BASC WORKING PAPER SERIES

THE RISE OF CHINA AS A CYBERSECURITY INDUSTRIAL POWER: PRINCIPLES, DRIVERS, POLICIES, AND INTERNATIONAL IMPLICATIONS

Tai Ming Cheung

Working Paper 2018-03

BERKELEY APEC STUDY CENTER
552 Barrows Hall
University of California
Berkeley, California 94720-1950
September 2018

This paper is part of a project "Comparative Industrial Policy in the Cyber Security Industry: Policies, Drivers, and International Implications," organized by Vinod K. Aggarwal and Andrew Reddie of the Berkeley APEC Study Center, UC Berkeley. The author would like to thank the Institute on Global Conflict and Cooperation for its continuing support as well as UC Berkeley's Center for Long-Term Cybersecurity, Institute for East Asian Studies, and Berkeley APEC Study Center for its support of the comparative industrial policy workshop series. The author would also like to thank Graham Webster, Phil Stupak, Barry Naughton, and Andrew Reddie for comments on prior drafts of this manuscript.

The Rise of China as a Cybersecurity Industrial Power:
Principles, Drivers, Policies and International Implications
Tai Ming Cheung
BASC Working Paper No. 2018-03

Abstract

This paper examines China's cybersecurity industrial development over the past two decades since the arrival of the internet in that country. This analysis takes place from a primarily security and technology perspective because the national security apparatus occupies a powerful presence in China's cyber affairs. Moreover, the development of the cybersecurity industry is significantly driven by the development of technological capabilities. Key issues explored include: 1) Chinese decision-making and thinking on cybersecurity development within the context of the Chinese leadership's general approach to development, national security, and technology advancement; 2) the nature and characteristics of recent Chinese cybersecurity-related development strategies and plans; 3) the drivers behind the development of China's cybersecurity industry, looking especially at market failures, national security rationales, and government intervention; 4) the proliferation of principal actors and coalitions in the Chinese cybersecurity industry and how this influences its development; and 5) the nature of the relationship between the state and cybersecurity firms, in particular examining four types of interactions: the state as a customer; state hiring of talent; the state's direct regulatory power, and the state as an investor. The paper concludes by considering the international implications of China's rise as an increasingly capable and confident cybersecurity power.

Tai Ming Cheung[1]
UC Institute on Global Conflict and Cooperation
1218 Robinson Building Complex
University of California, San Diego
La Jolla, California 92093-0518
tcheung@ucsd.edu

[1] Tai Ming Cheung is the director of the Institute on Global Conflict and Cooperation (IGCC) located at the University of California, San Diego in La Jolla, California. He leads the institute's Study of Innovation and Technology in China (SITC) that examines China's efforts to become a world class technology power. Dr. Cheung is also an associate professor at the School of Global Policy and Strategy at UC San Diego.

Introduction

An apt, if unflattering, description of China's cybersecurity industry in the late 2010s is that it is big but not strong. The industry has enjoyed two decades of rapid growth propelled by high level leadership support, deepening international economic, technological, and security competition especially over cyber-espionage activities, and the pressing need of the Chinese Communist Party (CCP) to exert tight information control over the world's largest Internet user community. But this boom has not led to the emergence of any internationally recognized Chinese cybersecurity firms and the country has become a hotbed for malicious cyber activity, both domestically and internationally.[2]

To address this problematic state of affairs, the Chinese authorities declared in the 2016 Outline of National Information Development Strategy that the "building of a strong cyber nation (网路□国) is an urgent matter and no time should be wasted."[3] They have formulated a wide-ranging series of development strategies and plans since the mid-2010s that sets out a detailed roadmap for China's informatization and cybersecurity advancement into the 2020s and beyond.[4] This is tightly coupled with a broader effort to fundamentally reform China's development model from industrial catch-up to innovation driven growth. What this means is a far-reaching overhaul of the country's industrial economy, national innovation system, state-market relations, and the integration between the civilian and defense portions of the national economy. However, entrenched political and bureaucratic interests, deep-seated structural weaknesses such as bureaucratic fragmentation, a weak regulatory regime, and competing economic and security rationales stand in the way.[5] Nonetheless, the prospects for China to become a potent cyber power appear promising because of the highly effective top-down mobilizational capacity of the Chinese authoritarian system to successfully carry out select critical priorities.

To understand the nature, drivers, dynamics, trajectory, and international implications of the rise of China as a leading cybersecurity industrial power, this paper will address a number of questions using Aggarwal and Reddie's framework associated with this special issue.[6] First, what are the key political, economic, security, and strategic drivers responsible for shaping Chinese cybersecurity industrial policy making, implementation, and operation? Second, what kind of 'strong' cybersecurity industry are the Chinese authorities seeking to construct, especially in

---

[2] In Symantec's 2016 annual Internet security threat report, China was identified as the source of the most bot activity in the world during 2015, accounting for 46.1 percent of total global bot activity compared to the U.S. in second place with 8 percent. Symantec Corp., ***Internet Security Threat Report***, Vol.21, April 2016.

[3] Chinese Communist Party Central Committee General Office and State Council General Office, ***Outline of National Informatization Development Strategy***, 27 July 2016. Although what is meant by being a "strong cyber nation" is not explicitly defined, the strategy points out that key weaknesses in China's cyber capabilities include: 1) lack of 'core technologies'; 2) underdeveloped information technology infrastructure; 3) seriously challenged internet security; and 4) a poorly developed legal and governance regime.

[4] Informatization as commonly used in China refers to the process of social, economic, and technological change that transforms states from the industrial into the information age.

[5] See "Opportunities, Challenges for China Information Security Industry", ***Liaowang [Outlook Magazine]***, 16 April 2012.

[6] Aggarwal and Reddie, 2018.

terms of the balance between state vs. market, commercial vs. security, open vs. insular? Third, what are the principles, guidance, and implementation mechanisms being applied in the development of China's cybersecurity industry? Fourth, who are the key actors and coalitions in the forging of China's cybersecurity system and how do they interact and align with each other?

Conceptually, this paper addresses the examination of the development of China's cyber industrial capabilities primarily from a security and technology perspective. This is because the national security apparatus –which includes the military, internal security, law and order, intelligence, and information control apparatuses- occupies a powerful presence in China's cyber affairs. Moreover, the development of the cybersecurity industry and associated information technology domain is significantly driven by the development of technological capabilities.

Organizationally, the paper will begin by locating Chinese decision-making and thinking on cybersecurity development within the context of the Chinese leadership's general approach to development, national security, and technology advancement. Section 3 will then turn to the nature and characteristics of Chinese cybersecurity-related development strategies and plans that have been issued in the past few years, especially under Xi Jinping's rule. This will be followed in section 4 by an examination of the development of China's cybersecurity industry, especially addressing market failures and government intervention. There will also be an extended discussion in section 5 of the national security rationales for state intervention. Section 6 considers the proliferation of principal actors and coalitions in the Chinese cybersecurity industry and how this influences its development. There is discussion of six major players: the Communist Party; the government system; the People's Liberation Army; the national security apparatus; the academic research and development system; and the corporate cybersecurity industry. Section 7 addresses the nature of the relationship between the state and the cybersecurity firms, in particular in particular focusing on four types of interactions: the state as a customer; state hiring of talent; the state's direct regulatory power, and the state as an investor. The paper finishes with a discussion of the international implications of China's rise as an increasingly capable and confident cybersecurity power, especially addressing what kind of increasingly prominent role that China under Xi Jinping is carving in the global cyber order.

2. Chinese Thinking and Policy Approaches on Development, National Security and Technology Advancement and Its Application to the Cybersecurity Domain

China's present day political economy consists of various actors interacting with a swirling mixture of state and market influences. Legacy elements and interests of the once dominant centrally planned economy continue to exert considerable sway despite efforts to implement market reforms and promote opening up to the outside world. At the industry level, a key factor in determining whether state or market forces are in the ascendancy is whether the industrial sector is categorized by the central authorities to be of a 'strategic' nature. However, what constitutes a 'strategic industry' (□略性□□) is far from clear as the label is constantly evolving and influenced by changing political, economic, and national security considerations. There are core strategic industries that are defined by their direct relevance to national security, such as the defense industry. But other sectors that have been classified as strategic by the Chinese government include those deemed to be critical to national infrastructure, which can be

very broad and covers finance, energy, utilities, and telecommunications.[7] The Xi Jinping regime has adopted a far more expansive view of what constitutes national security than previous administrations. The 2015 National Security Law, for example, identifies 11 areas that are important to national security: political, territorial, military, economic, cultural, social, ecological, science and technology, information, nuclear, and natural resources.[8] The law also requires that technology that supports crucial sectors must be "secure and controllable," which is a high priority for the cybersecurity industry.[9] Not surprisingly, cybersecurity is classified as strategic because of its importance to national and economic security and political control.

Central authorities play an especially active and interventionist role in shaping and guiding the development of strategic sectors, especially those that are technological in nature and have significant national security content. A central organizing principle in framing Chinese official thinking and policy making in this area is techno-nationalism. The 2006-2020 Medium and Long-Term Science and Technology Development Plan (MLP) is a leading example of a Chinese state plan that is avowedly techno-nationalistic in nature. The MLP argues that the only way that China can advance against international competition is to "improve its independent innovative capabilities and master a number of core technologies, own a number of proprietary intellectual property rights and groom internationally competitive enterprises in important fields." To achieve this, one of the central concepts in the MLP is the notion of indigenous innovation. This term is viewed "by some as a regression to the self-defeating techno-nationalist notions of self-reliance from the Maoist era," although the MLP seeks to define this concept not only from an ideological viewpoint but also from a functional perspective.[10]

The key elements of contemporary Chinese techno-nationalist doctrine that can be found in the MLP and other plans are:

- Technological development is strategic and has implications for the relative position of the state in the global military and economic balance.
- The state must invest in critical technological sectors because of the high risks and lengthy time cycles involved in high-technology R&D.
- The state should pursue import-substituting indigenization.
- The state must nurture an indigenous capacity to innovate.
- Technology diffusion, whether through spin-offs or spin-ons, should be a central long-term goal.

This techno-nationalist ideology coexists with a healthy dose of pragmatic opportunism that allows for flexibility and compromise in policy choices. This allows in particular for the embrace of more inclusive techno-globalist approaches, especially if this helps to advance technological innovation more rapidly and effectively.

---

[7] Roselyn Hsueh, ***China's Regulatory State: A New Strategy for Globalization*** (Ithaca, NY: Cornell University Press, 2011).

[8] "China Approves Sweeping Security Law, Bolstering Communist Rule," ***New York Time*s**, 1 July 2015.

[9] "Jitters in Tech World Over New Chinese Security Law," ***New York Times***, 2 July 2015.

[10] Cong Cao, Richard P. Suttmeier, and Denis Fred Simon, "China's 15-Year Science and Technology Plan", ***Physics Today***, December 2006, p40.

China embraced key elements of techno-globalist thinking in the early 1990s by opening up the national economy to FDI and rolling back state dominance of the S&T system by allowing participation from private and other non-state firms.[11] This led to massive inflows of foreign investment into the medium and high-technology sectors by multinationals, and soaring imports of technology goods by foreign and Chinese firms throughout the 1990s. In addition, large numbers of entrepreneurial domestic and foreign joint venture new technology enterprises were established or spun off from the state sector and quickly emerged as major players in the domestic technology marketplace.

China's technology development strategy has evolved into a pragmatic and sometimes messy hybrid that incorporates both competing and complementary strands of techno-nationalist and techno-globalist thinking. With these two camps firmly entrenched and wielding extensive influence among policymakers and key state agencies, there are occasional adjustments in technology-related policies to accommodate their different interests.[12] A prime example of such occurred in 2009 when China issued indigenous innovation procurement guidelines requesting that government agencies should only buy technology products containing domestic intellectual property. The move drew strong condemnation from foreign companies and governments, which argued that the policy went against established international norms. The Chinese government eventually retreated from this initiative.[13]

The procurement guidelines controversy reflects a broader effort by China to promote its own homegrown technical standards within the global technology system. The setting of international technical standards has traditionally been in the hands of multinational corporations, but China has raised its profile since the beginning of the twenty-first century, especially in areas such as telecommunications, digital audio and video, computer microprocessors, wireless local area network security, and Internet protocols. The MLP explicitly calls for China to "actively take part in the formulation of international standards and drive the transferring of domestic technological standards to international standards." Richard Suttmeier and Yao Xiangkui argue that China's technical standards strategy should be understood as a modified form of techno-nationalism, in which "technological development in support of national economic and security interests is pursued through leveraging the opportunities presented by globalization for national advantage."[14] How China flexes its growing technological power in this area will offer a good indicator of where the balance between techno-nationalist and techno-globalist impulses lie.

---

[11] Barry Naughton and Adam Segal, "Technology Development in the New Millennium: China in Search of a Workable Model," in William Keller and Richard Samuels (Eds), ***Crisis and Innovation: Asian Technology After the Millennium,*** (New York: Cambridge University Press, 2002), 170−76.

[12] State entities that are most supportive of techno-nationalist approaches include the National Development and Reform Commission, the Ministry of Industry and Information Technology, and People's Liberation Army. Organizations that are more techno-globalist in orientation include the Ministry of Commerce and Ministry of Foreign Affairs.

[13] Loretta Chao, "China's Curbs on Tech Purchases Draw Ire," ***Wall Street Journal***, 11 December 2009; US-China Business Council, "China's Innovation and Government Procurement Policies," May 1, 2013, https://www.uschina.org/sites/default/files/innovation-status-report.pdf.

[14] Richard Suttmeier and Yao Xiangkui, ***China's Post-WTO Technology Policy: Standards, Software, and the Changing Nature of Techno-Nationalism,*** National Bureau of Asian Research Special Report No. 7 (May 2004), 3. See also Christopher S. Gibson, "Technology Standards: New Technical Barriers to Trade?" in Sherrie Bolin (Ed), ***The Standards Edge: The Golden Means*** (Ann Arbor, MI: Bolin Group, 2007).

Hand in glove with techno-nationalism is the concept of indigenous innovation, which is widely referred to in Chinese state plans. What indigenous innovation actually means, however, is far from clear. The term first appeared in the MLP and is defined as a way to promote original innovation, re-assembling existing technologies in different ways to produce new breakthroughs, and the absorption and upgrading of imported technologies. The MLP puts forward three distinct models:

1. **Original innovation (*yuanshi chuangxin,* 原始□新)**: This refers to scientific discovery and technological invention carried out by Chinese research institutions that eventually are successfully developed and commercialized. The meaning of original innovation appears to have expanded in recent years to include an emphasis on breakthrough innovation.

2. **Integrated innovation (*jicheng chuangxin,* 集成□新):** This means the synthesis of related technologies and processes that facilitates the development of competitive products and industries. These technologies and processes can be both foreign and domestic.

3. **IDAR (introduction, digestion, assimilation, re-innovation):** This model is based on the identification, acquisition, and absorption of foreign technologies and processes through a multi-stage sequence of introduction (*yinjin,* 引□*)*, digestion (*xiaohua,* 消化*)*, and assimilation (*xishou,* 吸收) that leads to re-innovated (*zaichuangxin,* 再□新) output. This can be concisely referred to as the IDAR (Introduce, Digest, Assimilate, Re-innovate) strategy and can also be described as advanced imitation. Of these three approaches, IDAR is the most important and relevant to China's current S&T needs.

During Hu Jintao's presidency from 2002 to 2012, indigenous innovation was the main policy focus. In contrast, Xi Jinping's administration has come up with the more market-friendly 'Innovation-Driven Development Strategy' (IDDS) that embraces bottom-up innovation at the same time that it continues to emphasize top-down approaches. Although indigenous innovation as a phrase is now referred to less frequently by senior leaders and in policy documents, its core tenets continue to be the closely observed. While indigenous innovation is not mentioned at all in the 13th Five Year Plan (FYP), the document does reiterate the importance of original innovation, integrated innovation, and re-innovation.[15]

In the pursuit of indigenous innovation and techno-nationalism, the Chinese authorities have devised a set of policy instruments that are being vigorously implemented:

- **Protectionism:** The Chinese authorities view the protection of domestic science, technology, and industrial sectors from foreign competition as essential to ensure they are able to grow and thrive over the long term. Protection can be both direct and indirect in support of specific industries or firms. To avoid falling afoul of contravening international agreements and backlash from foreign firms and governments, Chinese

[15] ***The 13th Five Year Plan for Economic and Social Development of the People's Republic of China (2016-2020),*** http://en.ndrc.gov.cn/newsrelease/201612/P020161207645765233498.pdf

protectionist policies are rarely found in state plans but are often implemented in tandem with them when they are issued.

- **Cultivation of national champions:** An important plank of China's protectionist strategies is the building of domestic national champions. The MLP, Made in China 2025, and FYPs lay out specific industrial sectors that China aims to develop and which companies will receive greater attention from central and local policies. Industry consolidation is a key mechanism used by Chinese authorities to promote national champions so that they can be competitive in global markets. This primarily occurs among state-owned enterprises but is expected to occur in other less state-controlled industries such as additive manufacturing as industries grow and also respond to market forces. This state-backed consolidation has been witnessed many times across almost all of China's high-tech industries.

- **Technology transfers:** A major manifestation of China's efforts to become indigenously innovative is its active promotion of integrating technology from globally leading companies into domestic Chinese companies. The Chinese authorities have increasingly used access to its domestic market to selectively coerce technology companies into transferring technology to local companies. Since the early 2010s, national security concerns have intensified Chinese government demands for access to highly sensitive proprietary information from foreign companies. A key driver was US National Security Agency (NSA) contractor Edward Snowden's revelations of the scale, sophistication, and reach of US technical espionage. The Chinese authorities have drawn up sweeping national security, cybersecurity, and foreign investment laws and regulations that require national security reviews and only permit the use of technology that is "secure and controllable." This means that foreign technology companies are required to provide back-door access to their systems or encryption keys, or even transfer source code.[16]

- **The promotion of Chinese technology standards domestically and internationally:** China's effort to set unique technology standards is an effective trade tool that helps reduce the royalty rates Chinese manufacturers pay to use foreign intellectual property. Various state S&T plans directly encourage development of national standards. The Made in China 2025 plan expresses the need to ensure the important role of enterprises in standards development, and to encourage and support enterprises, research institutes, and industry organizations to participate in international standards development.

3. The Nature and Characteristics of China's Cybersecurity Development

A raft of cybersecurity-related strategies and plans have been released in the past few years that demonstrate a carefully crafted and high priority approach by the Xi Jinping regime to the development of China as a global cybersecurity power. This ranges from the framing of a grand cybersecurity strategy to more specific near, medium, and long-term plans for the development

[16] Paul Mozur, "Jitters in Tech World Over New Chinese Security Law," ***New York Times***, 2 July 2015.

of the cybersecurity industry as well as to the broader expansion of the information domain in China. They include a long-term national informatization development strategy, long-term industrial policies addressing the development of next generation Internet technologies, and infrastructure as well as advanced manufacturing capabilities for critical cyber-related hardware capabilities such as microprocessors and computers.

Xi Jinping offered an outline of an emerging Chinese cyber grand strategy in a speech in December 2015. He pointed out that a key Chinese cyber principle is the importance of a "safe, stable, and prosperous online space" that should not be "the site of a power struggle between all countries, and even more important, should not become a breeding ground for illegal criminal acts". Xi also highlighted the importance of cyber-sovereignty, which meant: 1) respecting each country's right to choose its own Internet development path, its own Internet management model, and its own public policies on the Internet; and 2) Participating on an equal basis in the governance of international cyberspace, which required states to "avoid cyber-hegemony and avoid interference in the internal affairs of other countries", which was an indirect reference to the U.S. and other Western countries.

Another key point in Xi's speech was that China wanted the global Internet governance system to be built on the basis of a "multilateral, democratic and transparent" process. The use of "multilateral" refers to insistence that states should play the dominant role when building the governance system. Besides China, Russia, Iran, and India are also pushing for the adoption of this approach. In contrast, Western countries are pushing for a multi-stakeholder-driven process that would include non-state actors such as international organizations, companies, academics, civil society groups and ordinary Internet users.

Xi's principles were enshrined in China's first national cybersecurity strategy titled the 'National Cyberspace Security Strategy' (NCSS) that was issued in December 2016 by the Cyberspace Administration of China (CAC).[17] The NCSS emphasized the necessity of securing critical infrastructure and the government's right to control cyberspace in Chinese territory. The strategy also pointed out that China's cybersecurity situation was "becoming tougher" with several serious risks and challenges:

- Cyberattacks threaten **economic security** because the Internet and information systems are nerve centers of key infrastructure and economic activities.

- **Political security** being endangered by cyber infiltration that allow countries to meddle into internal affairs of others, incite social unrest, subvert regimes, and allow widespread cyber monitoring.

- **Cultural security** being undermined by unfettered access to the Internet that is allowing harmful information, decadent culture, rumors, and superstitions to impact socialist core values.

[17] Ibid.

- Cyber terrorism and crime threaten **social stability** as the Internet is used by separatist and extremist movements to plot terror activities and by criminal gangs to spread viruses and Trojan horses.

The NCSS also pointed out that global competition for control of cyberspace strategic resources was "just unfolding" and becoming "increasingly fierce." A key goal among competitors is to "seize the right to set rules and gain the strategic high ground and seek the strategic initiative". The NSCC noted that this is causing countries to "strengthen their cyberspace deterrence strategies and intensifying a cyberspace arms race that poses a new challenge to world peace".

China also unveiled its approach in building the global cyberspace governance architecture in March 2017 when the Ministry of Foreign Affairs and the State Internet Information Office jointly issued the 'International Strategy of Cooperation on Cyberspace' (ISCC).[18] The ISCC is a revisionist document that points out that "the existing global governance system of basic Internet resources hardly reflects the desires and interests of the majority of countries". The ISCC states that China's strategic goals for taking part in global cyberspace cooperation are:

1) Safeguarding China's sovereignty, security and development interests in cyberspace
2) Ensuring secure and orderly flow of information on the Internet
3) Improving global connectivity
4) Maintaining peace, security and stability in cyberspace
5) Enhancing international rule of law in cyberspace
6) Promote development of the digital economy

The ISCC puts forward a number of key principles that the Chinese authorities hope will become the key foundations of the new global cyber order:

- **Cyber sovereignty:** "Countries should respect each other's right to choose their own path of cyber development, model of cyber regulation and Internet public policies, and participate in international cyberspace governance on an equal footing. No country should pursue cyber hegemony, interfere in other countries' internal affairs, or engage in cyber activities that undermine other countries' national security".

- **Shared Governance:** China says cyberspace governance should be multilateral in nature with "countries, big or small, strong or weak, rich or poor" being equal members and entitled to equal participation in developing global order and rules.

- **Reforming the Global Internet Governance System:** China wants major reforms that includes beefing up the UN Internet Governance Forum, increasing the independence of the Internet Corporation for Name and Numbers (ICANN), and taking a lead role in new initiatives such as the World Economic Forum's "Future of the Internet".

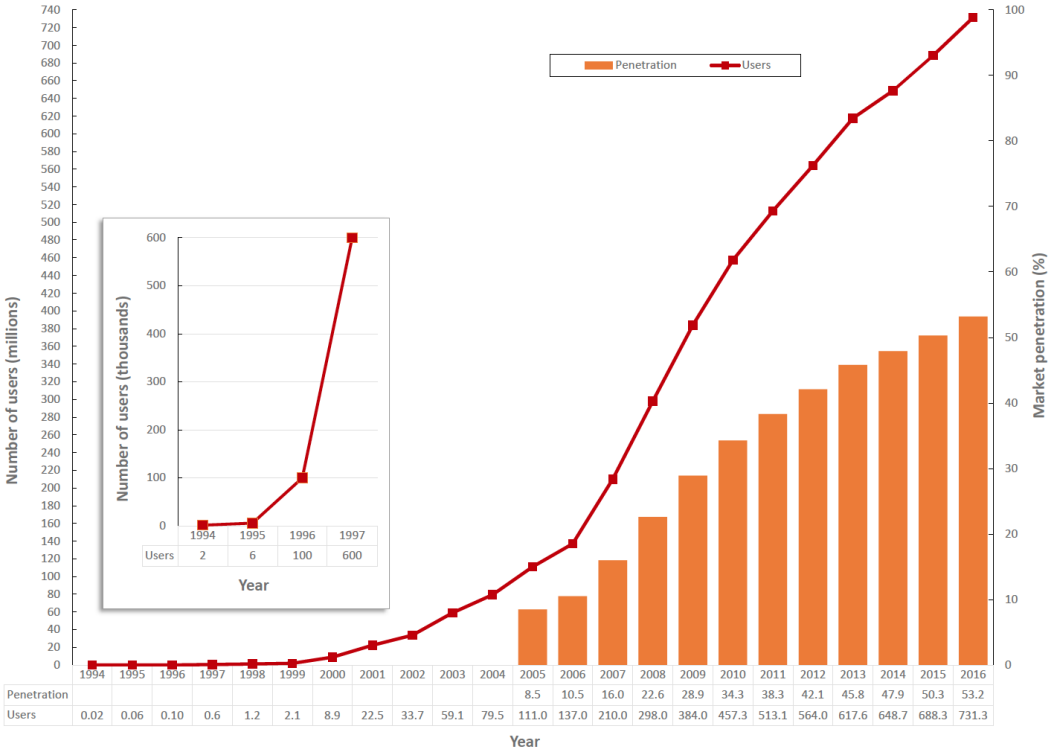
Through Xi's active leadership, China is determined to play a leading role shaping the nature of the global cyber order through the design of the international institutional architecture and setting

[18] Ministry of Foreign Affairs and State Internet Information Office, ***International Strategy of Cooperation on Cyberspace***, 1 March 2017.

guiding norms. While much of the views of Xi and the Chinese leadership are derived from the authoritarian nature of the Chinese political system, the development of the Chinese domestic cybersecurity industry is another important source of influence.

4. The Development of China's Cybersecurity Industry: Market Failures and Government Intervention

China's cybersecurity industry emerged in the late 1990s as the Internet began to gradually take root in the country. The growth of internet users and the penetration rate was slow for the first few years, and only began to significantly take off from the early 2000s. In this first stage of development, official attention and business interest in the internet was subdued, which allowed room for private start-up ventures to take the lead in market development.



	1994	1995	1996	1997	1998	1999	2000	2001	2002	2003	2004	2005	2006	2007	2008	2009	2010	2011	2012	2013	2014	2015	2016
Penetration												8.5	10.5	16.0	22.6	28.9	34.3	38.3	42.1	45.8	47.9	50.3	53.2
Users	0.02	0.06	0.10	0.6	1.2	2.1	8.9	22.5	33.7	59.1	79.5	111.0	137.0	210.0	298.0	384.0	457.3	513.1	564.0	617.6	648.7	688.3	731.3

Growth of China's Internet User Population and Internet Penetration Rate, 1996-2016[19]

[19] Data from Xueping Du, "Internet Adoption and Usage in China", paper for the 27th Annual Telecommunications Policy and Research Conference, 1999, and annual statistical reports on internet development in China by China Internet Network Information Center.

With little regulatory oversight, industry development was chaotic. The main focus for firms was to gain market-share with little near-term regard for profits as consumers, both individual and institutional, were strongly resistant to paying for cybersecurity services. The strategy for many firms in this race to the bottom was to outlive competitors and eventually find ways to monetize their market share.[20] Some of the money-making methods were of questionable legality, such as the selling of customer personal data for profit.[21]

From the early 2000s, as the internet population reached into the tens of millions, the central authorities began to devote more attention to cybersecurity issues as well as to broader information security matters. A cybersecurity regulatory regime began to take root with the issuance of the first generation of detailed guidance and regulations on cybersecurity matters. This included the country's first civilian cybersecurity strategy, released by the State Informatization Leading Group (SILG) in 2003, known as Document No. 27 and titled "Opinions for Strengthening Information Security Assurance Work." The document covered issues such as the establishment of a multi-level protection scheme, compulsory certification, disaster recovery, incident management, e-government security, trusted networks, information security standards, and an information security five year plan.

The mid-2000s marks the beginning of the second phase Chinese cybersecurity industry development as central authorities adopted a more engaged and interventionist role in guiding the country's information economy. The 2006-2020 National Informatization Development Strategy (NIDS), a long-term informatization development strategy, was enacted during this time.[22] The blueprint addressed some of the key market failures of the initial period of the cybersecurity industry's development such over reliance on imports and a lack of investment in developing domestic capabilities, and serious structural vulnerabilities caused by unregulated, ad hoc growth. The strategy called for the establishment of a national multi-tiered information security system that distinguished between the protection of critically important systems and more basic and mainstream networks.

An important goal of NIDS was to foster a more healthy and sustainable market that would attract more established and capable companies from other parts of the information and security sectors. These companies would take part in the improved market and allow the more successful early generation cybersecurity entrants a way to transform themselves into more developed and profitable entities. This goal was pursued by creating a two-tiered market in which one segment would cater to the needs of state, party, and national security agencies that would be willing to pay for specialized and premium services, and the other segment would be the price-sensitive consumer mass market.

---

[20] Zhang Wei: "Opportunities and Challenges in Information Security", ***Liaowang Magazine,*** 16 April 2012, p 48-49.

[21] Li Yuxiao and Xu Lu, "China's Cybersecurity Situation and the Potential for International Cooperation", Jon R. Lindsay, Tai Ming Cheung, and Derek S. Reveron (Eds), ***China and Cybersecurity: in Espionage, Strategy, and Politics in the Digital Domain*** (Oxford: Oxford University Press, 2015), p233.

[22] General Offices of the Chinese Communist Party Central Committee and the State Council, ***2006-2020 National Strategy for Informatization Development***, Xinhua News Agency, 8 May 2006.

This strategy appears to have achieved its intended target as the Chinese cybersecurity corporate apparatus in the mid-2010s is divided into a small elite of around 20 companies that account for 70 percent of the cybersecurity industry's total industrial value. Another 600-700 mostly small firms compete for the remaining 30 percent of the market. The top 20 companies include Beijing TopSec, Beijing Venustech, and Antiy Labs as well as leading telecommunications and IT firms such as Huawei.[23]

China's Top 25 Network Security Companies, 2016[24]

Rank	Company Name	Company Size (employees)	Registered Capital (million Rmb)	Areas of Focus
1	Huawei Technologies □□技□公司	180,000	39,908	Firewall, intrusion detection/prevention, unified threat management, anti-DDoS, VPN, cloud WAF
2	Beijing Venustech Co. 启明星辰信息技□集□股份有限公司	2,000	869	Firewall, network isolation, intrusion detection/prevention, unified threat management, anti-DDoS, database security, data leak prevention, vulnerability scanning
3	Sangfor Technologies 深信服科技有限公司	3,000	360	Firewall, unified threat management, internet behavior management, VPN, mobile terminal security
4	NSFocus Information Technology Co Ltd 北京神州□盟信息安全科技股份有限公司	2,000	364	Firewall, intrusion detection/prevention, unified threat management, host security, anti-DDoS, database security, vulnerability scanning, web application scanning/monitoring
5	Enterprise Security Group 360企□安全			Firewall, network, isolation, terminal detection response EDR, web application scanning/monitoring, cloud WAF, mobile APP security, threat intelligence, security large data analysis (APT), SOC & NGSOC
6	AsiaInfo □信安全	2,000	6,000	Unified security management, host security, terminal protection & anti-virus, data leaks, mobile terminal security, anti-phishing, SOC & NGSOC

[23] Geng Guining and Zhang Xiaoyu, ***"Civil-Military Integration Cybersecurity System Research" (□民融合的网□安全体系研究)***, China Xinan Southern Branch Institute中国信安南方分院, 9 October 2016 http://www.kunlunce.cn/gcjy/zxzz11111111/2016-10-09/108544.html

[24] Rankings and areas of focus from AQNiu.com: ***中国网□安全企□50□（2016年上半年）*** [China's 50 Top Network Security Enterprises (First Half of 2016)], AQNiu.com, 21 June 2016, http://www.aqniu.com/industry/16978.html). Employee size and registered capital from company websites, baidu.com (company-specific articles), and online financial sources.

7	Westone Information Industry □士通信息□□股份有限公司		432	Firewall, intrusion detection/prevention, VPN, data encryption, document security, encryption machine
8	Beijing TopSec Co. 北京天融信科技有限公司	2,000	75	Firewall, network isolation, intrusion detection/prevention, internet behavior management, VPN
9	H3C 杭州□三通信技□有限公司	5,000	550	Firewall, intrusion detection/prevention, unified threat management, VPN
10	DBAPPSecurity 杭州安恒信息技□有限公司		50	Database security, web application scanning and monitoring, web application firewall, large data analysis, level protection tools
11	Meiya Pico 厦□市美□柏科信息股份有限公司	900	487	Security forensics and public opinion monitoring
12	Hillstone Networks 山石网科通信技□有限公司	600	124	Firewall, intrusion detection/intrusion prevention, VPN, web application firewall
12	Beijing VRV Software 北信源□件股份有限公司		270	Network access control, terminal protection, anti-virus, data leak protection, mobile terminal security
14	Knownsec 北京知道□宇信息技□有限公司	600	61	Web application scanning/monitoring, cloud defense, cloud WAF, large data analysis
15	Antiy Labs 安天□□室		3	Terminal protection & anti-virus, threat intelligence, secure big data analysis (APT)
15	Bangcle 梆梆安全			Mobile APP security, mobile business security
17	PayEgis 江□通付盾信息科技有限公司		50	Cloud authentication, mobile APP security, anti-fraud
18	Eversec (Beijing) Technology 恒安嘉新（北京）科技有限公司	500	75	Mobile network security, large data analysis
19	Feitian Technologies 北京□天□信科技有限公司		418	Identity authentication, USB key and other equipment
20	Beijing NetentSec 北京网康科技有限公司	1,000	100	Firewall, internet behavior management, web application firewall, large data analysis

21	Bluedon Information Security Technologies □盾信息安全技□股份有限公司		1,175	Firewall, intrusion detection/prevention, security integration services
22	Beijing Lanxum Technology 北京立思辰科技股份有限公司		684	Encryption machine, industrial security
23	Beijing Kuangen Network Technology 北京匡恩网□科技有限□任公司		105	Industrial security
24	Tongdun 杭州同盾科技有限公司		50	Anti-fraud
25	Hangzhou DPtech Technologies 杭州迪普科技有限公司		360	Firewall, unified threat management, intrusion detection/prevention

However, NIDS did not address all market failures. One of the biggest structural problems of the cybersecurity and information security sectors was their fragmentation among fiercely competing state and national security bureaucracies. This was commonly known as the phenomenon of the "nine dragons controlling the water" (九□控水) that referred to the proliferation of government and security institutions each with a voice in the making and oversight of cybersecurity policy.

Coordination among these powerful and independently-minded bureaucracies was primarily undertaken during the 2000s through a National Network and Information Security Coordination Small Group (NNISCSG) that was subordinate to the SILG. All of these entities had a representative on the NNISCSG, which was chaired by a vice-premier. The NNISCSG was disbanded in 2008, briefly re-established in 2009, and then was not heard of again until the establishment of the Party Central Cybersecurity and Informatization Leading Group (CCILG - 中央网□安全和信息化□□小□) under the chairmanship of Xi Jinping in 2013. The CCILG was elevated into a commission in March 2018 as part of a broader effort to increase the authority of party institutions in the overall policy making and implementation apparatus. It is now known as the Central Cyberspace Affairs Commission (中央网□安全和信息化委□会 - CCAC).

One of the consequences of this fragmentation was that competing bureaucracies had control of different portions of the information security and cybersecurity sectors and this encouraged them and their affiliated firms to engage in rent seeking and protectionist behavior. The security agencies, for example, run their own certification schemes that allows them to control product access for areas under their jurisdiction. Another example is how only the State Encryption Bureau has the authority to set encryption standards and requirements.

5. National Security Rationales for State Intervention

While addressing market failures is important for the authorities, the overriding drivers for state intervention are dominated by national security and related techno-nationalist concerns.[25] This is evident in Chinese authorities' assessment of the global cybersecurity environment, which provides the underlying strategic context and logic to determine policy responses. China's national cybersecurity strategy that was issued in December 2016 pointed out that "the country's political, economic, cultural, social, national defense and citizens' legal rights in cyberspace are faced with serious risks and tough challenges", and specifically pointed to the following concerns:[26]

- **Political stability is being undermined by cyber infiltration from abroad:** The Chinese authorities see unnamed outside powers, including state and non-state actors, as engaging in activities such as "meddling into the internal affairs of other countries, attacking other countries' political systems, inciting social unrest, subverting other countries' regimes, large-scale cyber monitoring, and cyber theft" that threatens political security.

- **Economic security threatened by cyberattacks:** The strategy points out that Internet and information systems have become the infrastructure nerve centers for the country's economy and efforts to attack and sabotage them would lead to paralysis and catastrophic outcomes for the country's financial, transportation, and energy sectors.

- **Cultural security undermined by 'harmful' content:** The Chinese authorities have become extremely worried by what they see as the rise of 'harmful information' such as internet rumors, "decadent" culture, obscene content, and "superstitious beliefs that run counter to socialist core values" that is corroding the "mental health of younger generations, corrupting social values, and misleading values" that endangers overall cultural security.

- **Social stability being destroyed by cyber terrorism and cybercrime:** Terrorism-related activities, including separatist and extremist-related, are taking place online and represents a major danger to China's social order. In addition, computer viruses, Trojan horses, fraud, hacking, and other illegal criminal activities is intensifying and undermining social stability.

- **Cybersecurity international competition is in its early stages but growing rapidly:** The document paints a picture that cybersecurity competition among major cyber powers is becoming increasingly fierce as they all seek to gain the strategic initiative. This is

[25] National security considerations fall into three general baskets for the Chinese authorities: external threats from state actors engaged in activities such as cyber-espionage and hacking attacks; monitoring and control of domestic activities; and cybercrime.

[26] Cyberspace Administration of China, ***National Cyberspace Security Strategy***, (Beijing, 27 December 2016).

leading to an intensifying cyber arms race and the need for China to build up its cyber deterrence capabilities.

Although the Chinese authorities, especially the security apparatus, have been extremely wary and vigilant of the foreign cybersecurity threat from the earliest days of the country's internet connection, a defining shock was the Snowden revelations in 2014. His disclosures showed that the NSA's ability to compromise the security and integrity of the global information technology economy was far greater than was generally believed. Moreover, China was one of the NSA's top priorities for infiltration. Among the chief targets were the Chinese leadership, the PLA, defense industry, trade-related agencies such as the Ministry of Commerce, banks, and telecommunications companies. One especially prominent target was Huawei, the country's leading network equipment supplier. One of the reasons for focusing on Huawei were that many of the targets the NSA was going after used Huawei products; the company also supplied the Chinese authorities with the signals intelligence capabilities needed to engage in electronic and cyber intelligence activities.[27]

The Chinese government's response to the Snowden revelations was to urgently step up efforts to reduce reliance on imports of information technology products and to develop their own indigenous capabilities. This is reflected in a revised version of the NIDS that was issued in 2016 which provided a new, adjusted outline for the development of the country's information economy into the mid-2020s. On cybersecurity matters, the NIDS points out that cybersecurity is an integral component of informatization: "Cybersecurity and informatization are two wings of one body, two wheels of one cart, they must be planned together, arranged together, moved forward together and implemented together."

6. Key Actors and Coalitions in the Making of China's Cybersecurity Industry

The Chinese cybersecurity domain is crowded with multiple privileged actors and coalitions competing for their voices to be heard and their interests to be counted. There are six major constituencies. The first is the **Communist Party,** which sits at the top of the cybersecurity oversight system through the CCAC. Party officials have a significant presence on this body. Xi Jinping is the chair, while Premier Li Keqiang and Politburo Standing Committee member Wang Huning are deputy chairs. The CCAC's general office is headed by Xu Lin, who is also the director of the Cyberspace Administration of China and a deputy head of the Party Propaganda Department, which is the main Party organ engaged in cyber-related matters. The head of the Propaganda Department, Huang Kunming, is a member of the CCAC as are several other senior Party officials such as Politburo Standing Committee members Li Zhanshu and Wang Yang.

[27] "NSA Spied on Chinese Government and Networking Firm Huawei", ***Spiegel Online,*** 22 March 2014, http://www.spiegel.de/international/world/nsa-spied-on-chinese-government-and-networking-firm-huawei-a-960199.html

The second major actor is the government. The State Council is the nominal body in charge of government-related cybersecurity matters and the premier serves as a deputy head of the Party's Cybersecurity and Informatization Leading Group, but daily management comes from the Cyberspace Administration of China (CAC). The Ministry of Industry and Information Technology also plays an important role in cybersecurity and information security-related issues and has an information security coordination department to oversee these activities. In addition, the Ministry of Science and Technology is responsible for overseeing IT security and cybersecurity basic research and development projects. One of the most important of these projects was a new cybersecurity key project launched in 2016 aiming to concentrate resources to address many key technical challenges.[28] Other state entities with sizeable cyber responsibilities include the Ministry of Industry and Information Technology and the National Development and Reform Commission.

A third powerful constituency is the **People's Liberation Army,** which has an extensive cybersecurity apparatus that wields significant influence on cybersecurity issues. There is a PLA Cybersecurity and Informatization leading group that acts as a coordinating body, while operational management resides in the Strategic Support Force that has emerged since major organizational reforms to become the principal PLA command for cyber-related entities, Central Military Commission Joint Staff Department, and the various service arms and five regional theater commands.

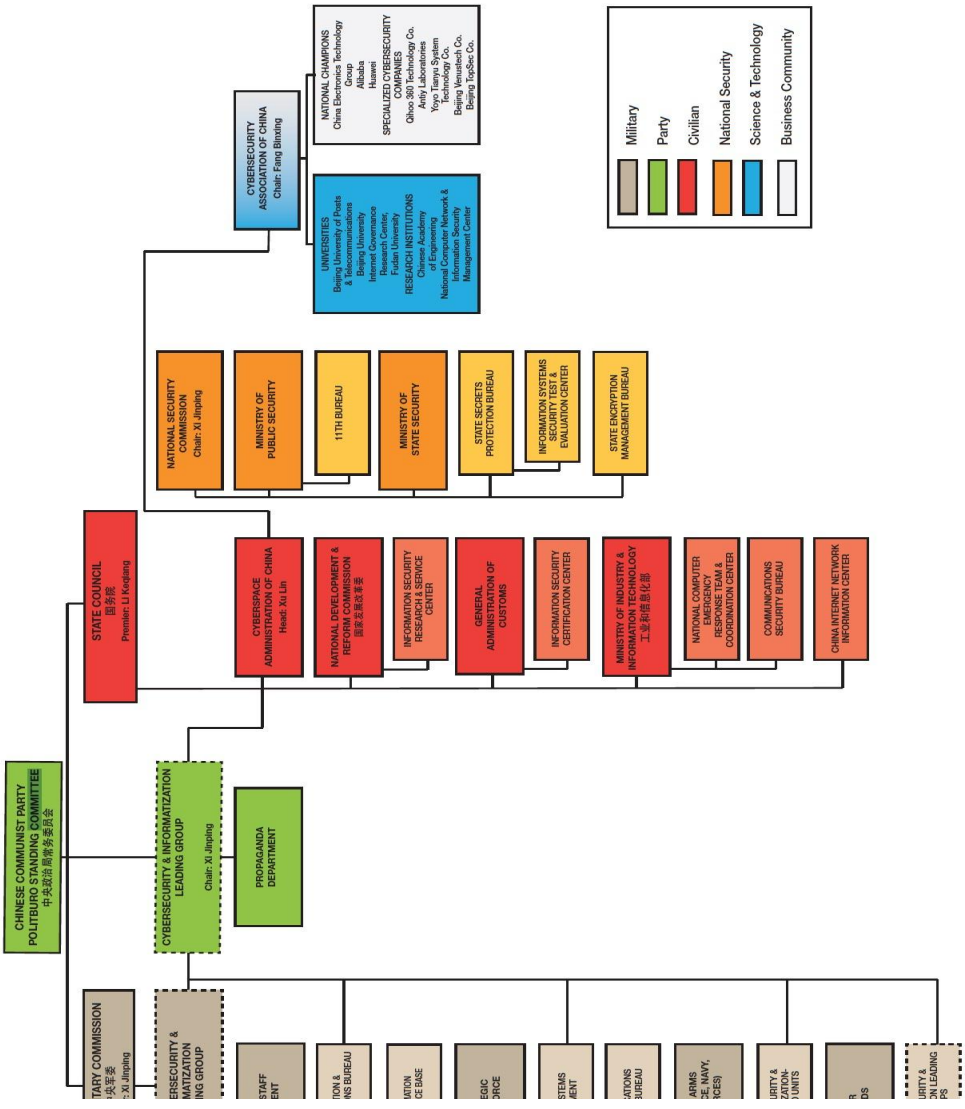
A fourth key player is the **national security system**, which is a highly compartmentalized apparatus consisting of many independent and competing bureaucratic fiefdoms. They include: 1) the Ministry of Public Security which is responsible for cybercrime and critical infrastructure protection and has a national network of research laboratories; 2) the Ministry of State Security that is the country's chief intelligence and counter-intelligence agency, which maintains a low profile but has considerable technical cybersecurity expertise, especially in information assurance; 3) the State Secrecy Bureau, also known as the Party Secretariat Secrets Protection Office, that manages all classified official networks; 4) the Certification and Accreditation Administration; and 5) the State Encryption Bureau, also known as the Party Central Office Confidential Bureau and Central Cryptography Commission, which is responsible for party, military, and civilian encryption management.

A fifth and much weaker constituency is the **academic research and development system**, which is an up and coming actor in the cybersecurity domain and its rapid rise in importance has been highlighted by Xi Jinping's call for the cybersecurity system to pursue indigenous innovation and pursue disruptive and breakthrough research and development. There is a modest but rapidly growing cybersecurity research and development community that includes universities such as Beijing University of Posts and Telecommunications and research institutions such as the Chinese Academy of Engineering.

Lastly, there is the **domestic corporate constituency** that is a highly decentralized constituency with few mechanisms for organization and coordination for its diverse set of corporate actors. In

[28] ***Cybersecurity Key Project 2017 Project Application Guide*** ("网□空□安全"重点□□2017 年度□目申□指南), Ministry of Science and Technology, October 2016, http://www.most.gov.cn/mostinfo/xinxifenlei/fgzc/gfxwj/gfxwj2016/201610/W020161013492765312410.pdf.

an attempt to promote more effective industry coordination, the Cybersecurity Association of China was established in 2016 with more than 250 entities becoming members.
There are additional actors and coalitions that seek to have a presence in the policy deliberations and representation on key bodies, but lack the clout and standing to be included. These include local actors such as provinces as well as foreign entities such as the foreign business community and foreign governments. Moreover, the vast community of more than 730 million Chinese Internet users have no representation or the means to organize themselves to gain access into the policy process.



The Six Major Constituencies in the Chinese Cybersecurity System, 2018

Several important features define the configuration of power arrangements within the cybersecurity domain that determine the relative power, influence, and alignment of these actors and constituencies. First, the cybersecurity system has only been in existence since the early 1990s so its institutional development is still in the making. The leadership arrangements overseeing the cybersecurity system has undergone regular reorganization, of which the most recent was the establishment of the CCSILG under Xi's command. A number of other key leading cyber management bodies such as the CAC have short institutional histories. This late institutionalization means that power and authority is often derived from personalities rather than organizations.

Second, the Chinese bureaucratic system is fiercely competitive, predatory, and compartmentalized which can be problematic for the development of newly emerging institutions such as the cybersecurity apparatus. These fledgling institutions are often subject to battles for control from dueling bureaucracies, especially if there are lucrative rents that can be extracted. The cybersecurity system is widely viewed within the Chinese system as a golden goose. Resulting turf wars are fierce and can lead to stunted or incomplete institutional development, especially of governance norms and mechanisms.

Third, as the cybersecurity industry is a strategic sector, the military and national security constituencies have far more influence and authority than their state and corporate counterparts. While the Party stands on top of the organizational hierarchy, its main role is to coordinate and set strategic guidance and principles, although the Party's Propaganda Department is active in areas such as information management. Operational matters will tend to be in the hands of the state, national security and military authorities.

The role and influence of the corporate coalition is one of the weakest of the six constituencies. They have no representation in the CCAC and the main organization that represents them, the Cybersecurity Association of China, was only created in 2016, and so is a newcomer in a fiercely competitive apparatus.[29] Moreover, there appears to be little cohesion and coordination among the country's cybersecurity companies. As already pointed out, the corporate cybersecurity sector has two distinct tiers of firms. There is a small elite of national champions, such as Huawei and Alibaba, who are primarily information technology or Internet commerce companies who have devoted a small proportion of their overall operations to expanding cybersecurity-related services. The heads of these firms are often picked by the authorities to be the designated representatives of the cybersecurity industry. Also in this elite tier are a small handful of the most successful specialized cybersecurity outfits, such as Qihoo and Topsec, who have established close, trusted ties with the state. The second general tier is comprised of the overwhelming bulk of small and medium-sized privately owned outfits (See appendix) This segmentation of the corporate constituency makes it unlikely that their influence in policy making and regulatory affairs will grow for the foreseeable future.

Another feature of the Chinese cybersecurity sector is its lack of transparency, which makes it difficult to have a clear understanding of the precise nature of the relationship between the

[29] "Father of China's Great Firewall to Lead New Cybersecurity Association", ***South China Morning Post***, 26 March 2016.

different sets of actors involved, and especially between state (Party, government, military, and security entities) and firms.

7. State-Corporate Cybersecurity Engagement

Elements of the five modes of state-corporate cybersecurity interactions that Aggarwal and Reddie put forward in their paper[30] can also be found in the China case, although with significant variations because of different political, economic, and security circumstances. There are four prominent types of relationships between the Chinese state and cybersecurity industry. The first is the **pocurement and licensing model**, which the **state acts as a customer.** The Chinese authorities have made considerable progress over the past two decades in establishing a robust public procurement system based on international best practices. However, difficult structural and normative obstacles, such as poor transparency and corruption, still remain to be overcome. The cybersecurity-related procurement system is subject to special national security considerations that allows state agencies wide-ranging discretion over its procurement practices. Regulations adopted in June 2017 require the procurement of "important network products and services" to go through a security review by security agencies before approval is given.[31] With deepening worries over foreign cybersecurity intrusions, there is intensive pressure from the national security apparatus that only highly trusted domestic firms should be awarded contracts.

A second state-cyber industry mode is the **hiring of technological talent into the government, military, and security apparatuses.** The rapid expansion of the Chinese technology-security complex means there is a huge demand from state, military, and security agencies for civilian talent. Moreover, there is an urgent push to forge an integrated civilian-military-security economy, of which cybersecurity is an important component. Xi Jinping has made civil-military integration (CMI) a high priority since the mid-2010s, demonstrated by the establishment of a high-level Central Commission for Integrated Civilian-Military Development in January 2017, which he heads[32] as well as the elevation of CMI into a national-level development strategy in 2015. Xi has urged the cybersecurity and information technology sectors to vigorously promote CMI while offering ample potential for civil-military coordination. As an article in the Liberation Army Daily, the mouthpiece of the Chinese military, pointed out in discussing how military and civilian players fit into the development of the cybersecurity industry, "give play to the role of the scientific research academies and institutes in the military as the vanguard and the role of civilian manufacturers, academics, and research institutes as the mainstay."[33]

---

[30] Vinod Aggarwal and Andrew Reddie, "Comparative Industrial Policy and Cybersecurity: A Framework for Analysis and the U.S. Case".

[31] This regulation is called "Measures on the Security Review of Network Products and Services". See "China Releases Final Regulation on Cybersecurity Review of Network Products and Services", ***Covington and Burling LLP***, 2 May 2017, https://www.insideprivacy.com/international/china/china-releases-final-regulation-on-cybersecurity-review-of-network-products-and-services/

[32] See Zhu Qichao, ""Build Impregnable Cyber Security on the Basis of Civil-Military Integration", ***National Defense Reference*** (***Guofang Cankao)*** No.8, June 2017; and "PLA Plans In-depth Development of Civil-Military Integration in Cyber Information Realm", ***Liberation Army Daily,*** 15 December 2016.

[33] Cheng Xiangran, "Civil-Military Integration in Building the National Cyberspace Defense System", ***Liberation Army Daily***, 3 April 2018.

A third category of the state-corporate cyber relationship is the direct regulatory power of the state. The Chinese authorities have significantly built up their cybersecurity regulatory regime over the past few years, of which the highlight was the 2017 Cybersecurity Law. These regulatory powers are broad, vague, and increasingly intrusive and have caused considerable consternation from foreign firms. International firms have shown concern over onerous requirements such as the need to store data within China, the need to go through hardware and software reviews for information technology firms, and restrictions on cross-border data transfers.

A fourth type of state-cyber industry relationship is the 'government as venture capital' model**.** Chinese state agencies, whether directly or through intermediaries, have become active in investing in technology-related commercial ventures at home and abroad since the early 2010s, especially in areas where there is civil-military dual use potential. For the cybersecurity sector, one of the first reported ventures took place in February 2016 when the China Internet Development Foundation, which is affiliated with CAC, established a modest Rmb 300 million (US$46 million) cyber security investment fund.

The central authorities significantly stepped up their interventionist approach in the financial domain in March 2018 when the CAC and the China Securities Regulatory Commission issued a joint policy guidance document to promote the role of "capital markets to serve the building of China into a strong cyber country".[34] This guidance, which will be followed by detailed regulations, is intended to "give full play to the capital markets" to support and accelerate the development of "cybersecurity and informationization" companies", especially so that they can "chose development paths that center on the goals of building China into a strong cyber country". One of these central goals is to cultivate the indigenous research and development of homegrown cybersecurity and information technologies. This initiative is intended to allow leading private cybersecurity firms the opportunity to list on domestic stock markets, to gain access to investment funding to help with their development, and to increase the influence of the party-state over these firms. In a keynote speech at a national cybersecurity and informatization conference in March 2018, Xi stressed the need for "centralized, unified leadership of the Party over cybersecurity and informatization."[35]

Concluding Thoughts: China and the International Cybersecurity Order: Cooperation or Competition?

The rise of a Chinese state that is increasingly technologically capable and obsessed with national security, of which the cybersecurity industry is a core component, has profound

---

[34] Office of the Central Cyberspace Affairs Commission and China Securities Regulatory Commission, ***"Guiding Opinions on Promoting Capital Markets to Serve the Strategy of Building China Into a Strong Cyber Country",*** Beijing, 30 March 2018. See also Lorand Laskai, Paul Triolo, Xiaomeng Lu, and Samm Sacks, ***"Unleashing China's Capital Markets to Build a Cyber Superpower"***, New America, 17 April 2018, https://www.newamerica.org/cybersecurity-initiative/digichina/blog/unleashing-chinas-capital-markets-build-cyber-superpower/

[35] "Xi Outlines Blueprint to Develop China's Strength in Cyberspace", ***Xinhua News Agency***, 21 April 2018.

international geo-political and geo-economic complications. First, Xi Jinping has sought to carve out a greater role for China on the world stage, which includes seeking to revise disagreeable norms and rules. This has been most visibly demonstrated in areas such as the South China Sea in which China has built man-made islands and used them as a platform to expand its sovereignty claims. In the cyber domain, China has been undertaking a campaign to define key foundations of the new global cyber order that puts it in direct competition with its Western counterparts. Key norms that the Chinese are advocating includes its definition of cyber sovereignty and shared governance. The Chinese authorities are actively lobbying foreign governments, hosting international conferences, and engaging in a concerted diplomatic offensive to win the support of developing countries and authoritarian regimes for its cause. The overarching goal for China is to become one of the leading global powers in defining and shaping the future international cyber order in terms of norms, governance, and organizational structure.

Second, as China looks to lay down the long-term foundations of its cybersecurity industry, one of its goals is to make the domestic cybersecurity sector a major exporter of its products and services. Chinese firms have already become leading global players in the sale of information technology hardware such as networks and switches, and they are looking to also become a major presence in the global internet arena. Firms such as Alibaba, Tencent, and Baidu are targeting foreign expansion as a top priority after becoming dominant players in the domestic internet market.[36] While there is considerable concern in advanced Western countries for allowing Chinese companies to provide information security-related products and services, there appears to be less reluctance in developing countries, especially if China is offering to provide critical infrastructure and networks at discount prices along with attractive financial assistance.

Third, as China finds itself engaged in intensifying strategic competition with the U.S., the cyber domain will be one of the principal arenas of contest. Much of this rivalry is already taking place in cyber espionage, but it is also beginning to spill over into other related technology areas. China's cybersecurity law, for example, is causing serious concern among a wide array of companies including those involved in supporting critical information infrastructure as well as firms in the energy, transportation, financial, and other sectors that collect personal information data in China. Moreover, highly promising emerging industries such as cloud computing and artificial intelligence could also become entangled in this strategic competition.

There are tentative glimmers of hope that the U.S. and China can mitigate this strategic competition in cyberspace by building channels of cybersecurity cooperation through dialogue and joint action in areas where their interests align. When tensions were soaring between the U.S. and China over an intensifying cyber espionage campaign that each country was apparently waging against the other, the presidents of the two countries signed an agreement in September 2015 promising not to engage in commercial cyber theft, although nothing was addressed about state-orchestrated intelligence operations. Despite widespread skepticism that the agreement would be effectively enforced, the evidence a year later showed a marked reduction in Chinese cyber activities to steal U.S. intellectual property and other commercial violations.[37] Moreover,

---

[36] "China's Internet Giants Go Global", ***The Economist Magazine***, 20 April 2017.

[37] Adam Segal, "The U.S.-China Cyber Espionage Deal One Year Later", Council on Foreign Relations, 28 September 2016, https://www.cfr.org/blog/us-china-cyber-espionage-deal-one-year-later; and FireEye, ***Redline***

the U.S. and Chinese governments have established an annual high-level dialogue between law enforcement and domestic security tsars since the mid-2010s on cyber-crime-related matters. Besides the U.S., China has also conducted similar cybersecurity cooperative exchanges with other countries and international institutions such as the United Kingdom and the G-20. But these seeds of cooperation exist in a hostile environment of deepening distrust, intensifying official cyber espionage activities, and a broader increasingly adversarial strategic rivalry, so their overall impact is likely to be marginal.

Drawn: China Recalculates Its Use of Cyber Espionage (June 2016), https://www.fireeye.com/content/dam/fireeye-www/current-threats/pdfs/rpt-china-espionage.pdf