C4ADS
innovation for peace

Testimony before the U.S.- China Economic and Security Review Commission
Hearing on "U.S. Investment in China's Capital Markets and Military-Industrial Complex"

The Party-State in China's Military-Industrial Complex: Implications for U.S. National Security

Jason Arterburn
Program Director, the Center for Advanced Defense Studies

Friday, March 19, 2021

Introduction

China's domestic political economy exposes the United States to national security risks that our regulatory systems are not well equipped to address. China's commercial system blurs public and private distinctions, which have become even less meaningful under General Secretary Xi Jinping as the party-state has become resurgent in the commercial sector. While the U.S. policymaking community has largely acknowledged the risks of U.S. exposure to China's military-industrial base, our regulatory community still faces challenges in how to identify and mitigate risks. This is largely because "the analytical frameworks that many of us are using to understand China's economy are stuck in past paradigms" that do not reflect the "entirely new political-economic order" that China's system has produced as both an emergent and intentional phenomenon.[1] Experts like James Mulvenon, Anna Puglisi, William Hannas, Didi Kirsten Tatlow, and others have previously produced extensive analyses of China's technology acquisition ambitions and military-civil fusion system, which have provided the policymaking community with a comprehensive overview of China's technology acquisition system and its changes over the last decade. In this testimony, I seek to complement their work by contextualizing China's military-industrial base against the backdrop of recent changes in China's political economy, with the goal of developing a framework that policymakers and the business community can use to mitigate national security risk as General Secretary Xi Jinping continues to pursue illiberal governance reforms.

First, I will describe the mechanisms through which the Chinese party-state participates in and regulates the commercial sector as a way to both induce and coerce companies, universities, and others toward its industrial policy goals, with an emphasis on those organizations that are involved in China's military-industrial complex. I will review recent academic literature which shows that the top 100 conglomerates—including major state-owned enterprises—comprise on average 15,000 companies, and consider how that network scale and complexity may reduce the effectiveness of U.S. regulatory mechanisms like export controls, financial sanctions, or investment review.

Second, given the blurred distinctions between public and private, I will propose a framework that U.S. investors, universities, and others can use to assess the risk that a company may be co-opted to advance China's policy goals at the expense of U.S. national security interests. Because equity ownership analysis may be insufficient on its own to establish "instrumentality"[2] in China's massive, complex, and politically enmeshed corporate networks, my framework proposes the inclusion of other elements relevant to state-business relations in China's political economy. These other elements are, namely, the political exposure of commercial shareholders and officers, industry sensitivity within China, market structure, and compatibility of the business's commercial goals with the party-state's policy objectives.[3]

---

[1] 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

[2] Definition: foreign instrumentality from 18 USC § 1839(1) | LII / Legal Information Institute. (2016). Cornell Law. https://www.law.cornell.edu/definitions/uscode.php?width=840&height=800&iframe=true&def_id=18-USC-1341432272-1439925515&term_occur=1&term_src=title:18:part:I:chapter:90:section:1831

[3] My proposed framework integrates theoretical contributions about state-business relations in China, most notably from 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* (No. 20-009). Harvard Business School Working Paper. https://www.hbs.edu/faculty/Pages/item.aspx?num=56422

Third, I argue that publicly available information (PAI) should play a greater role in policy responses to national security risks from China's commercial sector, and I consider the challenges that government agencies may face in adopting it. This argument expands upon recent recommendations from the House Permanent Select Committee for Intelligence, which call for more effective use of open source information to address threats from China. Specifically, I argue that PAI and derivative products can replicate the integration of multiple traditional intelligence disciplines to provide actionable analysis on the China target that can be more easily disseminated within government and beyond—and at a significantly lower cost. By leveraging the full range of publicly available information relevant to national security threats from China, U.S. and allied governments can not only direct specialized collection resources toward more difficult intelligence requirements, but also engage more easily with the full range of government and industry stakeholders who will be necessary to confront a whole-of-society challenge from China's party-state.

1. **China's military-industrial complex, like the rest of China's economy, blurs the line between public and private in ways that pose systemic risks to U.S. national security interests.**

The blurred lines between public and private ownership in China's military-industrial complex reflect China's broader political economy, in which the commercial sector and government have entered "special deals" to pursue mutually beneficial value propositions.[4] Over three decades, companies have been dependent on government cooperation or endorsement to guarantee market protections they may not otherwise receive from formal institutions, and local governments have competed to attract private enterprise that would spur economic development toward policy targets.[5] While collusion between governments and private enterprise is common in countries without formal market institutions, Bai, Hsieh, and Song (2019) assess that this "special deals" system of partnerships around "high [state] capacity and private benefits" has been responsible for China's growth over the last three decades because of the broad availability of special deals in China and unusually high administrative capacity of the Chinese state.[6] As a result, when Chinese companies pursue globalization today, they do so with complex relationships to the Chinese party-state that defy simple categorizations as "state-owned" or "private."

As Chinese companies increasingly pursue commercial activities that impinge on U.S. interests, China's "special deals" system has created two serious national security consequences. First, China's commercial system has become exceedingly complex. In fact, the average size of the largest 100 conglomerates in China increased from 500 companies to more than 15,000 companies between 1995 and 2015, and among the top 1,000 conglomerates, the share of subsidiaries that are joint ventures with other firms has increased from 30% to 80%.[7] As a result, corporate network complexity makes it less straightforward to establish a company's intent through equity ownership analysis alone, as a company of interest may receive investments a mix of state- and non-state companies through multiple layers of holding companies.

[4] 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
[5] For a broader discussion of these trends, see ibid.
[6] Ibid
[7] Ibid, pp. 22-23

Additionally, because networks may be broadly diversified in their commercial activities, particularly in the case of major conglomerates, one company's industry involvement may not be generalizable across the whole network. 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.[8]

Second, private investors in China rely in part on state proximity for capital growth and productivity, which may expose them to political interests that are difficult to assess or measure. Using bulk Chinese corporate registration data, 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.[9] These findings suggest that while the party-state may not directly control private investors, those investors are exposed to the party-state apparatus to varying degrees and may face economic incentives to align with the party-state's policy priorities. U.S. policymakers should seek to understand how closely a private company may be to the state, and if that proximity to the state has any significance to U.S. national security interests.

To this end, the next subsections consider the mechanisms through which the Chinese party-state engages with the commercial and research sectors in China as a way to both induce and coerce actors toward its policy objectives. These relationships are necessary considerations for those who wish to consider how investments may be directly or indirectly exposed to China's military-industrial ecosystem. Furthermore, they provide evidence that policy intended to mitigate national security risks from China may need to change in order to reflect the nature of state-business relations in China's political economy.

Direct Participation: State-owned Defense Contractors

State-owned enterprises (SOEs) advance policy objectives for the Chinese party-state by directing capital toward key sectors and spearheading policy initiatives both at home and abroad.[10] While commercial SOEs may lag behind privately-held companies in efficiency and productivity, they have been instrumental to China's ability to pursue key national priorities such as energy security and military research and development. By one estimate, China's SOEs collectively produce 4.5% of global GDP, which is greater than the GDP of the United Kingdom.[11] Ten defense SOEs directly under SASAC participate in trade fairs, collaborate in research with universities and key state labs, fund research, and make investments both domestically and abroad.[12]

---

[8] 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

[9] 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

[10] 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/

[11] 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

[12] The ten central state-owned defense corporations are China Aviation Industry Corporation (AVIC), Aero Engine Corporation of China (AECC), China Electronics Technology Group Corporation (CETGC), China Electronics Corporation (CEC), China South Industries Group Corporation, China North Industries Group Corporation, China State Shipbuilding Corporation (CSSC), China

The Chinese state directly owns and manages SOEs at the central and local level. For central SOEs, the Chinese Communist Party (CCP) directly controls executive leadership appointments and promotion and in some cases, will appoint foreign nationals to SOE boards.[13] [14] Wendy Leutert (2020) notes that General Secretary Xi Jinping has further institutionalized CCP control over central SOEs by increasing dual appointments for SOE leadership to CCP secretary and SOE managerial positions to "constrain managerial independence by bringing SOE leadership into the political realm of the CCP"[15]; and 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 than the CCP.[16]

China's central SOEs hold equity stakes in thousands of companies through complex, layered investment networks, which include other state-owned enterprises, publicly traded companies, privately held companies, and joint ventures with foreign businesses. Using Chinese corporate registration data, C4ADS mapped all subsidiaries or investment recipients within five degrees of SASAC.[17] **(Appendix 1: Network Visualization.)** SASAC's subsidiary and investment networks illustrate a key challenge with commercial network complexity and establishing national security risk in the Chinese commercial context. 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, particularly given the significant volume of investments that state-owned enterprises make in the Chinese economy.

Direct Participation: Financial Markets

In order to advance its industrial policy, the party-state engages in domestic and foreign capital markets directly through state-owned banks, state-owned asset management companies, and, more recently, government-guided investment funds (GGIFs). Similarly, China's policy banks, sovereign wealth funds, and state-run investment vehicles may help to make acquisitions. Recent innovations in financial markets are particularly relevant to understanding the risks that U..S investors may face from China's military-industrial complex.

Under General Secretary Xi Jinping, Chinese companies—including those that support China's military—have increasingly gained access to international financial markets by listing on stock exchanges in Shanghai, Shenzhen, and Hong Kong. In July 2019, the Shanghai Stock Exchange launched the Science & Technology Innovation Board ("STAR Market") in an effort to give Chinese technology companies greater access to foreign capital markets. The STAR Market is the most valuable stock market in Asia and has provided a significant boost to Chinese technology companies. A July 2020 report from U.S. Securities & Exchange Commission's Division

Aerospace Science and Technology Corporation (CASC), China Aerospace Science and Inudstry Corporation (CASIC), and China National Nuclear Corporation (CNNC).

[13] 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

[14] 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

[15] Leutert, W. (2020). p. 8.

[16] 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

[17] C4ADS sourced corporate registration data from a third-party provider, which collects the data from the Chinese government's corporate registry.

of Economic & 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 as a "national security threat."[18] A November 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.[19] By virtue of their presence in U.S. index funds, Chinese companies that may pose a serious national security risks are able to access significant pools of U.S. capital, including from some of the country's largest public pension funds.

Domestically, the Chinese government has increasingly used government guided investment funds (GGIFs) to drive capital toward companies that support its policy goals. To do so, central and local government entities establish investment funds with a defined purpose in line 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 February 2021, leading Chinese third-party aggregator of private capital markets data estimates that there are 1,741 GGIFs operating in China.[20] Unlike venture capital funds in the United States, only 27% of GGIFs are designed to support startups and early stage innovation.[21] [22] Instead, 62% of GGIFs are "industry funds" created to support the growth of targeted strategic industries.[23] For example, following government push for "indigenous innovation" for "core technologies,"[24] the number of registered companies working in semiconductors increased by 52% between 2018 and 2020, and the volume of investment by more than 800% over the same period increased.[25] 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.[26]

Alongside more traditional fiscal policy mechanisms, the Chinese party-state can use these financial market tools to direct private capital toward party-state industrial policy objectives. Perhaps the clearest case is China's semiconductor industry, which saw a quadrupling of equity investments from 30 billion RMB (4.6 billion USD) to 140 billion RMB (21.5 billion USD) between 2019 and 2020.[27] One GGIF alone, the China Integrated Circuit Industry Investment Fund, has made investments in 63 different companies in the industry since 2014.[28] By providing cheap capital that enables semiconductor companies to make investments in research and expansion, the

[18] 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
[19] 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
[20] Chinese third-party aggregator of private capital markets data
[21] Chinese third-party aggregator of private capital markets data
[22] Pan, F., Zhang, F., & 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
[23] Chinese third-party aggregator of private capital markets data
[24] *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
[25] 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
[26] Ma R. (2021, February 26)
[27] 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
[28] Chinese third-party aggregator of private capital markets data

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 IPO 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 CNIC Corporation, a state-owned sovereign wealth fund founded to operate in global—not domestic—markets.[29] In other words, by drawing on capital from multiple state-backed sources—a GGIF, a SOE, and a sovereign wealth fund—SMIC 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 five-fold since 2014.[30] However, these capital injections also advance state objectives by enriching opportunistic executives, as with Wuhan Hongxin Semiconductor Manufacturing.[31]

Direct Participation: Universities & Talent

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 certain benefits that the state provides.[32] While 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, other universities may support China's military R&D programs in less straightforward ways.[33] As one example, the Australia Strategic Policy Institute (ASPI) has identified and profiled more than 100 additional Chinese universities that work to varying degrees with China's military and security apparatus, e.g. through technology innovation parks or partnerships with state laboratories.[34]

Chinese universities, including but not limited to those involved in China's military research and development programs, also have holding companies that make significant commercial investments both domestically and internationally. Corporate registry filings indicate that Chinese universities maintain significant ownership interests in mainland China-based companies that appear to operate primarily in the research and development as well as consulting services sectors.[35] For example, Chinese corporate records report that Harbin Institute

[29] Semiconductor Manufacturing International Corporation. (2020). *Semiconductor Manufacturing International Corporation: Annual Report 2019*. http://www.smics.com/uploads/e_00981ar-20200418.pdf
[30] Cajing. (2021, January 29). **中国半**导体行业会不会迎来整合潮？ | **新年展望**. Finance.Sina.Com.Cn. https://finance.sina.com.cn/roll/2021-01-29/doc-ikftssap1761247.shtml?cref=cj
[31] 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/
[32] 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
[33] 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 & D. K. Tatlow, Eds.). Routledge.
[34] *Chinese Defence Universities Tracker—Home*. Chinese Defence Universities Tracker. https://unitracker.aspi.org.au/
[35] Chinese third-party aggregator of corporate registry data

of Technology (哈尔滨工业大学), one of the Seven Sons of National Defense, maintains direct or indirect ownership interests in approximately 1,000 China-based companies and owns a 50-percent or greater ownership interest in approximately 50 entities.[36] These subsidiary companies support China's military-civil fusion and technology transfer efforts through "legal, illegal, and extralegal"[37] means both domestically and abroad.

For example, Chinese corporate registration documents indicate that Tsinghua University Holding Company has a controlling stake in TusPark, a company that builds technology parks domestically and abroad. TusPark in turn has investments in 65 companies, including the National Military-Civil Fusion Industry Integration Fund and Beijing Highlander Technology.[38] In an example of illicit technology transfer, Department of Justice indictment filings from 2019 indicate that Beijing Highlander Technology attempted to acquire U.S. Navy submarine rescue technology for the PLA Navy "through a structured scheme using several front companies" abroad.[39]

Certainly, university investments in related organizations are not necessarily indicative of illegal or illicit technology transfer operations. Moreover, the national security significance of a university's stake in companies remains uncertain, given the extent to which university-affiliated holding companies participate in the global economic system. Future research should examine the relationship between China's defense-affiliated universities and companies in China, and consider how those companies may expose the United States and allies to China's military-industrial complex in ways that undermine national security interests.

Beyond universities and their companies, the Chinese government also coordinates global talent recruitment programs that target Chinese and foreign nationals for professional opportunities at Chinese universities and companies operating in priority sectors ranging from agriculture to biotechnology.[40] 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, state-owned enterprises, defense research and academic institutions, national laboratories, 'private' industry, domestic and overseas 'NGOs,' and global diaspora organizations."[41] China's talent programs—which recruit Chinese and foreign nationals alike—do not necessarily constitute illegal activity, and recent criminal prosecutions against Asian American academics in the United States have sparked debate about how the policy tools currently available to address illicit technology transfers through participation in talent programs may not be adequately designed and risk prosecutorial overreach and racial profiling.[42]

---

[36] Chinese third-party aggregator of corporate registry data
[37] *China's Quest for Foreign Technology.* p. 7 (W. C. Hannas & D. K. Tatlow, Eds.)
[38] Chinese third-party aggregator of corporate registry data
[39] USA v. Viau (2019), Criminal No. 2019-0009 (D.D.C. 2019), and United States v. OCEANWORKS INTERNATIONAL CORPORATION (2019), Criminal No. 2019-0304 (D.D.C. 2019) accessed through PACER.
[40] 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/
[41] *China's Quest for Foreign Technology.* p. 39 (W. C. Hannas & D. K. Tatlow, Eds.)
[42] 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

Indirect Influence: Interlocking Private Business in Political Institutions

China's party-state co-opts business leaders into formal political institutions, including but not limited to the Chinese Communist Party, the Party Congress, the People's Congress, and the People's Political Consultative Conference at all levels of administrative governance. At the national level, the China People's Political Consultative Conference (CPPCC) has a constituent committee that functions as a national chamber of commerce, called the All-China Federation of Industry & Commerce (ACFIC). The CCP's United Front Work Department 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.[43] Today, ACFIC functions as a formal institutional channel for private companies to lobby the government within the party-state apparatus, and 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."[44] One previous study found that for 95 of the top 100 private firms and 8 of the top 10 internet companies, the founder or the de facto controller was currently or formerly part of the People's Congress or the People's Political Consultative Conference.[45] C4ADS research also indicates that some members in ACFIC leadership and on ACFIC subcommittees also have familial connections to Chinese Communist Party elites, worked previously in the People's Liberation Army, or participate in ACFIC in their capacity with the Ministry of Public Security, United Front Work Department, or other government organizations. Forthcoming C4ADS analysis also indicates that ACFIC members control companies with substantial overseas investments, which have not been systematically examined for their possible national security implications to date. While CCP membership may not alone be a significant signal about a person's political alignment with the party-state given the number of CCP members and range of non-political incentives for joining, participation in political institutions that formally comprise the Chinese polity—where participation is circumscribed—indicates a greater degree of political exposure to the party-state apparatus.

Indirect Influence: Industrial Associations & Party Committees

Industrial associations provide the Chinese party-state with a mechanism for extralegal influence over companies in the private sector. Milhaupt and Zheng (2016) note that 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.[46] [47] The All-China Federation of Industry & Commerce directly oversees 31 industrial associations including in fields such as agriculture, energy, cosmetics, real estate, and more.[48] In September 2020, the Chinese Communist Party issued new guidance on strengthening the

[43] Huang, D., & 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
[44] Huang, D., & Chen, M. (2020)
[45] Milhaupt, C. J., & 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
[46] For background on industrial associations and their relationship to the Chinese party-state, see Milhaupt, C. J., & Zheng, W. (2015), p. 686
[47] 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
[48] *All China Federation of Industry and Commerce*. Acfic.Org.Cn. http://www.acfic.org.cn/zzjg_327/

role of the CCP 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.[49] As Milhaupt and Zheng (2016) note, 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.[50]

Party committees at companies also serve to provide the party-state with an extralegal means of corporate influence and control. 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.[51] While private companies are not necessarily required to have such committees, the number of those that do is growing. ACFIC survey data indicate that 48.3% of private firms in China have party committees, according to analysis conducted by Neil Thomas at the Paulson Institute.[52] On average, there has been a 2.1% increase in the number of private firms with reported party committees over Xi Jinping's tenure, which will likely continue to rise given the CCP's priority on the subject.[53] The survey data also indicate that party organizations are more common at bigger companies.[54] 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.[55]

In sum, China's party-state apparatus interacts with companies in a networked corporate environment to support its military-industrial base through both formal and informal mechanisms. These include appointing and managing leadership at state-owned enterprises, 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 and party committees. While those mechanisms do not guarantee full control over companies, they provide a range of tools to coerce or induce companies toward its policy objectives in ways that are both similar to and distinct from mechanisms for state-business relations in countries like the United States. To properly assess national security risks for engagement with a Chinese enterprise, U.S. investors and policymakers must therefore consider the unique features of China's political economy.

2. **A framework for assessing U.S. national security risks in Chinese companies should include not only equity ownership analysis but also attention to the conditions of China's domestic political economy that may render companies vulnerable to party-state co-option.**

[49] *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
[50] Milhaupt, C. J., & Zheng, W. (2015), p. 685
[51] 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 Labour Organization. https://www.ilo.org/dyn/natlex/docs/ELECTRONIC/92643/108008/F-186401967/CHN92643%20Eng.pdf
[52] 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
[53] Thomas, N. (2020, December 16)
[54] Ibid
[55] 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/

By understanding the direct and indirect ways that the party-state relates to companies in China, we can develop a framework for assessing the risk that a company's commercial activities may advance China's national security interests at the expense of the United States. My framework draws upon theory developed by William Norris to understand the conditions under which the Chinese party-state can successfully conduct economic statecraft, and by Meg Rithmire to disaggregate the logics by which Chinese companies pursue globalization. In this framework, I emphasize signals that are observable in public records and could therefore be used as generalizable heuristics for risk assessments by the range of U.S. companies, investors, universities, and others exposed to national security risk from China.[56] Specifically, U.S. policymakers should consider the following:

A. Party-state equity for financing
B. Political exposure
C. Industry sensitivity
D. Market structure, and
E. Goal compatibility between the company and the party-state.

Each element is considered in turn below.

A. Party-state equity or financing

While not sufficient in isolation, equity ownership analysis can provide information about how a company relates to the party-state and the mechanisms through which the party-state may co-opt the company to advance its policy interests.[57] First, policymakers should use publicly available corporate registry documents to determine whether or not the company is a state-owned enterprise. If so, U.S. law classifies those enterprises as a "foreign instrumentality," even as the company may operate with both market and policy incentives.[58] If the company is not a state-owned enterprise, policymakers should assess whether state-owned entities (like government-guided investment funds) may have taken equity stakes in the company. Bai et al. (2020) note that most equity investments by state-owned companies are not controlling stakes.[59] Public Chinese corporate records contain shareholder information and can be accessed for free, but websites are often unreliable to access and require Mandarin proficiency. Additionally, many beneficial ownership records in the United States, like U.S. Securities & Exchange Commission disclosure forms, do not include company or person names in Chinese, which can vary significantly from the English or Romanized name and therefore limit an analyst's ability to conduct comprehensive due diligence using Chinese public records.

B. Political exposure

[56] Norris, W. J. (2016) and Rithmire, M. (2019, June, Revised 2021, January)
[57] 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, I 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.
[58] Definition: foreign instrumentality from 18 USC § 1839(1) | LII / Legal Information Institute. (2016).
[59] 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

While the political enmeshment of a company's officers may be difficult to assess, policymakers and regulators should determine whether or not a company's shareholders, directors, or officers concurrently hold leadership positions in Chinese party or government institutions, on corporate Party committees, or at Chinese industrial associations.

While Chinese Communist Party (CCP) membership may be a weak signal in China given the ubiquity of the party and range of incentives that may exist for CCP membership, business leaders that participate in the People's Political Consultative Conference (which exists at all levels) may be at increased risk of political enmeshment with the Party, given that such membership is an invite-only institution designed to connect the Party with private business. Similarly, regulators should determine whether individuals participate in the People's Congress or serve in leadership positions with the Party or its constituent Congress/committees. Membership lists are often public for PPCCs and PCs but do not always contain the personally identifiable information required to disambiguate person identity across multiple data sources. Government organizations and financial regulators should ensure that their lists of Politically Exposed Persons (PEPs) in China include membership for these organizations, which will better support efforts to counter both kleptocracy and Chinese economic statecraft through business enterprises. Ideally, Chinese PEP lists would also include family members and associates, as factional politics remain a key feature of China's domestic political economy and contextualize the relationship between a business and the state.[60]

Because Party committees play a key role in corporate governance in China, policymakers should require that Party committee leadership is included in corporate disclosures related to beneficial ownership when investing in the United States. Party committee information is rarely public, including in Chinese corporate ownership records. Future research should seek to derive other metrics, like firm size or investment density, that could provide more robust empirical indicators about the degree to which a Chinese company is politically enmeshed within the party-state apparatus.

C. Industry sensitivity

Certain industries in China may be subject to greater party-state interest or scrutiny in China. For example, China has identified specific technologies like semiconductors and biotechnology as priorities for investment and development, and industries like real estate development need close regulatory attention.[61] If a Chinese enterprise is involved in a priority sector, then it may face market and political incentives to align with the party-state's policy priorities. In his work on Chinese economic statecraft, William Norris (2016) observes that unity of the state across all levels of government is a critical factor in whether or not the Chinese government can successfully instrumentalize companies toward its policy objectives.[62] Given this insight, policymakers and investors should pay particular attention to the Chinese party-state's stated

[60] For example, the *Wall Street Journal* reported that General Secretary Xi Jinping personally intervened in scuttling Ant Group's Shanghai IPO in part because it would have enriched his political rivals. See Wei, L. (2021, February 16). China Blocked Jack Ma's Ant IPO After Investigation Revealed Likely Beneficiaries. *The Wall Street Journal*. https://www.wsj.com/articles/china-blocked-jack-mas-ant-ipo-after-an-investigation-revealed-who-stood-to-gain-11613491292

[61] 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

[62] Norris, W. J. (2016)

policy priorities, which may create national security risks across certain sectors of the Chinese economy.

Other data points in public records may also provide indication that a company's commercial activities align with core Chinese national security priorities. For example, if a company participates in state-sponsored talent programs, the company may have received some degree of endorsement that its commercial activities advance party-state priorities. Similarly, if the company has authorizations to produce military equipment and/or dangerous materials, or regularly accepts/engages in procurement tenders for the military, then it may have a commercial dependency on China's military-industrial base that incentivizes alignment with Party priorities. Because publicly traded companies undergo close regulatory scrutiny, 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—may warrant additional scrutiny from U.S. investors and policymakers to mitigate risk of exposure to China's military-industrial base.

D. Market structure

Norris (2016) notes that market structure – that is, the relative amount of resources or expertise between the state regulators and companies – has also been a key factor in cases when the Chinese party-state has been able to instrumentalize companies toward its policy objectives. In other terms, the Chinese party-state cannot as easily manipulate a firm when the number of companies under its purview or degree of technical expertise required for oversight and regulation are high. At the sectoral level, U.S. policymakers and regulators should therefore consider relationship of certain segments in 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. At the company level, policymakers and regulators should consider the extent to which a company's commercial success or growth priorities are dependent on market access in China, which may also create market incentives for political alignment with Chinese party-state policy objectives.

E. Goal combability[63]

Finally, regulators should consider the extent to which a company's commercial goals do or do not align with the party-state's policy goals. Meg Rithmire (2020) theorizes different logics by which Chinese companies may pursue globalization, which in turn produce different relationships between the business and the state: "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.[64] While companies may reasonably exhibit qualities across each bucket, regulators can improve their understanding of national security risk by considering the extent to which a company's economic incentives align naturally with party-state objectives, broadly defined.

[63] 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)
[64] Rithmire, M. (2019, June, Revised 2021, January)

While these five variables may be useful as generalizable heuristics for determining areas where policy attention should be most seriously focused, policymakers and investors should resist the urge to classify Chinese enterprises on a binary of "high" or "low" risk, as these variables can change over time. While "high risk" classifications may be appropriate in some cases (e.g. with Chinese state-owned defense contractors) it may be counterproductive in others, as it may undermine consensus among stakeholders looking to mitigate risk from China and the development of a targeted policy response around the areas in which risk is most acute. Because the nature of risk is dependent on threat, vulnerability, and consequence, risk assessments are best executed on a case-by-case basis, and the heuristics above can help policymakers or investors reduce the plane of scrutiny to a more manageable scope to conduct a more comprehensive investigation. Additionally, by considering these features as useful indicators of risk, policymakers can determine where disclosure or reporting requirements in the U.S. system (e.g. corporate beneficial ownership) can be reformed to improve the government's ability to identify risk more proactively.

3. Publicly available information is an essential yet underused resource in contextualizing national security risk within the Chinese corporate environment.

Beyond more effectively collecting and exploiting data in the United States, the U.S. government can improve its ability to mitigate national security from China by more effectively exploiting publicly available datasets in the Chinese data environment. In September 2020, following a two-year review of the U.S. intelligence community's (IC) 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."[65] Among its unclassified findings, HPSCI stressed that the importance of non-traditional customers in 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.[66]

While several experts have previously recommended to the Commission that the U.S. government establish an open source center to better disseminate Mandarin-language materials to the policymaking community, most recommendations have focused attention on data sources that are within the traditional open source intelligence (OSINT) taxonomy, such as academic literature, news media, and policy documents.[67] However, there exists a significantly broader range of high-value sources of publicly available information that can provide actionable information about national security threats from China, which should also be more effectively exploited. In today's data environment, publicly available information (PAI) can inform analytic products that replicate the integration of multiple traditional intelligence disciplines and are free from classification restrictions that slow or inhibit dissemination across the

[65] 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

[66] Ibid

[67] For example, see Greitens, S. C. (2021, January). *Internal Security & Grand Strategy: China's Approach to National Security under Xi Jinping*. U.S.-China Economic & Security Review Commission. https://www.uscc.gov/sites/default/files/2021-01/Sheena_Chestnut_Greitens_Testimony.pdf, or Fravel, M. T. (2021, January). *Testimony before the US-China Economic and Security Review Commission Hearing on "US-China Relations at the Chinese Communist Party's Centennial."* U.S.-China Economic & Security Review Commission. https://www.uscc.gov/sites/default/files/2021-01/M_Taylor_Fravel_Testimony.pdf

government interagency, with industry stakeholders, or with partners internationally. Additionally, PAI can support actionable analysis at a significantly lower cost to help the IC direct its more expensive technical resources toward the most difficult intelligence requirements. Examples of publicly available datasets that have been used to expose and respond to national security threats from China include but are not limited to the following:

- 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, e.g. property, vessels, aircraft;
- Tender data that details government contracts, the companies supporting military technological development, and the capabilities that the PRC solicits from private enterprise;
- Academic publications, conference proceedings, details of masters and doctoral theses, lists of staff at institutions, science & technology awards, fellowship programs, and other academic-related datasets, which can provide information about possible international exposure China's military research & development 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;
- Signals data for vessel and aircraft positions;
- Domain registration records and web traffic data;
- Data containing details of selectors used by individuals, for example phone numbers, and social media accounts; and
- Databases for known PEPs and/or leadership in China's political institutions.

Because of the quality and variety of publicly available information in the world today, CSIS's Technology and Intelligence Task Force, co-chaired by current Director of National Intelligence Avril Haines, recommended that policymakers reimagine "how the IC's OSINT mission should be organized."[68] Given the complexity of the threat environment in China, there are several challenges that organizations will have to consider in order to exploit publicly available information to mitigate national security risks in engagement with the Chinese commercial and academic space.

- **Deep subject matter expertise.** China's political economy exhibits features that require careful treatment and analysis. Successful investigations require prior exposure to illicit activities in China, including an understanding of the different typologies of activity that have been used in the past. Additionally, successful investigations may require some degree of industry specialization in order to properly understand technical details or sector-specific risk factors.

[68] Center for Strategic and International Studies. (2021a). *MAINTAINING THE INTELLIGENCE EDGE: Reimagining and Reinventing Intelligence through Innovation*. https://csis-website-prod.s3.amazonaws.com/s3fs-public/publication/210113_Intelligence_Edge.pdf

- **Data acquisition.** While broadly available, Chinese datasets prove difficult to acquire because of the time needed for identification and collection and for overcoming the barriers to access on certain websites. For example, many Chinese sites require a Chinese IP address or other credentials, presenting a technical obstacle to access and collection. Identifying these data sources in this first place also requires analysts with subject matter and language expertise. Moreover, certain analytic questions may require significantly more preparation time than others, as subject matter experts identify available data, assess its strengths and limitations to ensure that it could be used appropriately, and determine that derivative outputs will be sufficiently robust (i.e. judicially admissible).

- **Data integration, fusion, and management.** Given the complexity of Chinese corporate networks and party-state influence in the commercial space, due diligence investigations related to China's military-industrial complex require significant amounts of data from diverse sources in variable formats. Relevant data may include unstructured documents, flat files, and high-volume structured data, which must be integrated, standardized, cleaned, and modeled in order to be exploited with the timeliness required to be actionable. Chinese names—for companies and individuals—may be difficult to disambiguate without other unique identifiers (e.g. ID numbers for companies or people) that facilitate entity resolution across English and Chinese language data sources. Relatedly, U.S. public records often do not capture information that is essential to conduct a comprehensive due diligence investigation on Chinese corporate networks. For example, while U.S. SEC Filings contain significant amounts of information about the people and companies investing in the United States, they rarely contain the Chinese names for people or companies that would be required to investigate those companies or people in Mandarin-language sources, which dramatically slows the investigative process and limits the potential for conducting risk-screening at scale. To do so, organizations will require technology that can integrate, process, and manage disparate data at a scale of hundreds of millions or billions of records, with the ability to refresh data on a regular basis. Data integration pipelines are complex and require additional services, such as machine translation and natural language processing, to enable use by non-Mandarin speakers and extract entities from unstructured documents, respectively. Finally, the data integration, fusion, and management must have a strong auditability function to track data provenance and support policy interventions with judicially admissible standards of evidence.

- **Analysis.** Subject matter experts require experience leveraging bulk structured and unstructured data to develop and test appropriate analytic tradecraft. Increasingly, technology companies are developing data management and exploitation tools that facilitate domain subject matter experts (e.g. China political analysts) in managing and analyzing data, even without significant technical training. Given the complexity of national security investigations on China, analysts would be best served with tools that provide not only a simple point-and-click interface for search, analysis, and visualization but also more complex back-end environments through which data scientists can implement advanced analytic approaches (e.g. machine learning) for more proactive alerting.

As HPSCI noted in the September 2020 China Deep Dive, "open source intelligence (OSINT) will become increasingly indispensable to the formulation of analytic products [on the China target]."[69] Given the quality and variety of publicly available information, analysts can replicate the integration of multiple traditional sources of intelligence to produce analytic products with the timeliness and quality required to support meaningful law enforcement action. Publicly available information can facilitate information sharing between the broad range of stakeholders inside and outside government who may unwittingly expose the United States to national security risks, and who therefore must be engaged in order to develop an effective response. It can also help the IC, which faces ever broader intelligence requirements on an increasingly multifaced threat, direct its most specialized assets toward most sensitive and difficult intelligence questions.

Bottom line: China's political economy poses systemic national security risks to the United States, but publicly available information can support policymakers and investors with the data they need to protect U.S. interests.

China's political economy creates systemic national security risks for the United States. In order to properly appraise and mitigate risk, U.S. policymakers and investors must be sensitive to the formal and informal mechanisms through which the party-state exerts control or influence over companies, universities, and other actors in China's commercial and research sectors. While some have suggested that "the actions or potential actions of every Chinese firm are ultimately subordinate to the control of the Party,"[70] the Party's latest efforts to reassert CCP primacy over the commercial sector suggest that this is not the case. Instead, it seems that as judged from the Party's view, there is still insufficient control on private commercial actors who, through the wealth they generate, can pursue commercial objectives regardless of party-state policy goals. Because China's party-state uses both legal and extralegal mechanisms to influence companies and universities toward its policy objectives, U.S. policymakers and regulators will continue to face challenges in appraising where the costs of engagement with Chinese enterprises outweigh the benefits, and in developing policy responses that mitigate national security risks.

Several studies have provided comprehensive accounts of the actors that comprise China's military-industrial base, such as state-owned defense contractors, government-guided investment funds, universities, state labs, and other supporting party-state institutions. Others have also detailed China's extensive, deliberate efforts to acquire foreign technology and conduct intelligence operations against the United States and its allies. In this testimony, I have emphasized the more fundamental features of China's domestic political economy that expose the United States to national security risk even in the absence of state-sponsored operations, which have received comparatively less attention in discussions about how policymakers should respond to the China challenge. As the U.S. grapples with mitigating the risks of engagement with China's commercial and academic sectors, it must be attentive to the ways in which the country's "special deals" economy and informal corporate governance institutions result in relationships between businesses, universities, industrial associations, and the state that are fundamentally different from the institutional relationships that comprise the U.S. economy. If

[69] House Permanent Select Committee on Intelligence. (2020), p. 29
[70] The Office of Senator Tom Cotton. (2021, February). *Beat China: Targeted Decoupling and the Economic Long War*. https://www.cotton.senate.gov/imo/media/doc/210216_1700_China%20Report_FINAL.pdf

policymakers and observers do not appreciate those differences, they may continue to produce threat assessments that overstate loose notions of "CCP malign influence" and understate more fundamental vulnerabilities that our rules-based, market-oriented system faces in extensive commercial engagement with China's "special deals" economy.

In some cases, as with responses to the COVID-19 pandemic or climate change, it will be 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. 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 reinforcing our liberal democratic values in the process).[71] These types of policy solutions can 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.[72]

Going forwards, publicly available information should be treated as an indispensable tool in both diagnosing the nature of threats from China and prescribing empirically-grounded policy responses. While some have recommended that the U.S. government devote more resources to translating and disseminating Chinese policy documents and gray literature, there exists a significantly broader range of high-value datasets in the public domain that U.S. policymakers and investors can and should use to mitigate national security risk.

Academics like Bai, Hsieh, and Song (2019) have demonstrated that rigorous data science work applied to Chinese corporate data can help discern the otherwise elusive networks of state/private collusion that are critical to China's party-state economy. U.S. policymakers should therefore reimagine the role that publicly available information can play in identifying and responding to threats from China—not only in providing a low-cost, first-stop solution to establish a baseline for the nature of the threat, but also in producing analytic products that can be more easily disseminated across the government's interagency, with industry, and with partners internationally.

To this end, the United States will need a national data strategy that it is fine-tuned to the ever increasing volume of high-value, publicly available datasets from China.[73]

---

[71] 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.

[72] Lindsay Gorman at the German Marshall Fund has discussed the importance of affirmative messaging in the context of U.S. partnership with the European Union on threats from China. See Gorman, L. P. [@LindsayPGorman] (2021, February 28). U.S. Enlists Allies to Counter China's Technology Push. Key point: The strategy has both offensive and defensive components. I hope we'll see more on the offensive, affirmative agenda in the coming months too. [Tweet] Twitter. https://twitter.com/LindsayPGorman/status/1366059094419910668?s=20

[73] In 2018, the U.S. government began to develop and implement a Federal Data Strategy to improve the government's ability to leverage its data as a "strategic asset," but its scope is focused primarily on the federal government's current data holdings. For more information, see *Welcome - Federal Data Strategy*. Federal Data Strategy. https://strategy.data.gov/

That strategy must pay attention to the specific details of Chinese datasets, where even minor changes in bureaucracy (e.g. how company names are recorded on disclosure forms to the U.S. government or the Entity Lists it publishes) can yield significant dividends in the analytic process for government agencies, financial institutions, investigative reporters, and others who have a role to play in protecting U.S. interests. As we continue to bring more stakeholders inside and outside government into the fold, standard approaches to data collection and modeling—particularly as it relates to publicly available sources intended for broader consumption—must be a top of mind consideration.

In the meantime, policymakers have a range of open questions for which they must find solutions, whether in enforcing export controls or financial sanctions against massive Chinese conglomerates, adjusting the Foreign Investment Risk Review Modernization Act (FIRRMA) and Foreign Agents Registration Act (FARA) to reflect our changing understanding of Chinese corporate entanglements, or reimagining how the national security enterprise should relate to new sources of data.

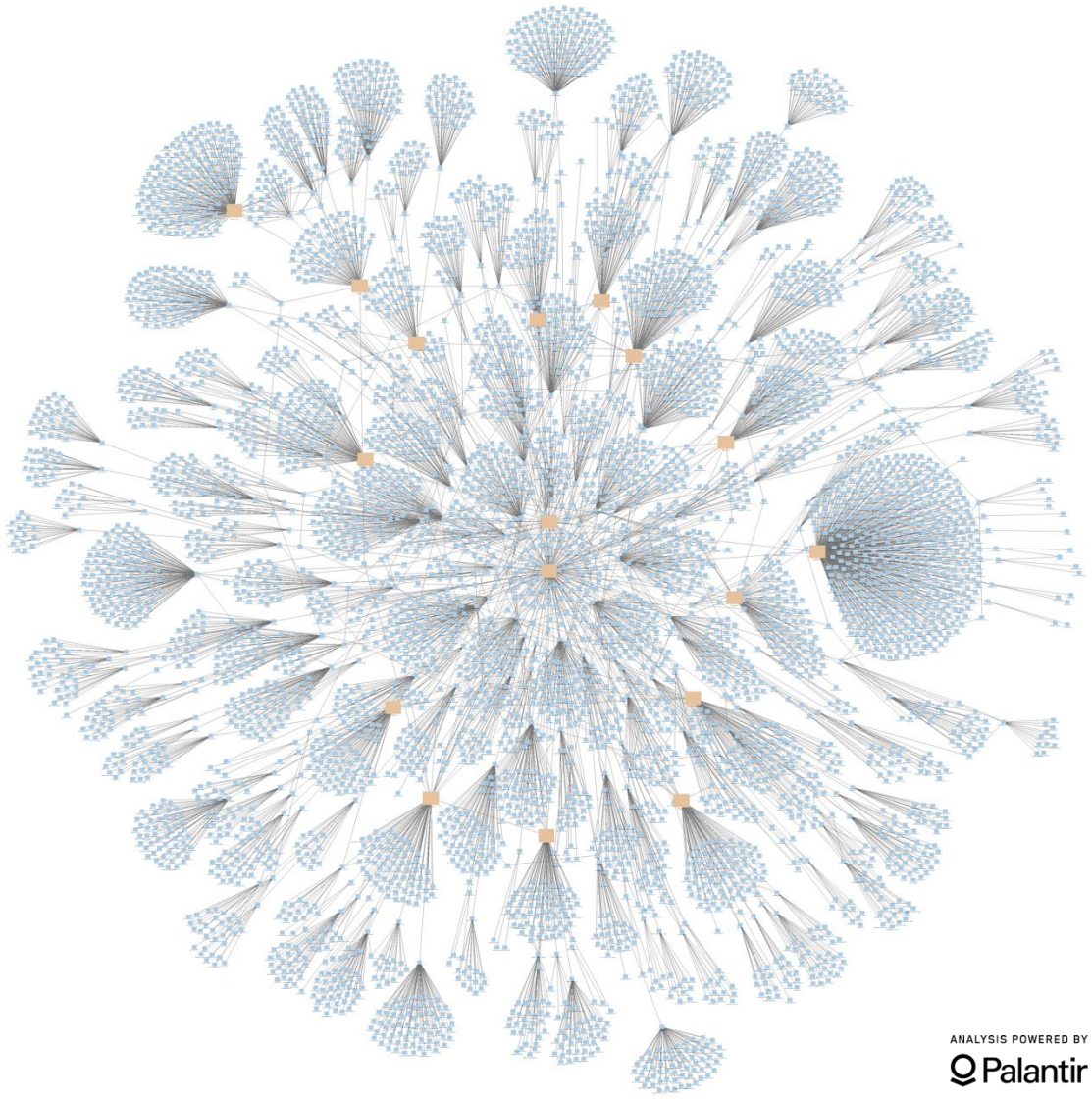
Throughout this work, analysis derived from publicly available information will be key. While PAI cannot replace the work of traditional intelligence agencies, it will help ensure that the intelligence community – whose requirements are growing far faster than its resources – can focus its capabilities on the hardest and most intractable of problems. In the coming years, PAI will become an increasingly important tool for protecting U.S. national security interests, and nowhere is that focus more needed today than in assessing U.S. exposure to China's military-industrial complex.

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."[74] Indeed, China's commercial system introduces complex national security threats that will require sustained attention and collaboration from a broad range of people who have expertise to contribute. I look forward to continued dialogue about these issues, their related policy implications, and the ways that new approaches to data and technology can help promote "constructive vigilance"[75] in the United States and among our allies.

[74] 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

[75] Schell, O., & Diamond, L. (Eds.). (2018, November). *China's Influence & American Interests: Promoting Constructive Vigilance*. The Hoover Institution. https://www.hoover.org/research/chinas-influence-american-interests-promoting-constructive-vigilance

Appendix 1: Companies within Five Degrees of China's State-owned Assets Supervision & Administration Commission (as Subsidiary or by Investment)



The above graph depicts all companies that are either subsidiaries of or recipients of investments from the State-owned Assets Supervision & Administration Commission (SASAC) within five degrees. SASAC is directly subordinate to the State Council and responsible for managing central SOEs.