research on the Chinese commercial system indicates that most equity investments by state-owned companies are not controlling stakes. For more information, see Bai, C.-E., Hsieh, C.-T., Song, Z. M., & Wang, X. (2020). Special Deals from Special Investors: The Rise of State-Connected Private Owners in China. National Bureau of Economic Research, Working Paper 28170. https://doi.org/10.3386/w28170

83 Norris, W. J. (2016)

84 Jim, C. (2020, September 22). China's property developers seek to dodge new rules with shift of debt off balance sheets. Reuters. https://www.reuters.com/article/uk-china-property-debt-analysis/chinas-property-developers-seek-to-dodge-new-rules-with-shift-of-debt-off-balance-sheets-idUSKCN26C38F

85 McClymont, K. (2020, March 26). Second developer flew 82 tonnes of medical supplies to China. The Sunday Morning Herald. https://www.smh.com.au/national/second-developer-flies-82-tonnes-of-medical-supplies-to-china-20200326-p54e8n.html

86 ADS-B refers to Automatic Dependent Surveillance-Broadcast, which are signals that planes use to support navigation that can be used to track an aircraft's position. For example, reporters used ADS-B data to track movements by Jack Ma's private plane amid a protracted retreat from the public eye and speculation about his safety in early 2020. See McMorrow, R., and Yu, S. (2021, March 21). Jack Ma's private jet records show billionaire is down but not out. Financial Times. https://www.ft.com/content/784fb680-3e58-4c7a-a375-2f78fad52c64. Hedge funds have also begun to use ADS-B data to predict investment deals. See Bachman, J. (2019, July 2). Hedge funds are tracking private jets to find the next megadeal. Bloomberg Businessweek. https://www.bloomberg.com/news/articles/2019-07-02/hedge-funds-are-tracking-private-jets-to-find-the-next-megadeal

87 Several academics have previously called for attention to goal compatibility between Chinese businesses and the state. For examples, see Norris, W. J. (2016) and Rithmire, M. (2019, June, Revised 2021, January)

88 In a paper on Chinese outbound investment, Meg Rithmire (2020) argues that Chinese companies pursue globalization with a range of motivations that in turn produce different relationships between the company and the party-state. Rithmire generalizes three categories of outbound Chinese capital: "tactical capital," which seeks political prestige or power for managers and/or the Chinese state; "competitive capital," which pursue revenue and/or profit abroad; and "crony capital," which seek capital accumulation and refuge from the state. Insofar as a company's commercial objectives are directly in line with the party-state's national security priorities, policymakers may turn focus from establishing the entity as a "foreign instrumentality" to the extent to which the party-state may have enabled the company to expand abroad through preferential policies or to the political relationships between the company's business executives and party-state elites as a means to determine whether or not the company could pose a national security risk, i.e., where "special deals" at home between the business's leaders may be facilitating completely legal commercial activities abroad that advance the party-state's interests at the expense of the United States. In cases of "crony capital," policymakers should look for evidence of corruption or threat finance abroad, for which more traditional legal instruments designed to disrupt financial crime may be sufficient to mitigate risks. For more information, see Rithmire, M. (2019, June, Revised

2021, January)

89 Definition: foreign instrumentality from 18 USC § 1839(1) | LII / Legal Information Institute. (2016).

90 While many Chinese data sources are publicly available and free to access, there are technical challenges to using them reliably and at scale. For example, queries in the Chinese corporate registry require the Chinese name of the company, which may be difficult to determine from the English name alone. Many beneficial ownership records in the United States, like U.S. Securities and Exchange Commission disclosure forms, do not include company or person names in Chinese, which creates ambiguity that can impede comprehensive due diligence investigations that leverage the full breadth of Chinese public records. Additionally, the website for China's corporate registry is often unreliable to access and requires Mandarin proficiency. While third party aggregators also provide the information in a more user-friendly fashion, their scope, completeness, and veracity can vary in ways that are difficult to assess.

91 Future work will seek to scale our beta model, test it in different data environments, and apply it to a broader set of national security questions related to Chinese economic statecraft.

92 Chinese Defence Universities Tracker—Home. (n.d.). Chinese Defence Universities Tracker. https://unitracker.aspi.org.au/

93 Goldberg, C. (2021).

94 Bai et al. (2020)

95 Rithmire, M., and Chen, H. (2021).

96 Rithmire, M., and Chen, H. (2021)

97 Junkets are a form of casino-based tourism organize travel, accommodation, and gambling for high net-worth individuals in special arrangements with casinos. In a December 2020 assessment of financial crime risks related to the gaming industry, the Australian Transaction Reports and Analysis Center (AUSTRAC), the Australian government's financial intelligence agency, defined junkets as "an arrangement between a casino and a junket tour operator to facilitate a period of gambling by one, or a group, of high wealth player(s) at the casino. In return for bringing the player(s) to the casino, the casino pays the [junket tour operator] a commission based on the collective gambling activity of player(s) on the junket." For more information, see Junket Tour Operations in Australia: Money laundering and terrorism financing risk assessment. (2020). Australian Transaction Reports and Analysis Centre. https://www.austrac.gov.au/sites/default/files/2020-12/JTO_2020_FINAL.pdf

98 "Fuzzy matching" refers to a statistical technique to identify correspondence between text strings that may not be exactly identical.

99 公司简介: Quantumctek Co.,Ltd. (n.d.). Sina Finance. http://vip.stock.finance.sina.com.cn/corp/go.php/vCI_CorpInfo/stockid/688027.phtml

100 Chinese corporate registry filings

101 HTTPS://QUANTUM.USTC.EDU.CN/WEB/NODE/141

102 Chinese corporate registry filings

103 Wang Bing Personal Resume (n.d.). http://dsxt.ustc.edu.cn/zj_js.asp?zzid=6521

104 Giles. M. (2018, December 19). The man turning China into a quantum superpower. MIT Technology Review. https://www.technologyreview.com/2018/12/19/1571/the-man-turning-china-into-a-quantum-superpower/

105 In December 2018, the Government Accountability Office conducted a study to identify long-range emerging threats to the United States as determined by the Departments of Defense, State, and Homeland Security and the Office of the Director of National Intelligence. The report indicates that "Quantum communications could enable adversaries to develop secure communications that U.S. personnel would not be able to intercept or decrypt. Quantum computing may allow adversaries to decrypt information, which could enable them to target U.S. personnel and military operations." For more information, see see National Security: Long-Range Emerging Threats Facing the United States As Identified by Federal Agencies (2018, December). U.S. Government Accountability Office. https://www.gao.gov/assets/700/695981.pdf

106 中华人民共和国国民经济和社会发展 第十四个五年规划和2035年远景目标纲要. (2021, March). https://www.ndrc.gov.cn/xxgk/zcfb/ghwb/202103/P020210323538797779059.pdf

107 Private equity and venture capital data compiled by Pitchbook

108 Private equity and venture capital data compiled by Pitchbook

109 Private equity and venture capital data compiled by Pitchbook

110 Tan, C.K. (2020, July 17). Shanghai's STAR market brings in new dawn for Chinese tech. Nikkei Asia. https://asia.nikkei.com/Business/Business-Spotlight/Shanghai-s-STAR-market-brings-in-new-dawn-for-Chinese-tech

111 Tan, C.K. (2020, July 17). Shanghai's STAR market brings in new dawn for Chinese tech. Nikkei Asia. https://asia.nikkei.com/Business/Business-Spotlight/Shanghai-s-STAR-market-brings-in-new-dawn-for-Chinese-tech

112 Chinese corporate registry filings

113 Chinese corporate registry filings

114 Chinese corporate registry filings; U.S. Department of the Treasury (2020, June 3).

115 Chinese corporate registry filings

116 Chinese corporate registry filings

117 Chinese corporate registry filings

118 FCC Designates Huawei and ZTE as National Security Threats. (2020, June 30). Federal Communications Commission. https://www.fcc.gov/document/fcc-designates-huawei-and-zte-national-security-threats

119 Chinese corporate registry filings

120 https://www.theage.com.au/business/companies/key-crown-junket-partner-blocked-from-australia-20190731-p52cmt.html

121 Chinese corporate registry filings

122 Masige, M. (2018, November 22). The ultimate VIP experience: Alvin Chau. The CEO Magazine. https://www.theceomagazine.com/executive-interviews/entertainment-leisure/alvin-chau/

123 Suncity launches VIP club at Macau satellite casino. (2015, July 19). GGRAsia.com. http://www.ggrasia.com/suncity-launches-vip-club-at-macau-satellite-casino/

124 The Macau junket Suncity Group remains separate from the Hong Kong-listed Suncity Group Holdings, although both are often referred to in the media as "Suncity". http://www.dicj.gov.mo/web/en/information/DadosEstat/2019/content.html#

125 Ibid

126 Master, M. (2019, July 9). Chinese state media target Macau's Suncity in online gambling report. Reuters. https://www.reuters.com/article/us-china-casinos/chinese-state-media-target-macaus-suncity-in-online-gambling-report-idUSKCN1U40M7

127 Chinese corporate registry filings

128 CITIC Howah website, accessed June 15, 2021. Link: http://howah.ecitic.com/web/h/ywjs.html?id=1

129 Chinese corporate registry filings

130 According to a Macau government gazette filing for corporate registration, Vast Investments (Macau) Co., Ltd 瀚华投资(澳门)有限公司 is registered to Room N to P, 12/F, China Civil Plaza, No. 263 Alameda Dr. Carlos d'Assumpção, Macau 澳門宋玉生廣場263號中土大廈12樓N-P室. This address is also listed in online business directories as the office address of SunCity Group 太阳城集团 in Macau.

131 Master, M. (2013, April 29). Gamblers not so anonymous: Beijing keeps closer eye on Macau. Reuters. https://www.reuters.com/article/casinos-macau-china/gamblers-not-so-anonymous-beijing-keeps-closer-eye-on-macau-idUSL3N0DA82U20130429

132 Chinese corporate registry filings

133 Conneller, P. (2019, August 5). "Suncity CEO Alvin Chau Reportedly Banned from Australia Over Alleged Triad Links," Casino.org. https://www.casino.org/news/suncity-ceo-alvin-chau-reportedly-banned-from-australia/

134 Conneller, P. (2019, August 5).

135 https://kknews.cc/entertainment/kmzkrop.html ; https://www.laonanren.com/news/2016-08/125768p5.htm

136 Boyle, D. (2019). CAMBODIA'S CASINO GAMBLE: All in on Sihanoukville. Al Jazeera. https://interactive.aljazeera.com/aje/2019/cambodia-casino-gamble/index.html

137 OFAC also designated the World Hongmen History and Culture Association. For more information, see Treasury sanctions corrupt actors in Africa and Asia. (2020, December 9). U.S. Department of the Treasury. https://home.treasury.gov/news/press-releases/sm1206#:~:text=Broken%20Tooth%20is%20designated%20for,personal%20gain%2C%20corruption%20related%20to

138 According to Chinese-language media, Chau also has links to organized crime in the non-gaming entertainment sector. SunCity company Sun Entertainment has produced several movies directed by Paco Wong Pak Ko (黃柏高) ("Wong"), who was also reportedly an associate of WAN Kuok Koi. Hong Kong media has also reported links between Chau and Charles Heung Wah-Keung, son of the founder of the Sun Yee On Triad. For more information, see 酸檸蒙 (2018, February 20). 黑勢力並肩向華強，44歲身家百億賭場十幾個，只因後台太強大! KKNews. https://kknews.cc/zh-hk/entertainment/kmzkrop.html

139 McKenzie, N. (2020, February 21). Crown casino hosted organised crime target as he built a gambling empire. The Age. https://www.theage.com.au/business/companies/crown-casino-hosted-organised-crime-target-as-he-built-a-gambling-empire-20200220-p542sa.html

140 McKenzie, N. (2020, February 21).

141 McKenzie, N. (2020, February 21).

142 McKenzie, N. (2020, February 21).

143 McKenzie, N. (2020, February 21).

144 Stradbrooke, S. (2018, September 5). Suncity partners with Cambodian integrated resort project. Calvin Ayre. https://calvinayre.com/2018/09/05/casino/suncity-partners-cambodia-integrated-resort/

145 Chinese corporate registry filings indicate that Dong Lecheng later left his position at the company. https://www.ggrasia.com/suncity-listco-unit-inks-agreement-for-cambodia-project/

146 "Hurun China Rich List 2019," https://www.hurun.net/EN/Article/Details?num=CE08472BB47D

147 Yunnan Jingcheng Group signs up 12.2-billion-yuan agreements on infrastructure projects with Yingjiang and Ruili. (2015, August 12). Ruili Government Website. http://en.ruili.gov.cn/News/content-196-158-1.html

148 云南第四富豪、瑞丽航空董事长涉嫌行贿被查, (2014, November 7). NBD. http://www.nbd.com.cn/articles/2014-11-07/874503.html

149 https://www.ggrasia.com/chow-tai-fook-takes-lead-on-vietnam-casino-scheme/; https://vietnamnews.vn/economy/275708/vinaland-sells-stake-in-casino.html

150 Ka-sing, L. (2020, June 21). New book pays homage to Cheng Yu-tung, Hong Kong tycoon who enjoyed helping friends, goldsmith apprentice who once upstaged Donald Trump. South China Morning Post. https://www.scmp.com/business/article/3089910/new-book-pays-homage-cheng-yu-tung-hong-kong-tycoon-who-enjoyed-helping.

151 Gates, G. (2012, October 25). The Wen Family Empire. New York Times. https://archive.nytimes.com/www.nytimes.com/interactive/2012/10/25/business/the-wen-family-empire.html?ref=china

152 SunCity Group is also invested in casinos and online gambling enterprises around the world. Suncity Group Holdings boosted its stake in Russia's largest casino operator, Summit Ascent in 2019, from a "small stake" to 28%. Summit Ascent operates Tigre de Cristal casino in Vladivostok. In June 2020, it was reported that Summit Ascent plans to increase its share capital and use a portion of the proceeds to purchase Suntrust Home Developers Inc., which is developing the Manila Westside City Resorts and is controlled by Chau. See Stradbrooke, S. (2020, June 2). Suncity takes majority control of Russia's Tigre de Cristal casino. Calvin Ayre. https://calvinayre.com/2020/06/02/casino/suncity-majority-control-russia-casino-tigre-de-cristal/

153 A Japanese Suncity subsidiary previously submitted documentation to take part in the request for proposal process for a casino in Wakayama, Japan but reportedly pulled out of the process in 2021. See Suncity interested in right-fit partners for Japan IR bid. (2020, May 6). GGRAsia. http://www.ggrasia.com/suncity-interested-in-right-fit-partners-for-japan-ir-bid/ and Ivica. (2021, May 15). Suncity is out but Wakayama stays put in the Japan casino license race. https://www.slotscasino.co.uk/news/suncity-is-out-but-wakayama-stays-put-in-the-japan-casino-license-race/

154 Suncity formerly ran the online gaming website 138.com from the Isle of Man, which appears to have targeted Asian gamers, including those in Mainland China. Gambling is banned in Mainland China (except through the state-run lottery), although individuals in the Mainland have historically accessed online gaming websites through VPNs. In July 2019, Chinese state media accused Suncity of running the largest online gaming operator targeting customers in the Mainland. 138.com shut down shortly after the article was published. See Stradbrooke, S. (2020, May 28). Online gambling mystery as 138.com shuts; M88 exits Cambodia, Malaysia. Calvin Ayre. https://calvinayre.com/2020/05/28/business/online-

gambling-mystery-138-com-shuts-down/

155 Reuters Staff. (2020, July 13). Macau junket Suncity gives rare details VIP finances in rebuttal of online criticism. Reuters. https://www.reuters.com/article/us-macau-casinos-suncity/macau-junket-suncity-gives-rare-details-vip-finances-in-rebuttal-of-online-criticism-idUSKCN24E0GX

156 Rithmire, M., and Chen, H. (2021).

157 Macau | Suncity Group signs agreement for casino management in Cambodia. (2018, October 4). Macau Business.com. https://www.macaubusiness.com/macau-suncity-group-signs-agreement-for-casino-management-in-cambodia/

158 Spegele, B. (2020, June 23). Political Donors Linked to China Won Access to Trump, GOP. The Wall Street Journal. https://www.wsj.com/articles/political-donors-linked-to-china-won-access-to-trump-gop-11592925569

159 Spegele, B. (2020, June 23).

160 华讯方舟：2019年年度报告. (2020, June 15). VIP.stock.finance.sina.com.cn. https://vip.stock.finance.sina.com.cn/corp/view/vCB_AllBulletinDetail.php?stockid=000687&id=6367161

161 华讯方舟：2019年年度报告. (2020, June 15); 华讯方舟 (000687.SZ)：业绩低迷负债高企，控股股东转让股权欲离场. (2019, July 25). Sohu.com. https://www.sohu.com/a/329245158_313170;《华讯绝非池中物 方舟破浪会有时》(好文，转). (2016, June 30). Gelonghui.com, https://www.gelonghui.com/p/65362; 吴立骏. (2020, November 9). 原标题：*ST华讯 实控人董事长又双叒领处分，年内跌幅“熊霸”两市受损股民可报名索. Finance.Sina.com.cn. 赔https://finance.sina.com.cn/roll/2020-11-12/doc-iiznctke1017068.shtml

162 Perper, R. (2020, June 24). Chinese nationals with ties to the Chinese government donated hundreds of thousands to support Trump's reelection, according to report. Business Insider. https://www.businessinsider.com/chinese-nationals-tied-to-chinese-government-donate-trump-reelection-wsj-2020-6

163 Chinese corporate registry filings

164 Chinese corporate registry filings

165 See footnotes 158-162, infra.

166 中国工商联十二大闭幕 华讯方舟集团董事长吴光胜当选执行委员会常委. (2017, November 30). Fdx-fund.com. https://www.fdx-fund.com/cn/news-detail-1168.html

167 全国工商联青年企业家委员会. (n.d.). All-China Federation of Industry and Commerce. http://www.acfic.org.cn/zzjg_327/zmwyh/2019_qnqyjwyh/

168 个人简介 : 吴光胜. (n.d.). Finance.Sina.com.cn. https://money.finance.sina.com.cn/corp/view/vCI_CorpManagerInfo.php?stockid=000687&code=30312588&Name=%CE%E2%B9%E2%CA%A4

169 许可馨(Ed.). (2018, March 24).【嘉宾介绍】吴光胜 | 华讯方舟科技有限公司董事长. Sznews.com. http://www.sznews.com/zhuanti/content/2018-03/21/content_18711496.htm

170 第五届全国非公有制经济人士优秀中国特色社会主义事业建设者名单. (2019, August 30). Cpc.com.cn. cpc.people.com.cn/n1/2019/0830/c64387-31328095.html

171 See footnotes 164-169, infra.

172 FCC Designates Huawei and ZTE as National Security Threats. (2020, June 30).

173 See footnotes 166-170, infra.

174 研究院简介. (n.d.). Shenzhen Institute of Terahertz Technology and Innovation. http://www.szthz.org/index.php/About-index-id-2.html

175 合作伙伴. (n.d.). Shenzhen Institute of Terahertz Technology and Innovation. http://www.szthz.org/index.php/Cooperate-index-id-7.html

176 学术交流. (n.d.). Shenzhen Institute of Terahertz Technology and Innovation. http://www.szthz.org/index.php/Cooperate-index-id-6.html

177 中国人民解放军防化研究院教授一行莅临华讯方舟集团参观交流. (2019, January 31). Shenzhen Institute of Terahertz Technology and Innovation. http://www.szthz.org/index.php/News-index-id-55.html

178 中电集团27所中电科信息产业有限公司倪晓岩副总经理一行莅临华讯方舟交流座谈. (2018, December 17). Shenzhen Institute of Terahertz Technology and Innovation. http://www.szthz.org/index.php/News-index-id-53.html

179 See footnote 172-174, infra.

180 Spegele, B. (2020, June 23).

181 未来产业促进会. (2017, July 12). 美国总统特朗普会见华讯方舟董事长吴光胜，推进中美科技合作，造福全人类. Freewechat.com. https://freewechat.com/a/MzA4NjExODA0MA==/2652372210/1 and 特朗普会见深圳工总主席团主席、华讯方舟董事长吴光胜 共同推进中美科技合作. (2017, July 10).

182 Spegele, B. (2020, June 23).

183 For information on U.S. law regarding participation by foreign nationals in U.S. elections, see Foreign Nationals. (2017, June 23). U.S. Federal Election Commission. https://www.fec.gov/updates/foreign-nationals/

184 Satterfield, J. (2021, June 13). Trial reveals federal agents falsely accused a UT professor born in China of spying. Knoxville News Sentinel. https://www.knoxnews.com/story/news/crime/2021/06/14/federal-agents-falsely-accused-university-of-tennessee-professor-spying-china/7649378002/

185 Viswanatha, A. (2021, June 14). Trial of scientist accused of hiding China work goes to jury. The Wall Street Journal. https://www.wsj.com/articles/trial-of-scientist-accused-of-hiding-china-work-goes-to-jury-11623696796

186 House Permanent Select Committee on Intelligence. (2020). The China Deep Dive: A Report on the Intelligence Community' s Capabilities and Competencies with Respect to the People' s Republic of China. https://intelligence.house.gov/uploadedfiles/hpsci_china_deep_dive_redacted_summary_9.29.20.pdf

187 Ibid

188 In her book The Scientist and the Spy, Mara Hvistendahl details the series of events in which American and Chinese employees of a Chinese agriculture company engaged in economic espionage in Iowa, and in doing so illustrates how the incentive structure of China' s domestic political economy—through which partnerships between powerful local governments and their selected private enterprises, brokered through special deals, compete in a fierce domestic market without formal protections for property rights—create national security issues in the United States. Her recounting shows that core national security threats like illicit technology transfer can and do emerge not necessarily from a CCP-orchestrated espionage operation but instead as a result of incentive structures in China' s domestic economy, where collusion is endemic.

C4ADS

innovation for peace

C4ADS is a digital-age think tank dedicated to providing data-driven analysis and evidence-based reporting on global conflict and transnational security issues.

1201 I Street NW
Washington D.C., 20005

+1 (202) 289 3332
info@c4ads.org