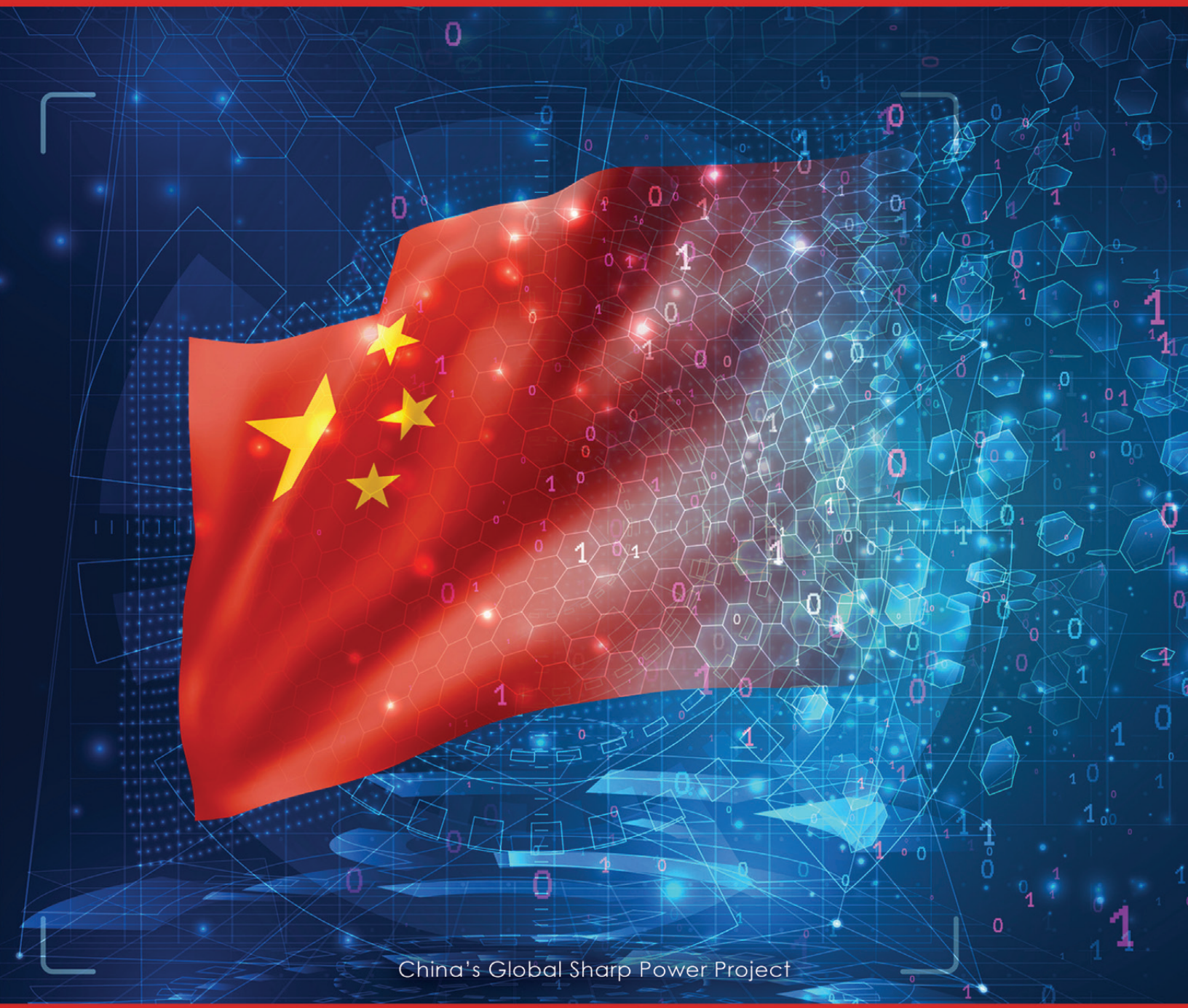
CGSP OCCASIONAL PAPER SERIES NO. 2 • APRIL 2023

CHINA'S GRAND STRATEGY FOR GLOBAL DATA DOMINANCE

By Matthew Johnson

EDITORS: Larry Diamond, Glenn Tiffert, and Frances Hisgen



China's Global Sharp Power Project

A PUBLICATION OF THE HOOVER INSTITUTION

This report is the latest in a series of collaborative ventures the Hoover Institution has undertaken with the Asia Society's Center on U.S.-China Relations.

CHINA'S GLOBAL SHARP POWER

China's Grand Strategy for Global Data Dominance

Matthew Johnson

Executive Summary

The United States and China are engaged in a global contest to shape how digitized information—data—will be distributed and controlled for the foreseeable future. For the Biden administration, the contours of this contest are only just becoming visible. While officials have addressed the importance of data in US-China competition, there is not yet a clear set of laws and policies that would support a strategy of protecting Americans' data from our biggest global rival. The opposite is true in Beijing, where Xi Jinping's Party-state is building a massive institutional architecture to draw more and more of the world's data resources toward China.

This report, based on the Chinese Communist Party's own documents, dissects how the CCP has created a policy and regulatory architecture to maximally exploit data as the fundamental resource of the future global economy and governance system. It illustrates how People's Republic of China (PRC) technology companies that are now omnipresent in foreign markets are increasingly integrated with the Party's data storage and processing—and control and security—systems. This embedding potentially exposes huge swaths of the world's population to a broad spectrum of data accumulation, espionage, and manipulation.

- Under Beijing's new data hierarchy, all companies are forced to integrate into a centralized national data infrastructure controlled by the Party, structured to serve Party objectives in strategic competition with the West, and based on the fundamentally nonreciprocal premise that **China maximizes the absorption of data from around the world while exporting as little of its own as possible**.

- The logic of China's interlocking data-security laws and the ubiquitous nature of China's surveillance systems means that **all customer data held by China-controlled companies will be potentially visible and accessible to China's security services**.

A Hoover Institution Essay

- Party-state requisitioning of data from commercial handlers is **already being used** to
  - build databases of individual human genomes;
  - map sensitive areas of other countries' economies and borders;
  - mine telecommunications networks for commercial secrets and intelligence;
  - manipulate the online information environment;
  - profile foreign citizens through social media; and
  - target journalists who critically cover China and PRC companies.

This challenge requires an urgent response by the United States and other democracies. To that end, this report makes the following policy recommendations:

- Restructure the Commerce Department's Information and Communications Technology and Services (ICTS) process to **block commercial operations that threaten the security of critical and personal data**.
- Reinvigorate the Committee on Foreign Investment in the United States (CFIUS) and update the Foreign Investment Risk Review Modernization Act (FIRRMA) to **restrict the ability of China-linked companies within the United States to operate in critical supply chain areas**.
- Join multilateral **frameworks for coordinating and strengthening data protections and scrutinize China's efforts to hollow emerging global digital trade standards**.
- **Pressure Beijing to agree to reciprocity** by limiting US companies from investing in PRC companies engaged in data exfiltration and abuse and supporting corporations seeking to relocate operations from China.

• • •

The United States and China are engaged in a global contest to shape how digitized information—data—will be distributed and controlled for the foreseeable future.

For the Biden administration, the contours of this contest are only just becoming visible. While officials have addressed the importance of data in US-China competition, there is not yet a clear set of laws and policies that would support a strategy of protecting Americans' data from our biggest global rival.[1] The opposite is true in Beijing, where Xi Jinping's Party-state is building a massive institutional architecture to draw more and more of the world's data resources toward China.

Xi has identified data as the single most important resource—and vulnerability—in what he describes as the existential struggle between China's political system and that of the West. Close analysis of his speeches shows a personal preoccupation with controlling data and the "critical core technologies" needed to store, process, and leverage it.[2] Now, as he begins his third term as China's paramount leader, Xi seeks to extend the control he has established over China's society and internet into the global digital domain.

This report highlights an opaque and intensifying aspect of Xi's data-dominance strategy—the role of commercial actors in creating the hardware and organizational linkages through which increasingly large pools of offshore data will be routed back to Beijing. Under Xi, the Party doesn't intend to simply steal from the world's largest and most strategically important information markets. Rather, it is building an operating environment and a commercial architecture designed to exploit openness, build nonreciprocal pipelines of access, and co-opt other countries into voluntarily exposing their data assets to the maximum extent, potentially exposing huge swaths of the world's population to a broad spectrum of data accumulation, espionage, and manipulation. People's Republic of China (PRC) technology companies that are now omnipresent in foreign markets are increasingly integrated with the Party's data storage and processing—and control and security—systems. Through China-controlled data platforms, apps, and companies, users are entering an entire ecosystem designed to facilitate a sustained campaign of espionage and other forms of data and technology transfer, while making it difficult to leave.

The report begins with an overview of the goals of the Party's accumulation-espionage ecosystem and then turns to a series of case studies that underscore the risks associated with the data-related operations of PRC companies in the United States. Following the case studies, it details the architecture of the system: how Xi's direction that data in all its forms should be controlled, accumulated, and exploited to serve the strategic interests of the Party-state has been translated into new laws, regulatory mechanisms, and enforcement options. It will conclude with a series of policy recommendations proposing solutions to the most urgent threats that China's digital grand strategy poses to the United States.

1. THE ACCUMULATION-ESPIONAGE ECOSYSTEM

An emphasis on security (national security, cybersecurity, etc.) has been a mainstay of Xi's data strategy. Throughout his first decade in power, Xi has repeatedly emphasized the importance of not just mitigating but preventing political instability through technology, including tools of systemic and top-down surveillance. In 2013, in the early months of his reign, Xi began to speak of data in the way Mao had spoken of indigenous oil production in the 1950s, when seeking to break reliance on the Soviet Union. Xi told the Chinese Academy of Sciences:

> The vast ocean of data, just like oil resources during industrialization, contains immense productive power and opportunities. Whoever controls big data technologies will control the resources and initiative for development.[3]

In 2014, Xi described information as a "factor of production," a category traditionally reserved for labor, land, capital, and technology.[4] In 2016, he began calling for the "deep integration of information resources."[5] Stressing that China should seek to become a network "great power" by ramping up capacity and proficiency in mastering digital infrastructure, he said: "We must . . . use data centralization and sharing as an approach [and] build nationally integrated national big data centers and promote technological integration, business integration, and data integration."[6]

Xi's data vision began to bear substantial fruit in 2015, when the General Office of the State Council issued a document innocuously titled "Several Opinions on Using Big Data to Strengthen Service and Supervision of Market Entities." Its key recommendations included using big data to enhance government supervision and control, including accelerating construction of a "social credit system" to regulate individual behavior.[7] That same year, the State Council issued an "action framework" initiating planning of a unified national big data infrastructure.[8] In 2016, Xi instructed China's intelligence and security agencies to adopt "an all-weather omnidirectional sensing cybersecurity posture."[9] Further measures extended Beijing's data-control powers over the most sensitive forms of data. These include encryption keys, as codified by the Encryption Law of 2020, and also include cyber vulnerability data, as codified by Data Security Law (DSL) of 2021's demand that network managers not only report all discovered cyber vulnerabilities to China's authorities, but also refrain from reporting any such data to foreign entities.[10] The blueprint for Party control over data processing and infrastructure extends information control downward to the more finely calibrated level of individuals and corporations.

Now Xi is attempting to move the entirety of China's data-control regime into the global domain. The 20th Party Congress, held in October 2022, has signaled the beginning of a new phase in his ambitions by enshrining "struggle"—a Maoist code word for internal purges and international confrontation—alongside "reform and opening" as the guiding principle of the revised Party Charter. This has major ramifications. Beijing's focus will now be even more on confronting perceived enemies at home and abroad, and even less on economic growth. In an official *People's Daily* interpretation of Xi's vision of "New Great Struggle" by Han Qingxiang, a lecturer at the Central Party School, Xi's personal vision of struggle is said to entail resource competition, currency war, market competition, ideological struggle, territorial disputes, anticorruption struggle, struggle in cyberspace, and struggle against separatism. Han said the "targets and forms of the struggle are diverse and 'battlefields' of struggle may be everywhere." He added:

> The targets of our ongoing "New Great Struggle" are both foreign and domestic, both outside and inside the Party, [and] they can be economic and political, cultural and social. They include visible hostile forces as well as invisible challenges, tests and dangers. There are struggles in all fields—economy, politics, culture, and society. Resources, currencies, markets, ideology, the internet, are all carriers of struggle.[11]

Likewise, in the run-up to his 20th Party Congress work report, Xi foreshadowed that the Party would struggle—that is, harden itself—to win strategic initiative globally amidst stormy and turbulent times:

> Our Party relies on struggle to create history, and even more must rely on struggle to win the future. On the new journey, the risks and tests we will face will be even more complex, to the point of encountering unimaginably stormy seas. The various struggles we face are not short-term but long-term, and will accompany the entire process of reaching the "second century of striving" goals [a reference to China becoming a more modernized and powerful socialist country]. In the face of major risks and strong opponents, to always want to live in peace and never want struggle is unrealistic. To contract "soft-bone disease" or "phobias" will be of no avail.[12]

The language and personnel moves—three of Xi's most economically literate Politburo colleagues were replaced by a phalanx of personal loyalists—revealed at the 20th Party Congress in late 2022 all indicate that Xi is hardening the Party to take on the outside world.

Data and technology are critical elements in Xi's "New Great Struggle." Data is the key ingredient in enabling the Chinese Communist Party (CCP) and government of the PRC (together, Party-state) to drive efficiency in economic productivity, governance, and social control. "If oil is the core resource in the era of industrial economy, then data is the most important strategic resource in the era of digital economy," according to the PRC State Information Center in March 2020.[13] Xi's drive to ensure all China-related data is controlled by the Party-state is reflected in new regulatory structures, new policy and political campaigns, and a matrix of new laws that are now being pushed across multiple bureaucratic systems and at all levels. His drive to control data is derailing listings of Chinese entities on the New York Stock Exchange and driving a regulatory crackdown on China's capital markets.

Xi's campaign to acquire these sources of economic and geopolitical leverage is backed by industrial policies, a vast apparatus of theft and espionage, and a complex tapestry of laws and extralegal enforcement tools. China's government makes no distinctions between defense and offense, commercial and military. Nor does it subscribe to Westphalian conceptions of state sovereignty or the boundaries of state power.[14] This has vast implications for all multinationals that use and store data, and not only within China. "It is estimated that 80 percent of American adults have had all of their personal data stolen by the CCP, and the other 20 percent most of their personal data," former top US counterintelligence official William Evanina told a Senate committee in August 2021.[15] Beijing's extreme efforts to control data and data technology suggest that it will spare no effort in identifying, acquiring, and exploiting American personal data and intellectual property (IP). Xi has clearly telegraphed intent, and he is showing increasing confidence in his country's capabilities.

The logic of China's interlocking data-security laws and the ubiquitous nature of China's surveillance systems mean that **all customer data held by China-controlled companies will be**

potentially visible and accessible to China's security services. No level of encryption or localization is effective when PRC authorities demand that their corporate subordinates hand over the decryption keys. Other countries' governments should start from the assumption that all data stored by China-controlled companies will be observable, accessible, and exploitable by China's Party-state. Similarly, all unsecured data resources—whether open or simply vulnerable—will be exposed to absorption and risk of exploitation. Because there are no effective limits, legal or otherwise, on how the Party-state makes use of this data, this means that personal or economic information may just as easily be accumulated for purposes of security and coercion as for industrial transformation.

The findings of this report paint a challenging picture for policy makers. Available open-source materials from the PRC highlight strategic intent along with supporting planning frameworks and bureaucracies. They do not provide as many specifics concerning implementation, which reflects the secretive nature of Party work within multinational corporate structures as well as the relatively recent declaration of Xi Jinping's big data–harvesting ambitions. Whether or not Xi is able to achieve his objectives, Washington and other capitals will need to come to terms with the scale of China's big data capabilities, even if deployed in piecemeal or fragmented form. As described below, Party-state requisitioning of data from commercial handlers is already being used to do the following:

- build databases of individual human genomes;
- map sensitive areas of other countries' economies and borders;
- mine telecommunications networks for commercial secrets and intelligence;
- manipulate the online information environment;
- profile foreign citizens through social media; and
- target journalists who critically cover China and PRC companies.

Any of these issues should raise serious questions about what can and should be done to stop an increasingly threatening totalitarian competitor from weakening democratic societies. The Party's increasingly potent abilities to neutralize critics, compromise foreign leaders, front-run the strategic policies of competitor nations, infiltrate sensitive technological sectors, amass commercial leverage, and shape public opinion abroad will all have serious long-term consequences for international security and, by extension, for human freedom.

Beijing is motivated in significant part by ambition—to maximally exploit data as the fundamental resource of the future global economy and governance system. To ensure that data in all its forms is accumulated, controlled, and exploited to serve the strategic interests of China and the Party-state, Xi, the Party, and the People's Liberation Army—the Party's

military force—are creating a new technological ecosystem intended to accumulate and exfiltrate data at global scale.

The primary purposes of this ecosystem are described in authoritative Party texts, as follows:

Supercharging China's processing infrastructure Made in China 2025 set the target for China's cloud computing and big data technology to "reach leading international levels" by 2025.[16] The infrastructure and technologies underpinning big data capability are listed as key products and technologies for information communication–equipment development.[17]

Leveraging data absorption for economic advantage Xi Jinping spoke to the CCP Central Committee Politburo in October 2018 of the need to "give full play to my country's massive data and huge market application scale advantages."[18] Xi means to integrate big data with the "real economy," using it to maximize domestic economic prosperity by building "an intelligent economic form that is data-driven."[19]

. . . and surveillance advantage The application of data to large-scale surveillance tools is equally important. A 2015 State Council policy encourages the development of indigenous big data companies and their integration into government surveillance networks:

> [Big data is] conducive to strengthening social supervision and giving play to the public's active role in regulating the behavior of market entities; conducive to efficient use of modern information technology, social data resources and socialized information services reduce the cost of administrative supervision.[20]

Harnessing the private sector and global innovation In its 14th Five-Year Plan, released in March 2021, the chapter on "Creating New Advantages in the Digital Economy" refers to "integrated research in general-purpose processors, cloud computing, and software core technologies" as areas to be developed and "opened" by Chinese enterprises, including through the development of "innovative consortia" and "international level industrial Internet platforms and digital transformation promotion centres."[21]

Eliminating barriers to military information acquisition Beijing's ambition is also seen in its aggressive prioritization of "military-civil fusion," its strategy of "reorganizing the Chinese science and technology enterprise to ensure that new innovations simultaneously advance economic and military development."[22] This involves eliminating barriers and maximizing technology transfer between China's commercial sector and its military—including technologies acquired from foreign businesses, whether through commerce or theft. Beijing's aggressive pursuit of military-civil fusion is a key reason why Washington and other governments have been increasingly tightening regulations on flows of technology, investment, and data.

Ensuring that China's data stays in China Since 2021, the Party has shown concern that large-scale data collection by Chinese companies listed on overseas stock exchanges, such

as ride-hailing giant Didi Chuxing, could pose a "national security risk" to Beijing. Regulators have therefore moved with striking speed to punish Didi and others, impose new data and cybersecurity standards on them, and extract portions of their data holdings into state hands.[23] Other recent securities-related regulations show an increasing preoccupation with regulating the activity of **all technology firms with large data operations**.[24]

Xi Jinping has declared that "informatization"—i.e., digital transformation—has "delivered the chance of a lifetime to the Chinese nation."[25] This charged language conveys something of what is at stake in Beijing's bid for making China into a "network great power." Xi believes China must acquire the capabilities to carry out a total technological transformation of infrastructure, the economy, and society. He insists that China rapidly become an "autonomous" innovator capable of generating its own technological breakthroughs. At its core, the CCP is structured and operated in accordance with its roots as an underground revolutionary organization. Most of the Party's top leaders manage portfolios that center on the Party's expansive conception of security. Now, in the wake of the 20th Party Congress, China's peak intelligence agency, the Ministry of State Security (MSS), is represented on the Politburo and the Central Secretariat (the body that carries out the day-to-day work of China's leadership, reporting to Xi). This places them more readily at Xi's disposal for duties from internal repression and intra-Party struggle to overseas influence ops and tech transfer. As a result, these security-focused organizational structures and ethos will further penetrate all economic and societal domains. Since the 19th Party Congress in 2017, the Party has dramatically eroded traditional boundaries that separate private technology companies and the state. The spectrum of notionally private enterprises runs from firms that began as adjuncts of the state system, such as Huawei, to those now in the late stages of being systematically coerced and co-opted by the state, such as Alibaba.

1.1 REPURPOSING THE PRIVATE SECTOR

Under Beijing's new data hierarchy, all companies are forced to integrate into a centralized national data infrastructure controlled by the Party, structured to serve Party objectives in strategic competition with the West, and based on the fundamentally nonreciprocal premise that **China maximizes the absorption of data from around the world while exporting as little of its own as possible**.

The Party has long required private companies to establish Party organizations and used legal and extralegal measures to bend private companies into submission. The pressure has been most acute on technology companies, such as Alibaba. In 2016, the deputy director of the Cyberspace Administration of China, Ren Xianliang, stated: "Since the establishment of Cyberspace Administration of China [in 2014], we place great emphasis on Party-building activity within Internet companies. It is a strategic task for the development of [China's] Internet industry."[26]

This Party-building work has been so extensive that China's most successful private enterprises should now be considered effectively as arms of the Party-state.

The temptation to see Xi Jinping's data-control drive as a Chinese domestic matter is understandable given the recent torrent of high-profile data-control moves made by Beijing against domestic Chinese entities. But Xi's campaign is also moving outward internationally. Firms processing data in China, or processing data overseas, are squarely in Beijing's crosshairs. The Party is positioning itself to be the world's largest data broker.

There is nothing in Xi's language that suggests he wants to confine his data strategy to China's borders. It applies wherever the Party believes it has leverage.

As the Party has deemed more and more data strategically and economically important, it has also tasked more and more actors to obtain it. Thus, when the Central Cybersecurity and Informatization Leading Small Group was elevated to the status of full commission in 2018, Xi's launch speech emphasized the Party's policy of using civilian institutions to support strategic military goals.[27] Xi said military-civil fusion would be a "focus area and area for advance" in cybersecurity affairs, and that the Party would seek to grasp the "intrinsic relationship between productive force and combat force, and between the market and the battlefield." The nonstate actors enlisted in this "informatization" fight included internet enterprises, scientific research institutes, think tanks, and citizens. Ultimately, Xi called on the "entire Party and nation" to assist in "reform of the global internet governance system."[28]

Because large and systemically important PRC companies, whether state owned or private, are host to chains of Party organizations connecting the company's top leadership to its everyday operations, they are potentially vehicles of the Party's interests—including with respect to data.

The Party's multiple channels of control work alongside legal channels in relation to strategic decision making and management of risks. Party structures are not designed to be transparent or accountable to international regulators, partners, or investors. Outside of China, these Party-directed companies operate comfortably, creating and accessing valuable new data sets primed for easy transfer back to China in all manner of data-intensive fields—biotech, pharmaceuticals, medical devices, drones, autonomous cars and trucks, social media, digital payments, e-commerce, and more. These data flows to China contain massive quantities of information about American citizens, American companies, American government, and American critical infrastructure.

China-linked companies have managed to mostly obscure their connections to the Party-state in Beijing. Their commercial cover poses a unique challenge to US policy makers who want to reassert values of democracy and security in the digital space. Complex chains of ownership, coupled with a lack of transparency, make the risks that China-aligned companies pose to American sensitive and private information difficult to identify and prevent. Beijing knowingly exploits this asymmetry. The case studies that follow will underscore current known harms associated with the data-related operations of PRC companies in the United States.

2. CORPORATIONS AND DATA HARMS

2.1 RISK OF CLANDESTINE INDIVIDUAL HUMAN GENOME ACCUMULATION AND PROFILING

BGI Group is the world's leading provider of genomic sequencing and proteomic services.

BGI cofounder Wang Jian describes his creation as a "big data company"—and argues that "in such an industry, an industry that is supported by scientific development, big technology platforms, and big data [possibilities] are endless."[29]

In 2016, BGI established the China National GeneBank in Shenzhen. "Owned by the state" and "run by BGI," the GeneBank is a powerful piece of data-storage infrastructure that BGI leverages to develop ever-greater data sets and provide its diagnostics business with the advantage of scale.[30]

BGI's central role in the China National GeneBank provides the most sweeping example of its role in transferring its proprietary data to national Party-state institutions. According to the National GeneBank website, its mission is to "store, manage and utilize genetic resources" and "serve national strategic needs."[31]

The GeneBank was approved by multiple national government agencies: the National Development and Reform Commission (NDRC), Ministry of Finance, Ministry of Industry and Information Technology, and the National Health and Family Planning Commission.[32] It was then officially launched in 2016 with heavy government funding. Its board of trustees includes the NDRC, the Shenzhen city government, and the Chinese Academy of Sciences.[33]

According to the NDRC website, genetic resources are national strategic resources and the foundation upon which China will compete in the future bioeconomy.[34]

Data collected by BGI is at significant risk of passing into the Party-state's GeneBank databases—and from there, being utilized as a "strategic resource" by Beijing:

- On November 9, 2011, Children's Hospital of Philadelphia (CHOP) and BGI announced a new **partnership**, BGI@CHOP, to "conduct large-scale human genome sequencing and bioinformatics analysis at a newly established, state-of-the-art Joint Genome Center."[35] Public relations press releases described the partnership as focusing on the "discovery of genes underpinning rare and common pediatric diseases using next-generation sequencing," including the pairing of CHOP's biobank with BGI sequencing and analysis techniques.

- On June 18, 2012, BGI and CHOP announced **initiation** of the 1,000 Rare Diseases Project to "accelerate the discovery of genetic variants underlying rare diseases" and use next-generation sequencing technologies to analyze DNA samples from CHOP patients and families.[36]

On August 16, 2016, BGI and Israel-based agricultural genomics company NRGene announced a **partnership** to jointly provide technology to the "Chinese genomics community."[37]

- On May 4, 2018, BGI announced **partnerships** with Johns Hopkins University and Mount Sinai Hospital (Toronto) to study pancreatic cancer and develop diagnostic tests for preterm births. BGI contributed sequencing services to both projects, which included building a genomic and immunogenic database and conducting tests on pregnant women.[38]

- In April 2020, California officials **rejected** BGI proposals to sell COVID-19 testing supplies and set up entire labs at the city, county, and state levels partly on the grounds that such arrangements "could give China access to sensitive patient data."[39]

- In July 2020, the US Department of Commerce added two BGI subsidiaries to its export-control Entity List for facilitating human rights abuses in China. It accused wholly owned subsidiaries Beijing Liuhe BGI and Xinjiang Silk Road BGI of enabling activities contrary to the foreign policy interests of the United States through conducting genetic analyses used to further the repression of Muslim minority groups in the Xinjiang Uyghur Autonomous Region (XUAR).[40] These allegations were denied by BGI.[41]

- On June 24, 2021, cell-free DNA testing company Natera and BGI announced the **launch** of the BGI/Natera Signatera Assay test to identify molecular residual disease (MRD) associated with non-small cell lung, bladder, breast, and colorectal cancers.[42]

- On September 7, 2021, Reuters reported that BGI's NIFTY-branded prenatal test was being **investigated** in five countries after scientific studies showed that the test—including clinical trials—had been developed in collaboration with the People's Liberation Army.[43] Regulators cited concerns about patient data protection. At the time of the report, 8.4 million women globally had taken NIFTY tests.

According to *Nanfang Daily*, a Party-owned newspaper in Guangdong, BGI said it had twenty-five Party branches by 2017.[44] BGI's subsidiaries in turn have their own system of Party cells. BGI's Shenzhen-listed arm alone had ten Party branches and more than three hundred Party members in 2019, according to BGI sources.[45]

2.2 RISK OF SUPPORT FOR FOREIGN-ADVERSARY BIOMEDICAL PROGRAMS AND ACCUMULATION OF HEALTH DATA

WuXi Biologics is a pharmaceutical manufacturing and research-services giant that helps Chinese and foreign pharma and biotech companies design, discover, manufacture, and test drugs, especially synthetically produced "biologics." WuXi Biologics is one member of a whole family of firms related to corporate parent WuXi AppTec. It is apt that Chinese state media have dubbed WuXi the "Huawei" of China's pharma sector.[46]

Parent WuXi AppTec has some sixty-five subsidiaries and offices in twenty-seven locations across Asia, Europe, North America, and Israel. With a combined market cap of $80 billion, WuXi ranks as China's largest contract research organization (CRO), China's second-largest contract development and manufacturing organization (CDMO), Asia's top pharmaceutical research and development (R&D) services platform by total revenue, and the twenty-eighth-ranked company on Fortune's Future 50 index.[47]

WuXi set up a Party committee in 2005 that today has at least twenty subcommittees. According to a 2013 article on Communist Party Member Net (a site launched in 2012 by Xi himself, supervised by the powerful Organization Department of the CCP, and operated by state broadcaster CCTV), WuXi's seven thousand–plus employees included more than one thousand Party members.[48]

WuXi talent recruitment has drawn on state, military, and private sector networks involving China's Thousand Talents Program, the Academy of Military Medical Sciences (now on the Commerce Department Entity List), government advisory committees, the Western Returned Scholars Association (supervised by the CCP's United Front Work Department), and the Pharmaceutical Innovation and Research Development Association (overseen by the State Council).[49]

In March 2016, WuXi AppTec and Huawei signed a strategic collaboration agreement to jointly advance the collection and use of medical data, and to develop technical platforms and information standards for "precision medicine" in China. Two months later, WuXi AppTec and Huawei jointly launched the China Precision Medicine Cloud, which they said would support the Chinese government's $9.2 billion Precision Medicine Initiative (PMI). WuXi AppTec's website announced:

> This partnership aims to deliver the benefits of genomic medicine to patients on an unprecedented scale. We will follow the guidance of China Food and Drug Administration (CFDA) and work closely with third-party secure life-science cloud providers to develop the data standards and exchange framework required to deliver the China PMI. We are thrilled to be deploying WuXi NextCODE's genomics technology with Huawei across China.[50]

Huawei's website has similarly boasted that its WuXi collaboration represents China's first big data cloud platform for precision medicine and will boost the government's PMI effort.[51]

Scientists from China's military and other state organs play a large role in precision medicine. In December 2016, the Academy of Military Medical Sciences (AMMS) launched a "Big Data Management and Sharing Platform for Precision Medicine" with the Beijing Institute of Genomics (part of the state-run Chinese Academy of Sciences), which promised to work on constructing a "standardized technical system for processing and utilizing big data for precision medicine."[52]

In 2018, WuXi AppTec and China Electronics Data Service Co. (CECD) announced the joint formation of CW Data Technologies. CECD is a health care data company under the auspices of China's National Health Commission. As of 2020, its largest shareholders were state-owned China Electronics Corp. (34.29 percent) and the China State-Owned Enterprise Structural Adjustment Fund (15.12 percent), of which state defense giant China Ordnance Industries Group Co. Ltd. (aka Norinco) is a key shareholder (at 5.06 percent).[53]

CECD chairman Li Shifeng said of the joint venture with WuXi in 2018: "The establishment of CW Data is an important cornerstone for CECD into health care analytics and big data. Health care big data is one of the key national strategic resources."[54]

The US government has placed both China Electronics Corp. and Norinco on the blacklist of firms tied to China's military and surveillance state, banning US trading in their public securities.[55]

In October 2021, the US National Counterintelligence and Security Center (NCSC) identified five technology sectors of key national security concern: artificial intelligence (AI), bioeconomy, autonomous systems, quantum computing, and semiconductors. The NCSC telegraphed a need for legal and regulatory changes, saying: "Compounding the security challenges is that many existing legal frameworks focus on protecting finished intellectual property or licensed/patented products; whereas large bodies of data—such as patient health records or genetic sequence data—represent long-term, unrealized development of products and applications."[56] In press interviews, NCSC deputy Edward You specifically cited US investments by WuXi AppTec.[57]

The US-China Economic and Security Review Commission report to Congress delivered in 2021 details CCP strategy on synthetic biology and cites WuXi Healthcare's investment in 23andMe to illustrate concerns that "Chinese entities have gained potential access to U.S. healthcare data through investment in U.S. firms" and other means. The report also cites CCP plans to use foreign capital to develop emerging technologies and advanced manufacturing.[58]

2.3 RISK OF TARGETED INDIVIDUAL SURVEILLANCE AND PUBLIC DISCOURSE CONTROL

ByteDance is a China-domiciled company that has developed video-sharing social networking services (apps) known as TikTok and, within China, as Douyin.[59] TikTok reportedly has more than one billion global users.

Beijing-based ByteDance was renamed Douyin on May 7, 2022.[60] The group of ByteDance companies, including Douyin, consists principally of entities based in China, Hong Kong, and the Cayman Islands.

Douyin's editor in chief, Zhang Fuping, is also the company's Party secretary. Zhang has also served as vice president of a Douyin subsidiary, Beijing Douyin Information Service Co., Ltd., which is also owned by a state entity.[61] According to Chinese-language media:

- The Party's disciplinary and investigative body, the Central Commission for Discipline Inspection, has referred to Douyin as an "extensive, dense, and powerful surveillance net."[62]

- PRC public-security organs have established official partnerships to use Douyin's "professional expertise" for big data analysis and public-security propaganda.[63]

- ByteDance Party secretary Zhang Fuping has announced integration of Douyin with China's national internet police, calling the initiative a model of "police close to the people."[64]

Based on these accounts, there appear to be no barriers between Party-state organs and ByteDance/Douyin's software and data. According to anonymous sources who are former senior employees of the company, TikTok's operations and strategy are directed by parent company ByteDance in Beijing.[65] A review conducted by Forbes has indicated that three hundred current employees of TikTok and ByteDance have backgrounds in PRC state media.[66]

An exclusive report by BuzzFeed News provided strong evidence that engineers in China have previously had access to US-stored data.[67] These revelations contradict previous testimony by TikTok executives.[68] Later they were confirmed by TikTok in a letter to US senators only after the appearance of the BuzzFeed News report.[69]

ByteDance was a founding member of the Beijing Academy of Artificial Intelligence, established by China's Ministry of Science and Technology and the Beijing Municipal People's Government in 2018.[70] Peking University, Tsinghua University, the Chinese Academy of Sciences, and AI giant Megvii are also members. The US government placed Megvii on its export-control Entity List for enabling repression in Xinjiang in 2019, then blacklisted US public investment in the firm in 2021.[71]

TikTok's browser is reportedly able to track every keystroke made by users.[72] ByteDance admitted on December 22, 2022, that an internal-audit team—including employees in China—had inappropriately tracked journalists from the *Financial Times* and Forbes by accessing their location data in an attempt to identify their sources inside TikTok.[73]

Toward the end of 2022, key US national security officials intensified their warnings about TikTok. In November, FBI chief Chris Wray stated that the FBI has "a number of concerns" regarding TikTok as a "national security threat":

> They include the possibility that the Chinese government could use it to control data collection on millions of users or control the recommendation algorithm which could

> be used for influence operations if they so chose, or to control software on millions of devices which gives it the opportunity to potentially technically compromise personal devices.[74]

On December 3, Director of National Intelligence Avril Haines addressed TikTok at the Reagan National Defense Forum:

> It is extraordinary the degree to which China, in particular . . . [is] developing just frameworks for collecting foreign data and pulling it in and their capacity to then turn that around and use it to target audiences for information campaigns or for other things, but also to have it for the future so that they can use it for a variety of means that they're interested in.[75]

The Biden administration and TikTok have recently begun negotiating a national security agreement.[76] On March 7, 2023, the White House endorsed the bipartisan RESTRICT Act (Restricting the Emergence of Security Threats that Risk Information and Communications Technology) that would give the federal government new powers to restrict, and potentially ban, technologies emanating from China and five other nations deemed to be US adversaries.[77]

2.4 RISK OF MILITARY SURVEILLANCE

According to reports from Drone Industry Insights, the global drone market was valued at $30.6 billion in 2022 and is expected to grow to $55.8 billion by 2030.[78] In this expanding market, Chinese companies dominate, with DJI controlling over half of the entire industry.

Founded in 2006, **DJI** rose to prominence through its production of drone models and components to eventually become the poster child for the drone industry. Critical to DJI's rise was American venture capital. A $30 million funding round by Sequoia China in 2014, followed by a $75 million round led by Accel Partners in 2015, led to a valuation of more than $10 billion in 2015.[79] Thanks in large part to American investors, DJI's revenue increased one hundred-fold from 2011 to 2015.[80]

While DJI was being propped up by American venture capital, it was simultaneously receiving funding from the Assets Supervision and Administration Commission (SASAC), a Chinese ministry that manages China's state-owned companies. This relationship was officially acknowledged in 2022 despite being known informally for years.[81]

With backing from US venture capital and the Chinese government, DJI has continued to dominate the expanding commercial drone market.[82] Though DJI's market share shrank by 15 percent in 2021, it still accounted for 54 percent of the global commercial drone market that year according to drone industry research firm DroneAnalyst.[83]

Another company, **Autel**, has picked up the slack created by DJI's modest decline. Autel has been one of the primary beneficiaries of global shakeups and has grown to account for roughly 7 percent of the global commercial market share.

Autel Robotics is a Chinese company, controlled by Chinese owners and headquartered in Shenzhen.[84] Autel's parent company, Daotong Intelligent Aviation Technology Co., Ltd., is part of the Shenzhen UAV [unmanned aerial vehicle] Industry Association (深圳市无人机行业协会), which includes members of the People's Liberation Army.[85] The UAV Industry Association features military-civil fusion initiatives in China, including exchange programs and integration efforts with military entities.[86]

According to the website of the 2022 China International UAV Systems Industry Exhibition, Daotong Intelligent Aviation is a supporting organization.[87] This website states that the exhibition promotes "in-depth development of military-civil integration" and will "aim to build a military-civil exchange program and exchange private enterprises' experiences in 'joining the army.'"[88] Daotong Intelligent Aviation also supported the development of China's first UAV industry Communist Party committee in 2021.[89]

Chinese drone manufacturers have partnered with US localities and offered drones free of charge in exchange for the data. In 2016, DJI partnered with the Wrightsville Beach Fire Department in North Carolina to allow it to use two drones without charging the department on the provision that DJI retain the data it gathered.[90] DJI also donated drones to forty-three law enforcement agencies operating in twenty-two US states to enforce social distancing rules during the COVID-19 epidemic.[91]

According to a 2020 public safety drones report by Bard College examining public procurement records, 1,578 state and local public safety agencies use drones. Of the drones used by those agencies, DJI drones accounted for roughly 90 percent.[92]

Many states still overwhelmingly use PRC-manufactured drones, but in 2021 Florida passed Senate Bill 44 creating a drone white list excluding Chinese brands such as DJI and Autel.

As one vehicle within Beijing's larger data-harvesting apparatus, Chinese drones present a unique security threat that has begun to receive attention. DJI was alleged to share critical infrastructure and law enforcement data with the Chinese government according to a 2017 memo from the US Army.[93] In 2019, the Department of Homeland Security (DHS) warned that Chinese-made drones may be sending sensitive flight data to manufacturers in China, where the data may be accessed by the Chinese government due to China's data laws.[94]

DJI's ultimate control over drone location data has also been highlighted through the ongoing Russia-Ukraine war. When asked to apply geofences (software-imposed no-fly zones) to DJI drones to prevent them from flying inside Ukraine, the company refused to do so even though it had previously demonstrated the capability, having applied geofencing over most of Iraq and Syria.[95] Other drone companies such as China's Xi'an Bingo Intelligent Aviation Technology have been even more blatant in their support for Russia's invasion of Ukraine. The company has reportedly agreed to manufacture and test one hundred ZT-180 prototype drones—capable of carrying a 35-to-50-kilogram warhead—before delivering them to the Russian Defense Ministry by April 2023.[96]

DJI's drone-detection product, AeroScope, which "rapidly identifies [drone] communication links, gathering information such as flight status, paths, and other information in real-time," also raises security concerns, as its systems have been proven to not be as secure as the company promised.[97] Last year, DJI was forced to admit AeroScope's signals weren't encrypted and that "anyone with a little technical know-how could access detailed information on where and when the company's drones had been flying."[98]

3. THE ARCHITECTURE OF THE SYSTEM

The preceding case studies illustrate the risks that China's digital grand strategy poses to US entities. The next two sections detail the policy and regulatory architecture behind that strategy. Readers interested primarily in policy recommendations may advance to section 5.

3.1 XI'S INSTRUMENT: THE CYBERSPACE ADMINISTRATION OF CHINA (CAC)

In Xi's bid to carry out a total transformation of China's technological infrastructure and put this infrastructure more firmly under the Party's control in the name of "national security," the CAC has taken on the role of organizational flywheel. In this respect, it is analogous to Beijing's Financial Stability and Development Committee, but in the domain of data rather than debt. The CAC has been the main office of the Cyber Security Commission, also known as the Party's Central Cybersecurity and Informatization Commission. China's new data regime cannot be understood without understanding the outsized role of the CAC.

Since its quiet formation in 2014, the CAC has been depicted outside of China as an internet content regulator with vague cybersecurity powers.[99] However, in 2021, it was fully revealed as the preeminent agency for transmitting Xi's voluminous opinions on everything relating to the digital world. Put simply, the CAC has been responsible for the management of China's digital network and the information contained within it.

Guided by Xi and the Party's top leaders, the Cyber Security Commission and CAC have ultimately been mechanisms for controlling which entities participate in China's digital ecosystem, what information they possess, and how this information circulates throughout China and abroad. Data has been at the heart of CAC's portfolio, mirroring Xi's focus on its role as a key strategic and economic resource.

Many of these actions point to a broader mandate for the CAC in line with its cybersecurity goals—keeping data out of foreign hands and preventing its monopoly by the private sector. Importantly for foreign investors, it also now appears to be a key agency responsible for regulating overseas listing, including in Hong Kong, on the grounds of protecting personal and nationally sensitive data against inadvertent foreign leaks.[100]

Foreign investors got their first taste of the CAC "unplugged" with its probe of Didi and review of all data-rich Chinese companies listed overseas. The Didi inquiry was first announced on

July 2, 2021, by the CAC's little-known Cybersecurity Review Office, citing China's National Security Law, its Cybersecurity Law, and its own internal cybersecurity review measures.[101] Three days later, the same office announced additional probes into listed US companies Full Truck Alliance (freight) and BOSS Zhipin (online recruitment).[102] Since then, the CAC has driven a series of interministerial meetings and "interviews" with online transportation and navigation companies focusing on implementation of stronger data-security measures.[103]

These activities show that the CAC's purpose has been to support Xi's comprehensive data strategy—not only to control online content, but also to protect China's data, gain access to foreign data, and develop the technology, talent, and norms that will extend the Party's information controls into the digital domain at home and abroad. For this reason, the CAC was expanding its remit to include reshaping social media, restricting corporate data collection, and guarding against the leaking of sensitive data out of China while maintaining oversight over all data—Chinese and foreign—of potential strategic and economic value:

- According to a multiyear plan unveiled in late September 2021, the CAC and other Party-state bodies will impose additional "governance" and "supervision" standards to make algorithms "secure and controllable."[104]

- The CAC is responsible, along with the Ministry of Industry and Information Technology and the Ministry of Public Security, for regulations concerning the management (by any entity in China) of network product security, making it part of the Party's institutional system for identifying, and potentially exploiting, vulnerabilities in foreign technology.[105]

- Through a state-owned fund, WangTouZhongWen (Beijing) Technology, the CAC has taken a 1 percent stake in ByteDance and in Weiming Technology, a subsidiary of Weibo.[106] According to Reuters, WangTouZhongWen is owned by the China Internet Investment Fund, established by the CAC and Ministry of Finance in 2016.[107] WangTouZhongWen's investment means that the CAC holds a board position in both companies.

Crucially, the Cyber Security Commission, the CAC's parent organization, is headed by Xi himself. The CAC is therefore not a mere regulator. Its origins are intertwined with Xi's strategy to make China a "network power." The CAC's composition and organizational structure therefore provide a window on the extent of the Cyber Security Commission's powers:

- Xi's vice chairs on the commission have included former premier Li Keqiang and current chief theoretician Wang Huning.[108] In addition to the CAC, other organs involved in implementing commission policies include the Ministry of Industry and Information Technology, the Ministry of Public Security, the Party Secretariat, the Central Commission for Discipline Inspection, and elements from the military, the justice system, state enterprises, the private sector, state media, and provincial and urban governments.

- Through the CAC, the Cyber Security Commission implements national policy for lawful data transmission; manages internet content; supervises the online news industry;

regulates online gaming, media, publishing, and other entertainment; strengthens the Party's online presence; and directs telecommunications companies in registration of businesses and services and other "basic network management."[109]

- While information on the internal working of the CAC is scarce, appointments and hiring announcements have shed light on some of its notable internal structures. They include departments for transmission of authoritative official information online; management of the mobile internet; cybersecurity coordination; statistical analytics and technology; information services; emergency response and public information management; international cooperation; and cybersecurity review.

Xi's widening cybersecurity and data ambitions are reflected in the position of the Cyber Security Commission itself. Unlike a leading small group, a commission is responsible for top-level strategic planning, coordination, and deployment of administrative resources in ways that cut across enormous swaths of otherwise bureaucratically divided government activity.[110]

While effectively closing the loop on domestic data circulation, the CAC has also been creating a template for **directing massive amounts of data from the private economy to the security institutions of the Party-state**. In March 2023, the State Council established a new institution for implementing national data policy, the National Data Bureau (NDB).[111] While the impact of the reorganization remains to be seen, the creation of the NDB further underscores the centralization imperative first signaled by the CAC.

3.2 CONTROLLING THE DIGITAL ECONOMY

If the CAC has been the flywheel of the data strategy, then control over the digital economy is the linchpin. By expanding the cross-border activities of China's digitally proficient corporations, economic and cybersecurity planners—with Xi Jinping pointing the way—envision a vast data-absorption network capable of revolutionizing industries and strengthening China militarily.

Though not widely covered at the time, an October 2021 speech to the Politburo was Xi's most significant statement concerning the role of corporate entities in building the integrated data systems that he seeks to expand overseas. At that "collective study" meeting, Xi laid out his plan to "grasp the trends and laws of digital economy development" in order to transform China into a "network great power."[112] In this speech, Xi highlighted the significance of corporations and digital trade for positioning China's economy at the center of global data flows. He stressed:

- **Global economic competition** The role of the digital economy in the "reorganizing of global [production] factors and resources" and the reshaping of global economic structure and the competitive landscape.

- **Data and national strength** The intertwining of China's "network great power" strategy—its national cybersecurity and network control strategy—and national big data strategy.

- **Technological integration** Understanding the digital economy as consisting of the internet, big data, cloud computing, artificial intelligence, blockchain, and other innovative technologies.

- **Strategic resource absorption** Making the "strategic choice" to use this digital economy to "promote the rapid flow of various resource factors" toward China.

- **Party-state-military integration** Strengthening R&D and achieving independent innovation in core technologies by employing China's "new national system"—an integrated national modernization architecture comprising state, military, and corporate entities—in the "battle" for core technology control.[113]

- **Corporations as catalysts** Integrating domestic and global information systems through the creation of new enterprise "champions" to lead the economy.

- **Political control at home and abroad** Increasing regulatory government, and security control over digital technology while leveraging bilateral and multilateral relationships to "put forward the China model" and "project China's voice."

According to Xinhua, Xi told his leadership group:

> We should stand at the commanding height of overall strategy of the great rejuvenation of the Chinese nation and the great changes in the world unseen in a century, [and] **coordinate two major issues, namely domestic and international development**, and the security of development. **[We should] fully utilize the advantages of having massive data and a wealth of application scenarios**; promote deep integration of digital technology and the real economy; empower the transformation and upgrading of traditional industries; generate new industries, new business forms, and new models; and continuously strengthen and expand China's digital economy.[114]

This lecture was the culmination of years of building the vocabulary, policy-making apparatus, regulatory system, and legal regime that Beijing believes is needed to exploit the opportunities and counter the vulnerabilities brought about by the digital revolution.

Xi's digital-economy speech was given just a week before the appearance of a new document crystalizing his digital-economy vision into policy. A circular from the CAC and the National Development and Reform Commission announcing release of the 14th Five-Year Plan Electronic Commerce Development Plan instructed that e-commerce enterprises should focus on "manufacturing and data sharing."[115] The CAC's role in leading China's e-commerce development plan is a strong signal that the Party's data control and absorption agenda has been embedded in cross-border trade policy.

The Electronic Commerce Development Plan echoes Xi's vision of data as a resource with a wide range of strategic applications. It calls for construction of cross-border data

infrastructure, application of digital technology for expanded data circulation, and development of data collection and analysis capacity. It is an extension and enabler of the Party's design for routing more data from the world's economic activity back to China for processing. Key objectives articulated by the plan include these:

- **Manufacturing innovation** E-commerce should use data as the key link for accelerating integration and innovation within China's manufacturing industry.

- **Social credit and government information sharing** E-commerce should incorporate elements of social credit and data sharing as part of its "public service system."[116]

- **Overcoming trade blockages** The main obstacles to implementation of China's economic strategy include global competition to shape privacy protection, data flow, and other rules.

- **Establishing a new global economic layout** China should develop "high-level" cross-border e-commerce and global networks of warehouses, logistics, data, payments, and services.

- **Integrated data utilization** Data resources created through e-commerce activity should be integrated into government data-sharing and standardization systems, and integration of data resources across e-commerce platforms accelerated. E-commerce data should be registered as a national resource and its wider circulation across China's domestic economy promoted.

- **Party leadership and monitoring** Local governments should support the creation of a centralized supervision and monitoring system for tracking data-resource use.

- **Outbound data security** All outbound data related to e-commerce must be secured and reviewed for "risk prevention" purposes.[117]

In essence, the 14th Five-Year Plan Electronic Commerce Development Plan is a blueprint for obtaining data through cross-border trade and integrating it into new platforms for sharing information across industries and with the Party-state. Since it was issued, implementation plans covering absorption and utilization of cross-border data flows have appeared at the provincial level. These, in turn, detail cooperative arrangements between government and enterprises for gaining access to foreign data through trade agreements and expanded access to enterprise databases.[118]

The superimposition of layers of political control over cross-border state and private commercial activity illustrates how Xi's data-absorption model is being applied across China's economy—and across the markets of foreign trade partners.

3.3 DATA STRATEGY AND GLOBAL ACQUISITION

Xi's October 2021 lecture on the digital economy, and subsequent commercial data plan, capped years of internal policy guidance directing the Party to utilize corporations as chess pieces in China's data-focused economic strategy.

Since coming fully to power in 2013, Xi has ascribed outsized significance to data as a driving factor of national development and international competition. At the first meeting of the Party's Central Cybersecurity and Informatization Leading Small Group in February 2014—an event that marked Xi's first major foray into shaping China's cyber policy—Xi said:

> Network information flows across borders, and information flow leads technology flow, capital flow, and talent flow. The degree of information technology and industrial development determines the level of informatization development. It is necessary to strengthen independent innovation of core technologies and infrastructure construction, [and] improve information collection, processing, dissemination, utilization, and security capabilities, to better benefit the people's livelihood.[119]

In the same speech, he outlined how informatization and economic globalization would "promote each other." He directed that China "use security to ensure development" in public opinion work and cross-border information-flow management, and he initiated plans to secure independent state control over technology, infrastructure, and domestic and cross-border information flows. "Information resources are increasingly becoming an important factor of production and social wealth," he said.[120]

A year later, during an inspection tour of Guizhou province, Xi expanded on how "seizing the commanding heights" in informatization would win China new development opportunities. He directed that China should seek to be at the "forefront of the world" in the application of big data to industrialization.[121] "Our country's big data gathering and utilization has just started," he added. In tandem with seeing data as a critical factor of production, these political instructions cascaded into a set of formal policies combining Xi's vision of China as a "network great power" ("network strong country" or "network superpower") with an economic agenda of integrating foreign technology, Party-controlled network infrastructure, and open "sharing" of data through trade.[122] This agenda was revealed and developed through a pair of speeches given in 2016 in which Xi addressed the global dimensions of the Party's big data strategy, including the role to be played by corporations.

In April 2016, Xi directed the Party's Work Conference for Cybersecurity and Informatization to make "deep integration of information resources" a key goal of cyber policy.[123] Xi called mastery of internet core technologies the "vital gate"—meaning the ultimate goal—of supply chain security and the "main battlefield" of national economic policy. He emphasized the necessity of "secure and controllable" foreign participation in critical sectors in order for China to achieve R&D self-reliance, and the "sense of mission and responsibility of [our] Internet companies" for ensuring cybersecurity, economic development, and "spreading into the world" to "expand overseas development space." He further directed establishment of a "national

information resource sharing system" to improve government data utilization, and parallel mechanisms for government-enterprise information sharing in cybersecurity and industrial development.

Next, in October 2016, Xi spoke to other members of the Politburo on the theme of "accelerating and promoting independent innovation in network information technology (IT) and tirelessly building a 'network great power.'"[124] During his speech, Xi directed that the Party "cultivate new kinetic energy" for China's economy by focusing on investment in infrastructure and "deep integration of the internet with the real economy" in order to augment China's national strength. Concerning use of data by government, he said: **"We must . . . use data centralization and sharing as an approach [and] build nationally integrated national big data centers and promote technological integration, business integration, and data integration."**

Xi was promoting a plan for expanding China's big data gathering and integration capabilities to anywhere that its enterprises could reach. Though its consistent message was one of data control, the vectors (corporations, China's market leverage) and long-term strategic goals (positioning China at the top of manufacturing and big data supply chains) were more far-ranging than "techno-authoritarian" cybersecurity and surveillance applications.[125] This vision reached its most mature form in 2017, when Xi launched the Party-state's "Digital China" construction strategy—a national-level development initiative for China's digital transformation through "data-driven socialist modernization."[126] An unmistakable component of this strategy was the role of enterprises as "supply chain" catalysts for flows of data back to China, where they would be utilized in new systems of sensing, control, and innovation. Thus did Xi outline a framework of technological ambition that applies to the development of hardware, software, network security, data management, and every element in the cyber domain, including the following:

- **Big data supply chain control as commercial strategy** China's digital economy players should concentrate their "superior resources" on making breakthroughs in big data technology and constructing an "autonomous and controllable" big data supply chain for China.

- **Interconnection and Party-state-corporate integration as competitive strategy** The Party should "construct basic information resources . . . in important fields" and "form an interconnection of all things [through] human-computer interaction and 'integration of heaven and earth.'" Utilizing "the advantages of our country's [political] system and market," China's approach to economic competition should incorporate elements of big data development, market leadership, and integration of production and research through data, he said.

- **"A digital economy with data as the key factor"** According to Xi, the digital economy and real economy should be fused through IT technology, big data, and AI, with data serving as the "innovation engine" for China's manufacturing industries and overall development strategy.

- **Accumulation of "social" data for governance and control** In order to improve data-driven governance and control systems, data should be centralized and integrated through big data platforms such as e-governance and "smart cities." Social data accumulated by enterprises should be utilized to strengthen governance by state authorities and network managers.

- **New imperatives for data circulation and use** To ensure national data security, China should pursue a policy of strengthening critical information infrastructure protection while formulating new systems for opening and circulating data resources. Xi also directed that the Party strengthen research on international data governance and "propose a Chinese plan" in response. Cadres, he instructed, should be "good at obtaining, analyzing, and using data" in their work, and China should build a new national data "team" of talented individuals crossing all economic sectors.[127]

According to Party ideological media, this meeting marked the inauguration of China's "national big data strategy."[128]

Xi's strategy has remained essentially unchanged since its inauguration. At the Party's National Cybersecurity and Informatization Work Conference held in April 2018, he described informatization as delivering the "chance of a lifetime" to the Chinese nation, and directed again that big data be "deeply" integrated and utilized for China's industrialization and economic development.[129] In particular, Xi called on corporations to support Party-state informatization goals, including engaging in military-civil fusion and forming part of an "all-factor, multidomain, and high-efficiency system" for merging IT and productivity advances with military combat needs. "It is necessary to seize the historical opportunity of contemporary information technology change and new military change, and deeply comprehend the internal relationships between productive power and combat power, and the market and the battlefield," he said.

According to these policies, no effective distinctions exist between government and corporate organizations.[130] Their goal is to promote China's utilization of data resources for strategic goals—industrial development, innovation, resource accumulation, and global competition. Just as acquisition of strategically important technologies abroad has been backed by a mix of corporate maneuvering, espionage, and coercion, big data industry policy created in Beijing is tactically eclectic, but focused on a single, unifying strategic objective—data accumulation.

3.4 CHINA'S NEW NATIONAL DATA ARCHITECTURE

Xi Jinping's ambition to exploit data as a catalyst for China's economic development and globalization describes digitized information as the fundamental building block of a new industrial society—not just politically totalitarian, but economically integrated through IT and the accumulation of strategically important data "resources" and "production factors."

The Party's charged rhetoric of making China into a "network great power" has attracted attention for what it has said about the rapid modernization of China's indigenous IT

capabilities for security, governance, and omnipresent social surveillance. At the same time, the Party-state has also implemented the economic modernization aspects of Xi's data strategy through a series of frameworks, laws, and other mechanisms intended to incorporate data-driven modernization into all aspects of economic planning.

Viewing data as a valuable production factor means that the Party is, in essence, overhauling decades of received wisdom concerning the sources of economic growth. The genesis for this transformation is Xi's own emphasis on data as a "basic resource" and big data as signifying a "new stage of informatization development."[131] Xi's formulation was later enshrined and expanded by the rest of the Party in the Fourth Plenum Resolution on China's socialist institutions and governance system issued in October 2019, which listed data alongside labor, capital, land, technology, and management as "important factors" for production.[132] The resolution also directed that the Party establish rules for management of Chinese society using big data, strengthen "orderly sharing of data," and optimize databases for economic governance.

Data-focused policy transmission intensified during the lead-up to the 14th Five-Year Plan, when the Party Central Committee convened for another plenary session in October 2020 to set parameters for China's economic development road map. According to the Plenum's recommendations:

- Big data, the internet, and AI should be used to facilitate "deep fusion" of China's strategic emerging industries.
- China's infrastructural construction should focus on creation of more big data centers.
- Systems and standards should be established to promote data sharing with government entities, cross-border transmission, and development and utilization of data resources.
- New systems should be developed for incorporating data into governance and macroeconomic management, and for creating a marketplace for data and other production inputs.[133]

Unveiling of the 14th Five-Year Plan (2021–2025) and 2035 Long-Range Goals in March 2021 added further details on how this data development road map was to be implemented. The data accumulation and utilization platforms it authorized included these:

National Infrastructure and Oversight

- A national integrated big data system, including national hub nodes and supercomputing facilities.
- A national public data resource system for registering and securing sensitive data and making data more accessible to governments and third parties.

- Protection systems for critical information infrastructure and data resources, and to ensure political security.

- Use of the United Nations and other international bodies to advance China's interests through the formulation of rules, standards, and law enforcement mechanisms.[134]

Industrial and Third-Party Transfer

- Creation of an integrated industrial cloud for use across industries, including "digital economy key industries" (cloud computing, big data, internet of things, industrial internet, blockchain, AI, virtual and augmented reality).

- National research platforms for transferring and licensing R&D to enterprises.

- Opening of enterprise data from search, e-commerce, and social media, and development of a third-party big data services industry.

- Data-trading platforms for use by market entities.

Governance

- A national e-government network and construction of a government cloud platform and data system for future data migration.

- Government decision-making monitoring and predictive systems, and macroeconomic governance and policy assessment systems, utilizing big data and AI.

- City data resource systems and smart city "data brains."

- Public resource data-sharing platforms.

- "Intelligent platforms" for public security, law enforcement, and the judiciary.

New Pilots and Databases

- Hainan Free Trade Port pilot for cross-border data transmission.

- Establishment of a biological data and biosecurity data system.

These planning targets highlight Beijing's ambition of creating a single, integrated data infrastructure capable of supporting a strategic objective in areas ranging from industrialization to security. Beijing took steps to formalize this objective in the March 2023 creation of the National Data Bureau.

As the Party, guided by Xi, has incorporated data into its guiding frameworks for economic development and industrialization, it has also unveiled a series of tactical measures to augment and integrate information networks within China in order to significantly increase state processing capacity. This planned transformation of China's infrastructure was signaled by the 2015-issued Made in China 2025 industrial road map for "reaching leading international levels" in cloud computing and big data technologies within a decade.[135] The appendix on page 48 gives more details of how the implementation of Xi's big data agenda has been continuously updated and fine-tuned through a series of less widely studied plans and measures beyond Made in China 2025, including the Action Framework for Promoting the Development of Big Data (2015), Big Data Industry Development Plan, 2016–2020 (2016), 14th Five-Year Plan Big Data Industry Development Plan (2021), and Overall Layout Plan for Constructing Digital China (2023).

3.5 GLOBALIZING THE DATA AGENDA

In recent years, Beijing has initiated a new phase in China's national data-accumulation effort, relying on cross-border trade and e-commerce agreements, as discussed above, to accelerate data flows and improve accessibility abroad. The approach is nakedly nonreciprocal, relying on open access to foreign data while denying foreigners access to Chinese data. The United States, after all, has no federal approach to data governance, while Europe's General Data Protection Regulation (GDPR) is focused mostly on consumer privacy and is ineffective in stopping nonreciprocal data flows to China. China has adopted a mercantilist posture that appears to assume that foreign governments are incapable of responding.

Beijing's new laws and sanctions also seek to deter vigorous use of new US regulatory tools—such as the Commerce Department–led ICTS process for curbing cross-border data flows—by threatening that US firms in China will face retribution for any data-related restrictions imposed by Washington. To date, the regulatory action has been directed mainly at the data of domestic companies. But Xi's campaign is also moving out to international targets.

China's Global Data Security Initiative

Speaking to the G20 Leaders' Summit in October 2020, Xi Jinping delivered a direct message to the world's economies: keep your innovation ecosystems open (to us). "Creating small circles artificially, or even drawing lines with ideology . . . will harm scientific and technological innovation," he declared.[136] Instead, leaders should join in "promoting deep integration of digital technology and the real economy" and "actively create an open, fair, just, and nondiscriminatory digital environment." Xi proposed two additional steps to support his vision of innovation and data without borders: the launch of the Global Data Security Initiative (GDSI), a governance mechanism established by Beijing, and China's application to join the Digital Economy Partnership Agreement (DEPA), a digital-economy partnership established by Chile, Singapore, and New Zealand.

Among the key points of the **Global Data Security Initiative** was that signatory countries should "maintain open, fair, and nondiscriminatory business environments."[137] It continued:

"Countries should look at data-security issues in a comprehensive and objective manner based on facts, and actively maintain an open, safe, and stable global chain of information technology products and services." In addition (perhaps secondarily), it advocated for a series of data-sovereignty measures: countries should not damage each other's critical infrastructure or steal each other's data, should protect personal information against abuses of information technology, and should not attempt to directly access data stored in other countries without legal permission.

The Global Data Security Initiative was not new—it was first launched in September 2020 by the PRC Ministry of Foreign Affairs. In the accompanying announcement, Foreign Affairs Minister Wang Yi stated that while all countries had a right to data security, they also had the obligation to "provide all companies with an open, fair, and nondiscriminatory business environment," and should reject "digital protectionism."[138] At the time of Wang's announcement, Chinese technology company Huawei was seeing its products removed from global ICT supply chains and its manufacturers cut off from microchip technology over security concerns, which may have explained Wang's further statement that "politicizing data-security issues, deliberately applying double standards, even spreading rumors and 'smearing,' [all] violate the basic norms of international relations, and seriously interfere with and hinder global digital cooperation and development."[139]

The Global Data Security Initiative was therefore arguably a response, and rebuttal, to the US Department of State's "Clean Network" proposal, which sought to counter threats to data security created by China-manufactured technology.[140] But it was also a revealing document because it exemplified Beijing's view of data security writ large: all countries should enjoy the basic right of data security, so long as they allow Chinese companies to operate freely within their borders and do not cut off data and technology flows to China.

While uptake of the GDSI has not been widespread, neither has it been negligible. In March 2021, China and the League of Arab States signed a joint data-security agreement incorporating seven of the GDSI's eight proposals.[141] And in August 2021, the Cyberspace Administration of China (CAC) announced the launch of a Cyberspace Community of Common Destiny initiative together with fourteen African countries and the African Union Commission.[142]

Multilateral Digital Trade Agreements

China's proposal to join the **Digital Economy Partnership Agreement**, also mentioned in Xi's G20 speech, represents another potential channel for data and technology absorption. Among its component provisions, DEPA's aims are these:

- establish universal digital "windows" for exchange of data related to trade administration;

- create rules for digital interoperability and standards for data exchange;

- remove requirements forcing use of computing facilities in partner countries as a prerequisite to trade;

- enhance cybersecurity cooperation; and

- facilitate data sharing to promote creativity and innovation.[143]

These are not principles that sit easily alongside China's own legal-regulatory data regime (see below). In 2021, China was ranked the most data-restrictive country in the world by the Information Technology and Innovation Foundation, while DEPA signatory Singapore's data-storage and cross-border policies are far more relaxed by comparison.[144] Instead, China's DEPA application was announced with great fanfare by official media and commentary stating that membership would "further consolidate China's influence in the field of digital trade governance" and "promote innovation and sustainable development" for China's economy.[145] With China's application now under formal review, the PRC government has again taken to describing the goal of accession as "creating an open and safe environment" for Chinese firms to operate without restriction.[146]

Beijing's diplomatic strategy of accessing benefits from other countries' openness is visible in other agreements China has joined or is seeking to join. Under the **Regional Comprehensive Economic Partnership (RCEP)**, China will have an opportunity to play a shaping role in shaping the digital trade rules, including laws and policies for e-commerce.[147] Likewise, approval of China's long-shot application to join the **Comprehensive and Progressive Agreement for Trans-Pacific Partnership (CPTPP)** would allow Chinese companies to facilitate cross-border data transfer in an environment with reduced security restrictions—though China's own data restrictions are one of several areas likely to make accession impossible barring significant reforms.[148] (It may also be the case that China's application is a move to challenge Taiwan, which has also applied to join CPTPP.[149])

Legalized Mercantilism

China's recent data laws run contrary to the principles of the multilateral trade organizations to which Beijing seeks accession. Data-processing restrictions have increased steadily as data accumulation has become more tactically sophisticated and overt. Led by Xi Jinping, the Party has initiated a dramatic expansion of laws formalizing the Party-state's claim to all data and establishing greater coercive power over entities involved in data creation, storage, and transmission, not only in China but around the world.

The first wave of data-related laws placed obligations on all PRC citizens and other entities to cooperate with state security and cybersecurity authorities. Included are these:

- The **State Security Law**, promulgated in 2015, requires that PRC citizens and organizations provide information, support, and other requested assistance to national security bodies, public security bodies, and the military, whose responsibilities include collecting information relevant to national security (Article 52). State control over

all network infrastructure and data is mandated by the law, as is the "safeguarding of national cyberspace sovereignty, security, and development interests." The law further states that China's development interests include "construction of autonomous innovation capabilities" and control over "strategic high-tech and core technologies in key fields" (Article 24).[150]

- The **Intelligence Law**, which took effect in 2017, compels PRC entities to support China's intelligence services by turning over data collected in China or overseas, and to do so in secret. The law states in Article 7 that "any organization or citizen shall support, assist, and cooperate with the state intelligence work in accordance with the Law, and keep the secrets of the national intelligence work from becoming known to the public."[151]

- The **Cybersecurity Law**, also effective from 2017, similarly compels companies and individuals to make networks, data, and communication within China available to the police and security services (Article 28). The law also institutionalizes the localization of all data concerning PRC entities and individuals (Article 37), helping to ensure that no information stored in China, or sent cross-border to or from China, will be protected from Beijing's comprehensive security and surveillance framework.[152]

- The **Encryption Law**, which took effect in 2020, requires that foreign companies seeking to use or sell encryption tools in China first get them approved by Beijing's State Cryptography Administration, a process that requires providing the government decryption keys, passwords, and access to all underlying data.[153]

Having codified the requirement that tech companies make data accessible to the state, the Party in 2021 enacted laws to make sure that it could not only access data but also control it—that is, regulate its storage and transmission, block its transmission where and when desired (especially cross-border), and otherwise govern others' use of it.

- The **Data Security Law**, which took effect in September 2021, asserts Beijing's power not just to access private data (including Chinese "national" data processed overseas), but to regulate or block its transmission.[154] It establishes strict regulations for "important data" and "core data," and prevents either from leaving China without national security review (Articles 21, 31).[155] In addition, the DSL includes extraterritorial provisions imposing "legal responsibility" on data operators around the world for any processing of data contrary to China's national interests (Article 2), and states that punitive measures will be imposed on any country limiting flows of data and data technology back to China. The DSL also states that if another country "adopt[s] discriminatory prohibitions, restrictions, or other similar measures against the PRC in terms of investment and trade related to data and data-development and utilization technologies," Beijing will take "equivalent measures" in return.

- The **Personal Information Protection Law** (PIPL), which took effect in November 2021, requires companies handling Chinese citizens' personal data (anywhere in the world)

to minimize its collection and disclose how it is used, while forbidding its transfer and storage without state permission.[156] The PIPL also promises punitive actions and blacklisting for foreign data processors harming the interests of the PRC government or citizens through personal data. Like the DSL, the PIPL promises punitive action against any foreign government deemed to discriminate against China with respect to the protection of personal information.

None of these laws protect data stored in China from access by the Party-state. Instead, their intent is to make acceptance of China's data-security norms a precondition of digital commerce.

What this means in the aggregate is that the Party's strategy for data accumulation through multilateral trade agreements is intentionally offset by domestic laws making the vast majority of China's data a protected resource. Even limited access to this resource is conditional on foreign countries and corporations accepting measures—contrary to principles espoused by other multilateral signatories—making forced data localization a precondition of trade.

Another, more obvious, discrepancy is between Beijing's emphasis on security for its own data, and open access to the data and related technologies of other countries. The Party appears to be attempting to preserve the relative advantages of the size of China's data market as a source of economic and technological leverage. With the Data Security Law, for example, Beijing has adopted a posture of seeking to keep domestic data localized and out of foreign hands, while asserting jurisdiction over data processing activity worldwide. To the extent that this asymmetric and nonreciprocal "accumulation plus hoarding" approach is successful, it will be in part because other countries are willing to compromise on issues of data sovereignty in exchange for promises of trade and other economic benefits.

4. THE ECOSYSTEM: OBLIGATIONS, INFRASTRUCTURE, AND EMERGING PLATFORMS

The CCP takes a three-part approach to data and data technology: control, accumulate, and indigenize. While extracting data resources from foreign counterparts through trade, China's laws and security barriers create obstacles making reciprocity impossible. Left unregulated, data flows and trade agreements become vectors for Party "tunneling" into target systems—and societies. Over time, this will only further narrow the competitive gap between China and technologically advanced countries, while compromising the privacy of individuals in countries vulnerable to China's inroads through infrastructure and commercial expansion.

Corporate structures are therefore the most important building blocks of Party data strategy. This is not only because they are less detectable as vectors of Party-state activity, but also because they are already integrated into ongoing efforts to create innovative capacity at the level of national industrial competition.

At its Fourth Plenum, held in October 2020, the Party Central Committee resolved to "perfect science and technology innovation institutional mechanisms" by "building a new national system for making breakthroughs in key core technologies".[157] The resolution described "enterprises as the main body" of this system, and further proposed a "deep fusion of industry, universities, and R&D institutions" as well as the "integration of large, medium, and small enterprises" to produce innovation. In a section on the Party's absolute leadership over the military, the resolution stressed "accelerated deepening" of military-civil fusion and building of a "unified national strategic system and abilities"—a phrase referring to the intertwining of economic development with national defense.

The October 2021 Fifth Plenum, which unveiled Xi's vision of a more technologically self-reliant "dual circulation economy," further emphasized the role of enterprises as leaders of innovation. The key policy document that this meeting produced was a set of recommendations serving as the basis for China's 14th Five-Year Plan and 2035 development goals. In these recommendations, enterprises were again described as the "main body" of innovation, with an added "important role" for entrepreneurs.[158] All, the document stated, should undertake research in support of national goals. The recommendations also instructed that "innovation factors"—a broad reference to labor, capital, land, technology, and data according to Party media—be concentrated in enterprises, and that enterprises further construct "technology platforms" for sharing innovation resources more widely across the economy.[159]

All of these themes were repeated in the 14th Five-Year Plan itself, which additionally directed that "national research platforms, science and technology reports, and research data" be fully opened to enterprises as support for the national enterprise innovation system.[160] Consistent with the data-sharing underpinnings of Beijing's industrial policy, the plan also called for the "opening of search, e-commerce, and social data" **by enterprises** to unspecified entities within China to create a "big data services industry" based on these data sets.

At the highest level of Party-state economic planning, **enterprises are therefore the fulcrum of China's data strategy for supporting national science and technology innovation goals**. They also serve as creators of data for the Party's big data ambitions.

These obligations are reinforced by a thickening mesh of legal and institutional top-down controls. Since the Fourth Plenum, top officials have echoed the Party's call for a fused system of corporate, educational, and state R&D known as the "new national system" (新型举国体制)—the same as outlined in the Party Central Committee's Fourth Plenum in 2020. The contours of this sprawling modernization architecture are dim, but they reinforce the goals of integration and top-level strategic guidance that are cascading through all areas of China's economy. Jiang Jinquan, head of the Party's internal think tank, the Central Policy Research Office, has said that the new national system will mobilize "all national resources" in overcoming technological bottlenecks and obstacles created by the US technology blockade.[161] His 2021 article in *Study Times*, the journal of the Central Party School, proposed that the state should "buy achievements" from the private sector in order to drive China's mastery of emerging technology.[162]

Because the relationship between data and innovation has been so tightly sutured together by the Party-state's centralized planning schemata, the "achievements" of corporations include the data that they are able to acquire and transfer to the innovation-absorption mechanism described by the Fourth Plenum resolution and by Jiang.

This new strategic-industrial form of national integration is a new layer being transposed on top of existing mechanisms and obligations that bind corporations, and individuals, to Party goals. Data, as another form of information, is already being redirected toward China through institutional and human networks that predate commercial data strategy but are now intertwined with the Party's technology-supremacy obsession.

Private Companies

Underpinning the Party's strengthening of its commercial data strategy, it has also sought to assert greater control over private companies. The divide between private and public companies has narrowed through the Party's aggressive expansion of Party organizations within private companies, and use of extralegal measures to purge prominent leaders of private companies.

Party members in Chinese private companies are required to establish formal Party structures in all organizations with three or more full Party members, according to the CCP Constitution.[163] **The Constitution directs that Party organizations "implement the Party's principles and policies" and "exercise leadership" where they are present, including in all non-public sector entities.** Separately, the role of Party leaders includes "guidance" of the nonpublic economy.

The Party Constitution should be read in conjunction with Article 19 of the PRC Company Law, which carries the following requirement:

> In a company, an organization of the Communist Party of China shall be established to carry out the activities of the Party in accordance with the charter of the Communist Party of China. The company shall provide the necessary conditions for the activities of the Party organization.[164]

In addition, companies must "accept supervision by the government and the public and assume social responsibilities" (Article 5). The recently promulgated PRC Civil Code likewise imposes political strictures on companies, forbidding them from "carrying out acts that endanger the national or social public interest" (Article 534).

The pressure has been most acute on technology companies. In 2016, the deputy director of the Cyberspace Administration of China, Ren Xianliang, stated:

> Since the establishment of CAC [in 2014], we place great emphasis on Party-building activity within internet companies. It is a strategic task for the development of [China's] internet industry.[165]

In light of these developments, it is fair to say that China's most successful private enterprises should now be considered effectively arms of the Party-state.

Party Members

The introduction of Party control mechanisms into private companies means that distinctions between the state and nonstate sectors have dissolved. According to the CCP Constitution, all Party members are required to "be ready to make any personal sacrifice" (Article 2) and prioritize "the interests of the Party and the [Chinese] people . . . before all else" (Article 16).[166]

The Constitution further confers upon Party members an obligation to protect the Party's secrets, including the secrets of their own Party identities. New Party members take the following oath:

> It is my will to join the Communist Party of China, uphold the Party's program, observe the provisions of the Party Constitution, fulfil the obligations of a Party member, carry out the Party's decisions, strictly observe Party discipline, protect Party secrets, be loyal to the Party, work hard, fight for communism for the rest of my life, always be prepared to sacrifice my all for the Party and the people, and never betray the Party.[167]

These obligations—in particular the obligation of secrecy—supersede all other legal obligations that Party members may be placed under.

Large, systemically important companies are likely to have many Party members. There is no public information to suggest that private companies are exempt from legal and extralegal obligations to develop and strengthen Party organizations. Scholars have shown that the Party has been systematically building the strength and influence of Party committees since the global financial crisis in 2008.[168]

Entrepreneurs

Increasingly, the Party system has been exerting its power to press and incentivize the private sector to directly support political and policy objectives, such as centralized economic planning. This is clearly stated by top leaders and through authoritative Party documents.[169]

Xi Jinping has taken the message of Party control directly to China's private companies. He has explicitly tied their future success to their demonstrations of "patriotism"—a term the Party uses interchangeably with "Party loyalty." In a July 22, 2020, speech to entrepreneurs, Xi was quoted as saying:

> If entrepreneurs want to lead . . . and move toward a more brilliant future, they must continuously improve themselves in patriotism. . . . **Enterprise knows no borders, and entrepreneurs have a motherland.** Excellent entrepreneurs must have a lofty sense of mission and a strong sense of responsibility for the country and the Chinese nation.[170]

At the time they were given, Xi's remarks provided a key indicator that the current 14th Five-Year Plan would prescribe more-formal cooperative structures for building relations between politics and business. His audience for these remarks included heads of state-owned enterprises, private entrepreneurs, and managers of foreign-funded enterprises.

Military-Civil Fusion

Private companies are expected to support military-civil fusion initiatives. MCF is a national strategy to use the private sector to develop and acquire IP, research, and technological advances in order to ensure that new innovations simultaneously advance economic and military development. Xi Jinping is chair of the CCP's Central Military Commission and the Central Commission for Military-Civil Fusion Development, which he established in 2017.[171]

According to Xi, the goal of MCF policy is to "seize the strategic commanding heights of science and technology innovation" in military, civilian, and dual-use technologies.[172] This involves eliminating barriers and maximizing technology transfer between China's commercial sector and its military—including technologies acquired from foreign businesses, whether through commerce or theft.

According to the former US State Department's assistant secretary of state for international security and nonproliferation, Christopher Ford, PRC tech companies "have no meaningful ability to tell the Chinese Communist Party 'no.'"[173] A 2016 CCP Central Committee document, "Opinions on the Fused Development of Economic Construction and National Defense Construction," whose appearance augured the creation of the Central Commission for Military-Civil Fusion Development the following year, referenced the establishment of "legal guarantees" for deepening integration—in other words, requirements of civilian support.[174] In addition, the document laid out a policy framework for accelerated "guidance" of private enterprises into MCF research fields, including through the opening of defense research platforms and "opening" of new military-civil innovation platforms drawing on research from industry, universities, and state R&D institutions.

This framework has been expanded and deepened in new policies bearing Xi Jinping's personal imprimatur. The "Military-Civil Fusion Development Strategic Framework," approved in March 2018, states that innovation should be "coordinated" across military and civilian research fields, including through infrastructure and resource sharing.[175]

4.1 STORING AND PROCESSING

The Party's agenda of accumulating and controlling data depends on infrastructure as well as on networks of cooperative corporations and individuals.

Beginning especially in 2015, Xi Jinping has worked to create national data infrastructure—both physical and governmental, including servers, monitoring and processing facilities, bureaucracies, and laws—to accomplish the myriad functions necessary for implementing his national and global strategy of data dominance.

For foreign firms, this has meant learning to comply with legislation such as the National Cybersecurity Law (2017), the Data Security Law (2021), and the Personal Information Protection Law (2021), which demand that China-related data be stored and processed according to Beijing's rules, regardless of jurisdiction.

Now the next stage of Beijing's data-infrastructure strategy is coming into view.

National Data Clusters

According to the National Development and Reform Commission, growth in China's big data industries and its application will be fueled by construction of four data center "mega-clusters" in the country's northern and western regions.[176] The NDRC formulates and implements national economic, social, and development programs, including major construction projects.[177] It is the modern incarnation of the old State Planning Commission. Its Department of Innovation and High-Tech Development coordinates the implementation of China's national big data strategy.[178] The NDRC is also involved in the development of security technologies with applications in intelligence and surveillance. The NDRC supervises the National Engineering Research Center for Big Data Collaborative Security Technology, of which the Ministry of State Security's China Information Technology Security Evaluation Center and the Ministry of Public Security's Third Research Institute are members.[179] The Ministry of State Security is China's lead intelligence agency; the Ministry of Public Security is the lead internal security agency.

In February 2022, the NDRC officially launched the "Eastern Data, Western Computing" (EDWC) project, which coordinates the layout of China's National Integrated Big Data Center System.[180] According to *People's Daily*, the initiative aims to build a new type of computing network that integrates cloud computing and big data capabilities, while servicing the growing computing needs of China's east through data centers in its west, where energy is cheap.[181]

Among the ten planned data center clusters, five are in China's underdeveloped, energy-rich west: Inner Mongolia, Ningxia, Gansu, and Guizhou. The remaining clusters are to be built in the Beijing-Tianjin-Hebei region, the Yangtze River Delta region, the Chengdu-Chongqing economic circle, and the Guangdong-Hong Kong-Macao Greater Bay Area.[182]

Major telecommunications operators China Telecom and China Unicom have indicated that they will build data centers in line with the EDWC layout.[183] Tencent, Alibaba, ZTE, and Huawei are also publicizing their involvement in the project.[184]

4.2 EMERGING PLATFORMS

As it constructs a new national network of data clusters, the Party-state is simultaneously introducing new policies and regulations designed to reinforce the obligations of industry and corporations to support Party-defined science and security aims.

Through this emerging system of **data accumulation and transfer platforms**, commercial data in strategically important—and nationally sensitive—industries is drawn into an entire

ecosystem designed to facilitate long-term sustained espionage, IP theft, and interference. Unlike better-documented practices of data "tunneling" through hacking, insider threat, and co-optation, platforms exploit access to the free flows of information and trade that characterize open societies.

Notable examples of the Party-state directing corporations to accumulate and "open" data in the name of national objectives through the creation of new platforms include these:

- **E-commerce** The 14th Five-Year Plan Electronic Commerce Development Plan (see above) guides digital enterprises to create and support a "public service system" incorporating social credit and other data—in particular, data related to development of China's manufacturing sectors.[185] The plan outlines an integrated system of cross-border e-commerce and supporting logistical services, and requires that data resources created through e-commerce activity be shared across government systems and registered in national databases for the good of the national economy.

- **Genomics** The March 2022 "Human Genetic Resources Management Regulations Implementation Instructions" reinforce the obligations of industry and corporations to support Party-defined science and security aims.[186] The scope of the instructions is both domestic and extraterritorial: it specifically restricts any unapproved research on China's "national" human genetic resources, regardless of jurisdiction (Article 11, Article 12). In addition, the instructions direct the establishment of a national program for genetic "preservation work" through the construction of a "basic [genetic] preservation platform and database" (Article 20).

- **Blockchain** In October 2019, Xi Jinping addressed fellow members of the Politburo in a "collective study" and directed them to ensure that China seize the "commanding heights of innovation" in blockchain technology.[187] In the course of tapping blockchain's "new industrial advantages," Xi continued, China would become an international standards-setter and "network power." The next year, the NDRC-governed "Blockchain-Based Service Network" (BSN) unveiled its global infrastructure network for supporting development of blockchain and distributed-ledger technology.[188]

- **Fintech and payments** Since April 2020, the People's Bank of China (PBOC) has gradually unveiled its Digital Currency Electronic Payment network (DCEP, since rebranded as e-CNY), culminating with the international debut of China's new digital payments system at the Beijing Winter Olympics in 2022. When DCEP gets off the ground, it is likely to create the world's most powerful database of personal financial information. Unlike Alipay and WeChat Pay, DCEP is a state initiative intended gradually to replace physical legal tender and extend throughout the entire economy.[189] The PBOC, along with the central banks of United Arab Emirates and Thailand, is currently piloting a cross-border foreign-exchange mechanism using DCEP and distributed-ledger technology.[190]

- **Logistics** The 14th Five-Year Plan Modern Circulation Construction Plan, released in January 2022 by the NDRC, represents another blueprint for integrating internal and external "circulation" of data and resources into a China-centered whole.[191] The Party-state's conception of circulation extends beyond traditional logistics to include any channels for resource flow, including digital and financial networks. It states that China should "integrate, analyze, and utilize" all commercial, trade, and circulation big data available through government and social platforms. E-commerce platforms and other enterprises are directed to circulate and share data to support targeted marketing and other digital services. In addition, the plan proposes expanding overseas use of China's Cross-Border Interbank Payment System (CIPS) settlement system and strengthening "supervision" over cross-border financial networks.

- **Autonomous vehicles (AV)** Another NDRC document, the "Strategy for Innovation and Development of Intelligent Vehicles," instructs companies to leverage the strengths of China's "national [innovation] system" and establish an "open source and resource-sharing cooperation mechanism" and "vehicle innovation development platform."[192] This document also directs that AV development support parallel modernization efforts in other areas including digital networks, transportation, and military-civil integration. Beijing's totalizing approach to centralized economic planning means that its instructions are binding for private companies as well as state-owned entities. In addition, the strategy indicates that AV innovation will utilize overseas R&D capabilities and "domestic and foreign innovative factors and market resources," including data.

As PRC companies extend operations internationally, they are increasingly capable of—and supported by the Party-state in—transferring data back into China's growing data ecosystem.

As the documents and initiatives in the previous two sections make clear, the Chinese Communist Party is taking a multipronged approach to achieving supremacy in the control of data, and through that, broader societal and geopolitical control. Ultimately, this means drawing more and more of the world's data resources toward China, while at the same time building systems and technologies that will be needed to store, process, and leverage that data.

5. POLICY RECOMMENDATIONS

Under Xi Jinping's direction, the Party is vigorously competing in what its leaders view as an evolving contest with Washington to become the world's largest data broker. By targeting the data of Americans through commercial means, Xi's offensive campaign—incongruously carried out in the name of "security"—is also fundamentally covert and coercive. Unlike the United States, China has no effective barriers in place to sequester personal data from state espionage and security services.

The same goes for China's commercial partners who, whether offshore or onshore, are claimed by Beijing as being subject to China's data laws, and who are forced to relinquish

control over their data in exchange for access to the Chinese market. One of the most important decisions that other countries can make concerns how to balance demand for China-produced goods and services with data protection for individuals, corporations, and public institutions. The Party's data-control drive cuts across all of these elements of society. It holds them at risk because wherever Xi believes he has leverage, he will use it as part of an overall effort to win the longer-term contest he envisions between socialist and democratic systems. The United States and other democracies urgently need a targeted response to this threat.

This final section of the report lays out a series of policy recommendations to undergird a coherent US counterstrategy. Alongside these policy steps, we must get more broadly serious about scrutinizing the behavior of corporate entities linked to political actors whose stated goals run explicitly counter to US interests.

5.1 ABSORPTION OF DATA THROUGH CROSS-BORDER FLOWS

Solution: Block commercial operations that threaten the security of critical and personal data.

How: More regularly implement the US Department of Commerce's "information and communications technology and services" (ICTS) process to arrest the operations of any foreign adversary–linked commercial entity handling US data. Consider using a sanctions-based list to prohibit applications from specific foreign adversary–linked entities of concern. Increase ICTS resources.

It must be assumed that all data obtained by China-linked companies is visible to PRC authorities and exposed to being appropriated, manipulated, and leveraged for future exploitation.

However, the process for restricting ICTS transactions is also capable of playing a broader role by blocking any data-related activity that poses a clear risk to national security in specific critical sectors.

During the last full day of the Trump administration, the Department of Commerce published an Interim Final Rule implementing the May 2019 Executive Order on the ICTS emergency by establishing a process for interagency review of cross-border data flows. Under the rule, an interagency panel led by the commerce secretary would have broad discretion to investigate, modify, block, or unwind commercial transactions believed to present "undue or unacceptable risks" to US national security.[193]

As set out by the Trump administration, the ICTS panel would be a major new part of the federal regulatory constellation. According to the Department of Commerce's Interim Final Rule, the new ICTS panel has authority across six sectors:

- critical infrastructure, including all sectors designated under the Presidential Policy Directive on Critical Infrastructure Security and Resilience;

- network infrastructure, including satellites, wireless networks, cable access points, and so forth;
- data hosting, including computing services that process sensitive personal information for more than one million US persons;
- surveillance and monitoring technology, including sensors, surveillance equipment, home networking devices, drones, and so forth;
- communications software, including desktop, mobile, web-based, and gaming applications; and
- emerging technology, including AI, machine learning, quantum, autonomous systems, and advanced robotics.[194]

In a moment of bipartisan consensus, in late February 2021, despite concerns from US industry and some US officials, the Biden administration decided to stick with the ICTS panel as outlined by the outgoing Trump administration.[195]

Two years ago, Commerce subpoenaed multiple Chinese ICTS companies in the United States to review transactions under Executive Order 13873.[196] However, since then the Biden administration has taken few steps to actually block "transactions"—a wide category of data-related activity including acquisitions, software installations, hosting, and data transmissions. Though the ICTS process gives Commerce authority to restrict acquisitions and use transactions controlled by "foreign adversaries" including China, Cuba, Iran, North Korea, Russia, and Venezuela, this authority appears to be exercised primarily at the review level, and has not yet advanced to regular implementation.

The Biden administration has expanded the Trump-initiated ICTS process to focus on personal data gathered by connected software applications ("apps"). Under Executive Order 14034 ("Protecting Americans' Sensitive Data from Foreign Adversaries"), the Department of Commerce can take measures to block the current operations of any foreign adversary–linked commercial entity engaging in storage and processing of personal data within US jurisdictions through "connected software applications."[197]

E.O. 14034 represents the expansion of measures set out in the Trump administration's E.O. 13873 declaring a "national emergency" concerning ICTS, and requiring the construction of a new regulatory regime for restricting cross-border data flows to and from "foreign adversary" countries that may threaten national security.[198] In addition, it reiterates the threat posed by China:

> The increased use in the United States of **certain connected software applications designed, developed, manufactured, or supplied by persons owned or controlled by, or subject to the jurisdiction or direction of, a foreign adversary, which the**

> **Secretary of Commerce . . . has defined to include the People's Republic of China, among others**, continues to threaten the national security, foreign policy, and economy of the United States. The Federal Government should evaluate these threats through rigorous, evidence-based analysis and should address any unacceptable or undue risks consistent with overall national security, foreign policy, and economic objectives, including the preservation and demonstration of America's core values and fundamental freedoms.[199]

The Commerce-implemented ICTS framework therefore also serves as the basis for protection of personal information, including health and genetic information, for Americans.

One of the chief risks to the Commerce-led process itself is a lack of resources and clarity of scope. One proposed resolution to this issue is a sanctions-based "list" approach that prohibits applications from specific foreign adversary–linked entities.[200]

5.2 NO PROTECTION FOR DATA OBTAINED BY CHINA-LINKED COMMERCIAL ENTITIES

Solution: Restrict the ability of China-linked companies within the United States to operate in critical supply chain areas.

How: Revamp the Committee on Foreign Investment in the United States (CFIUS) toward a simplified approve/reject model for covered transactions. Update the Foreign Investment Risk Review Modernization Act (FIRRMA) to define specific critical technology areas where new foreign adversary–controlled investment will be reviewed on the basis of presumed denial. Create a review system for cross-border research partnerships involving foreign entity–linked institutions.

The new ICTS regime represents a powerful means of restricting the presence and operations of China-linked companies with access to sensitive American data. Yet currently, CFIUS review of inbound foreign investment represents the most visible—if only sporadically employed—process for screening and identifying data risk posed by China-linked companies operating in the United States.

CFIUS should continue reviewing the activities of China-linked companies for signs of data transfer and misuse.[201] While previous mitigation measures have relied on the appointment of special board members to serve as Government Security Committee members, a more robust monitoring and enforcement mechanism may require the resources of the Department of Homeland Security and Department of Justice, as well as stiffer financial penalties for violations. The Department of Justice and Department of Commerce have recently announced a new Disruptive Technology Strike Force to target threats arising from illicit actors, including from foreign technology investments.[202]

A more action-oriented CFIUS approach would be to move to a simplified approve/reject model for covered transactions linked to foreign-adversary countries. This option would circumvent the current lengthier CFIUS mitigation process. President Biden's E.O. 14017 on supply chain protection and security ("Executive Order on America's Supply Chains") provides clear guidelines for sectors that should be at the top of CFIUS investment screening lists for risks to national security:

- semiconductor manufacturing and advanced-packaging supply chains;
- high-capacity batteries, including electric vehicle (EV) batteries;
- critical minerals and other identified strategic materials, including rare earth elements;
- pharmaceuticals and active pharmaceutical ingredients;
- critical pandemic-related items, including personal protective equipment (PPE); and
- supply chains related to
    - defense industrial base;
    - public health and biological preparedness industrial base;
    - critical sectors and subsectors of the ICT industrial base, including the industrial base for development of ICT software, data, and associated services;
    - energy sector industrial base;
    - transportation industrial base; and
    - agricultural commodities and food products.[203]

Given the sensitivity of each of these areas to industrial espionage, IP theft, and data exfiltration touching on sensitive areas of the economy and national defense, FIRRMA should be updated to define specific areas of "critical infrastructure and technology" in or around each of these supply chains where new foreign adversary–controlled investment will be reviewed on a basis of presumed denial.

Lawmakers should also consider imposing a parallel review, monitoring, and enforcement system for cross-border research partnerships involving foreign adversary–linked institutions.[204]

5.3 EXPLOITING DATA WEAKNESSES IN OPEN SOCIETIES

Solution: Establish common frameworks for coordinating and strengthening data protections.

How: Consider joining democratically minded digital ecosystems. Scrutinize and oppose China's efforts to hollow emerging digital trade standards through multilateral organizations. Create data-protection infrastructure for research partnerships involving foreign adversary–linked institutions.

The United States and like-minded countries should continue to find ways to restrict data sharing with China. Beijing's DSL already blocks most outward data flows from China to other countries. The United States and democratic allies should likewise limit flows to China while continuing to promote secure data sharing among themselves.

Beijing is fully aware that the United States and other democracies are beginning to fill regulatory loopholes concerning digital trade. This is why China's trade negotiators are pushing for entry into the Comprehensive and Progressive Agreement for Trans-Pacific Partnership (CPTPP) and Digital Economy Partnership Agreement (DEPA)—to hollow out emerging digital trade standards as they emerge.[205]

Data Free Flow with Trust (DFFT), proposed by Japan's prime minister Shinzo Abe in 2019, is a promising model for establishing a digital ecosystem based on democratic values that at the same time restricts access by adversaries who undermine those values.

Efforts by congressional lawmakers should focus on addressing shortcomings in restricting the sale and export of data, currently limited to commercial transactions. Research is another important area where more layers of data protection are currently needed to reduce threats posed by the PRC and other adversaries. University and other research partnerships involving foreign adversary–linked institutions and individuals should potentially be subject to the same licensing and review process as required of commercial actors seeking to obtain sensitive and/or personal US data (see above).

5.4 CO-OPTATION AND COERCIVE EXFILTRATION OF DATA HELD BY FOREIGN ENTITIES OPERATING IN CHINA

Solution: Accelerate decoupling in the ICTS domain until Beijing accedes to reciprocity.

How: Increase reporting requirements for US firms operating in China's information environment. Limit US companies from investing in PRC companies engaged in data exfiltration and abuse. Support corporations seeking to relocate operations from China.

The US regulatory environment has changed significantly in the last three years. Policy makers and lawmakers are increasingly skeptical of companies whose presence and

commercial activity in China supports Party agendas of military-civil fusion, "surveillance state" development, human rights abuses, and compromising of IP and trade secrets.

Beijing's policies of data mercantilism put foreign corporations in a position of being forced to choose between complying with legal requirements in the US and facing legal sanctions, and complying with China's Cybersecurity Law, Data Security Law, and Personal Information Protection Law. All of these PRC laws leave corporations and their clients vulnerable to data absorption and theft.

US firms operating in China's information environment should be able to prove to their own government that no non-PRC customer data is exposed to China's authorities, and to disclose in customer contracts any risks of exposure. Technical solutions may also be necessary to render software inoperable if compromised. Consistent reporting by corporations to US policy makers and law enforcement will further improve transparency.

Lawmakers should support the process of accelerated decoupling by establishing clear standards for national security and personal data protection that include restrictions on data sharing in foreign-adversary jurisdictions.

The United States government should provide support and incentives for corporations seeking to relocate their operations from China. In addition, US companies investing in PRC companies engaged in data exfiltration and abuse should be prohibited from similar behavior in the future, possibly through a mechanism similar to the Office of Foreign Assets Control's "Non-SDN Chinese Military-Industrial Complex Companies List" and related Executive Order ("Addressing the Threat from Securities Investments that Finance Certain Companies of the People's Republic of China"), which limit purchase or sale of securities (and derivatives) of companies operating in the defense and surveillance technologies sectors of China's economy.[206]

6. CONCLUSION

This report has examined how China's digital grand strategy represents an underappreciated expansion of China's power into the center of the United States' heartland, with implications for how Americans live their lives, how US companies compete, and how our government protects its citizens and interests both at home and abroad. In the meantime, lack of a coherent US counterstrategy means that even the most critical sectors of our economy have become vulnerable to CCP data appropriation.

It will take considerable resources and resolve to develop robust mechanisms for curtailing the behavior of entities whose ownership may be entirely private, but whose behavior is shaped by political directives from foreign-adversary governments through extralegal and clandestine methods. Traditional tools of analysis honed by the competition between nation-state actors—or targeting transnational terrorist and criminal organizations—are no longer

wholly adequate to the challenge, though they still represent important elements of the response. Each of the policy remedies proposed above relies, ultimately, on the ability of the US government to regularly and comprehensively access information surrounded by barriers of language, political system, and ideological framing. This report seeks to provide a model for how to link different evidentiary chains of Party policy making, industrial-level deployment, corporate organizational structures, and likely and/or demonstrable data-related harms in a way that makes both the drivers and outcomes of Party data ambitions clear. However, as its scope and inevitable analytic leaps attest, evidence of how Beijing accesses and instrumentalizes data flows is equally reliant, if not more so, on forensic analysis of commercial firm behavior.

This is why, if China-linked firms have nothing to hide, their executives and investors will not object to enhanced regulation, monitoring, and law enforcement regarding their operations. It is also why the US policy response needs to move beyond sporadic review to a better resourced, more institutionally coordinated posture. While much of the discussion surrounding this response to date has focused on the issues of future standards for national data security and privacy protection, the mandate already exists *now* to ensure that US supply chains are free of risk from foreign-adversary threats—data-related and otherwise—and Americans' personal data is not being unknowingly exposed to foreign-adversary collection and analysis.

APPENDIX

As the Chinese Communist Party, guided by Xi, has incorporated data into its guiding frameworks for economic development and industrialization, it has also unveiled a series of tactical measures to augment and integrate information networks within China, in order to significantly increase state processing capacity.

Domestically, these measures have included the following:

ACTION FRAMEWORK FOR PROMOTING THE DEVELOPMENT OF BIG DATA (STATE COUNCIL, 2015)

- Calls for developing the use of data as a "national basic strategic resource."
- Emphasizes use of big data for economic competition and social governance, including creation of a "unified social credit system."
- Initiates planning of a national big data infrastructure.
- Authorizes "industrial big data resource aggregation and analysis," including "cross-border internet integration," to facilitate economic transformation.
- Promotes the creation of new "channels" for transfer of scientific research to enterprises.
- Encourages international exchange and cooperation in big data technology, including "making full use of international resources" to promote development of China's big data technologies.
- Guides domestic and international enterprises to work together in R&D, and for internationally competitive enterprises to "support domestic enterprises in global market competition."[207]

BIG DATA INDUSTRY DEVELOPMENT PLAN, 2016–2020 (MINISTRY OF INDUSTRY AND INFORMATION TECHNOLOGY, 2016)

- Describes big data as a national basic strategic resource and the "diamond mine of the twenty-first century."
- Follows China's 13th Five-Year Plan (2016–2020) directive to create a national big data strategy and supporting industry.

- Proposes to "gather global big data technology, talent, and capital" in support of China's big data development, and to "promote the open sharing of data resources and information circulation."

- Sets "application of big data in innovation and entrepreneurship" as a national goal.

- Calls for enterprises to play a leading role in development of "key technologies" for data collection, transmission, storage, management, processing, analysis, application, visualization, and security.

- Authorizes construction of a national "industrial big data architecture" to support industrial policy (e.g., the Made in China 2025 strategy, military-civil integration) and establishment of industrial big data centers.

- Directs enterprises to carry out cross-border R&D and create open big data platforms for industries and scientific research.[208]

Since 2020, these measures have been expanded and superseded by the creation of a new big data industry plan and infrastructural layout:

14TH FIVE-YEAR PLAN BIG DATA INDUSTRY DEVELOPMENT PLAN (MINISTRY OF INDUSTRY AND INFORMATION TECHNOLOGY, 2021)

- Describes data as an "important factor of production and national basic strategic resource" and a "new driving force for promoting economic transformation and development."

- Acknowledges the formation of nationally integrated big data centers, an interministerial meeting system to promote the development of big data, and big data management agencies and promotion bodies.

- Calls for China to "seize the commanding heights of the big data industry" and "seize first-mover advantage" in linking big data to other emerging technologies.

- Directs sharing of data resources to promote industrial transformation and "upgrade government governance efficiency."

- Outlines goals to create a multilevel "national industrial base database" to promote data use across regions and industries through the comprehensive collection and cataloging of all available data.

- Authorizes the creation of industry platforms serving "government, society, and enterprises," and instructs enterprises to participate in collaborative "government-industry-university-research institution" joint R&D efforts.

- Plans for stronger ties between Chinese and foreign big data standardization and research organizations, and introduction of more foreign R&D into China.

- Mandates use of national coordination mechanisms, technology transfer, and government funding to promote local big data transformation.[209]

NOTES

1. Matt Pottinger and David Feith, "The Most Powerful Data Broker in the World Is Winning the War against the US," *New York Times*, November 30, 2021, https://www.nytimes.com/2021/11/30/opinion/xi-jinping-china-us-data-war.html.

2. "努力成为世界主要科学中心和创新高地" [Strive to Become an Important World Scientific Center and Innovation Highland], speech given May 28, 2018, *Qiushi*, March 15, 2021, https://archive.ph/pC0k7.

3. Original text: "浩瀚的数据海洋就如同工业社会的石油资源，蕴含着巨大生产力和商机，谁掌握了大数据技术，谁就掌握了发展的资源和主动权." "受权发布：《习近平关于科技创新论述摘编》（六）牢牢把握科技进步大方向" [Authorized Release: Excerpts from Xi Jinping's Discourses on Science and Technology Innovation (6) Firmly Grasp the General Direction of Scientific and Technological Progress], CCP News Net, March 30, 2016, https://archive.ph/gxeZt.

4. "中央网络安全和信息化领导小组第一次会议召开" [The First Meeting of the Central Leading Group on Cybersecurity and Informatization Was Held], PRC Central People's Government, February 27, 2014, http://archive.today/sSBbx.

5. "习近平在网信工作座谈会上的讲话全文发表" [Xi Jinping's Speech at the Cybersecurity and Informatization Work Conference Published in Full], Xinhua, April 25, 2016, https://archive.ph/hnnFI.

6. "习近平: 加快推进网络信息技术自主创新 朝着建设网络强国目标不懈努力" [Xi Jinping: Accelerate the Independent Innovation of Network Information Technology and Make Tireless Efforts toward the Goal of Building a Network Great Power], Xinhua, October 9, 2016, https://archive.ph/tBTNY.

7. "国务院办公厅关于运用大数据加强对市场主体服务和监管的若干意见" [Some Opinions of the General Office of the State Council on the Use of Big Data to Strengthen the Service and Supervision of Market Entities], MIIT, July 2, 2015, https://web.archive.org/web/20180213232922/http://www.miit.gov.cn/n1146290/n1146392/c3299036/content.html.

8. "国务院关于印发促进大数据发展行动纲要的通知" [Notice on the State Council Issuance of the Big Data Development Action Plan], PRC Central People's Government, September 5, 2015, https://archive.ph/p6U7g.

9. "习近平总书记在网络安全和信息化工作座谈会上的讲话" [General Secretary Xi Jinping's Speech at the Cybersecurity and Informatization Work Conference], Xinhua, April 25, 2016, https://archive.ph/LKQJZ.

10. "关于印发网络产品安全漏洞管理规定的通知" [Notice on the Issuance of Network Products Security Vulnerability Management Regulations], PRC Central People's Government, July 12, 2021, https://archive.ph/rGsY1.

11. "深刻理解和把握"新的伟大斗争"" [Deeply Understand and Grasp the "New Great Struggle"], *People's Daily*, July 23, 2014, https://perma.cc/XQU5-YPHN.

12. "习近平: 高举中国特色社会主义伟大旗帜 为全面建设社会主义现代化国家而团结奋斗——在中国共产党第二十次全国代表大会上的报告" [Xi Jinping: Holding High the Great Banner of Socialism with Chinese Characteristics and Uniting and Striving for the Comprehensive Construction of a Socialist Modernized Country—Report at the 20th National Congress of the Chinese Communist Party], Xinhua, October 25, 2022, https://archive.ph/dCWzW.

13. "我国构建数据新型要素市场体系面临的挑战与对策" [Challenges and Countermeasures for Building a New Factor Market System for Data in China], National Information Center Big Data Department, March 10, 2020, https://archive.ph/e9wHK.

14. See Ian Easton, *The Final Struggle: Inside China's Global Strategy* (Manchester, UK: Eastbridge, 2022).

15. Statement of William R. Evanina, CEO, The Evanina Group, before the Senate Select Committee on Intelligence at a Hearing concerning the Comprehensive Threat to America Posed by the Communist Party of China (CCP), August 4, 2021, https://www.intelligence.senate.gov/sites/default/files/documents/os-bevanina-080421.pdf.

16. The State Strategic Advisory Committee for Building China into a Manufacturing Superpower, "Roadmap of Major Technical Domains for Made in China 2025," Center for Security and Emerging Technology, October 29, 2015, https://cset.georgetown.edu/wp-content/uploads/t0181_Made_in_China_roadmap_EN.pdf.

17. The State Strategic Advisory Committee, "Roadmap."

18. Elsa Kania and Rogier Creemers, "Xi Jinping Calls for 'Healthy Development' of AI (Translation)," *New America*, November 5, 2018, https://www.newamerica.org/cybersecurity-initiative/digichina/blog/xi-jinping-calls-for-healthy-development-of-ai-translation.

19. Original quote: "We should focus on this new development path, and push for deep integration between big data and the real economy." Matt Ho, "Xi Jinping Sends Message on Growth through Innovation, Big Data in Guizhou," *South China Morning Post*, February 9, 2021, https://www.scmp.com/news/china/politics/article/3121055/xi-jinping-sends-message-growth-through-innovation-big-data; and Kania and Creemers, "Xi Jinping Calls."

20. "国务院办公厅关于运用大数据加强对市场主体服务和监管的若干意见" [Some Opinions of the General Office of the State Council].

21. "中华人民共和国国民经济和社会发展第十四个五年规划和2035年远景目标纲要" [Outline of the People's Republic of China National Economic and Social Development 14th Five-Year Plan and 2035 Long-Range Goals], Xinhua, March 13, 2021, https://archive.ph/ZTF2U.

22. "The Chinese Communist Party's Military-Civil Fusion Policy," US Department of State, n.d., https://2017-2021.state.gov/military-civil-fusion/index.html.

23. Elizabeth Chen, "Rapidly Implementing a Chinese Data Security Regime," The Jamestown Foundation, July 16, 2021, https://jamestown.org/program/rapidly-implementing-a-chinese-data-security-regime/; and "国家互联网信息办公室关于《网络安全审查办法（修订草案征求意见稿）》公开征求意见的通知" [Cyberspace Administration of China Notice of Public Consultation, "Network Security Review Approach," Revised Draft for Public Comment], Cyberspace Administration of China, July 10, 2021, https://archive.ph/nOFd6.

24. See "中办、国办印发《关于依法从严打击证券违法活动的意见》" [Some Opinions of the General Office of the Central Committee and the General Office of the State Council on the Use of the Law to Severely Crack Down on Illegal Securities Activities], Xinhua, July 6, 2021, https://archive.ph/nntG8.

25. "习近平出席全国网络安全和信息化工作会议并发表重要讲话" [Xi Jinping Delivers an Important Speech at the Cyberspace Administration of China Meeting], Xinhua, April 21, 2018, https://archive.ph/hkCni.

26. "中央网信办召开互联网企业党建工作现场会" [Cyberspace Administration of China Held a Meeting on Party Building in Internet Corporations], Office of the Central Cyberspace Affairs Commission, October 26, 2016, https://archive.vn/Lvs8W.

27. "习近平: 自主创新推进网络强国建设" [Xi Jinping: Independently Innovate to Advance the Creation of a Strong Internet Nation], Xinhua, April 21, 2018, https://archive.ph/5PBwo.

28. "习近平: 自主创新推进网络强国建设" [Xi Jinping: Independently Innovate].

29. "华大基因汪建:大数据云计算支撑下的基因产业没有冬天" [BGI cofounder Wang Jian: "In an industry supported by scientific development, big technology platforms, and big data, there is no off-season"], ScienceNet.cn, December 20, 2012, http://archive.today/Ae0Lj.

30. "DNA Sequencing Services," BGI, https://web.archive.org/web/20220123181753/https://www.bgi.com/global/dna-sequencing.

31. China National GeneBank [国家基因库] home page, archived December 24, 2021, http://archive.today/F6KKI.

32. "林念修副主任出席国家基因库理事会第一次会议并赴华大基因研究院调研" [NDRC Deputy Director Lin Nianxiu Attended the First Meeting of the China National GeneBank Council and Visited BGI], NDRC, November 20, 2015, http://archive.today/OKZYn.

33. China National GeneBank [国家基因库] home page; and "林念修副主任出席国家基因库理事会第一次会议并赴华大基因研究院调研" [NDRC Deputy Director Lin Nianxiu].

34. "林念修副主任出席国家基因库理事会第一次会议并赴华大基因研究院调研" [NDRC Deputy Director Lin Nianxiu].

35. "Children's Hospital of Philadelphia and BGI Partner to Launch Joint Genome Center," Fierce Biotech, November 12, 2011, https://www.fiercebiotech.com/biotech/children-s-hospital-of-philadelphia-and-bgi-partner-to-launch-joint-genome-center.

36. Children's Hospital of Philadelphia, "BGI and the Children's Hospital of Philadelphia Launch the 1,000 Rare Diseases Project to Advance Gene Discovery," Cision PR Newswire, June 18, 2012, https://www.prnewswire.com/news-releases/bgi-and-the-childrens-hospital-of-philadelphia-launch-the-1000-rare-diseases-project-to-advance-gene-discovery-159410855.html.

37. "BGI Partners with NRGene to Provide Broadest Genomic Analysis Available," AgNews, August 16, 2016, https://news.agropages.com/News/NewsDetail---19011.htm.

38. Staff reporter, "BGI Partners with Johns Hopkins, Mount Sinai Hospital; Plans to Place First BGISEQ in North America," GenomeWeb, May 4, 2018, https://www.genomeweb.com/sequencing/bgi-partners-johns-hopkins-mount-sinai-hospital-plans-place-first-bgiseq-north-america.

39. Jeanne Whalen and Elizabeth Dwoskin, "California Rejected Chinese Company's Push to Help with Coronavirus Testing. Was That the Right Move?" *Washington Post*, July 2, 2020, https://www.washingtonpost.com/business/2020/07/02/china-bgi-california-testing.

40. "Addition of Certain Entities to the Entity List; Revision of Existing Entries on the Entity List," Federal Register, National Archives, July 22, 2020, https://www.federalregister.gov/documents/2020/07/22/2020-15827/addition-of-certain-entities-to-the-entity-list-revision-of-existing-entries-on-the-entity-list.

41. "Statement Regarding BGI's Subsidiaries Being Added to US's Entity List," BGI, July 24, 2020, https://archive.ph/jlThj.

42. Natera, Inc., "Natera and BGI Genomics Announce Commercial Launch of the BGI/Natera Signatera Assay in China," Cision PR Newswire, June 24, 2021, https://www.prnewswire.com/news-releases/natera-and-bgi-genomics-announce-commercial-launch-of-the-bginatera-signatera-assay-in-china-301319176.html.

43. Clare Baldwin and Kirsty Needham, "BGI Prenatal Gene Test under Scrutiny for Chinese Military Links," Reuters, September 7, 2021, https://www.reuters.com/world/china/bgi-prenatal-gene-test-under-scrutiny-chinese-military-links-2021-09-06.

44. "从克隆猪研发骨干 到"健康中国"践行者" [From Cloning Pigs to Building a Healthy China], Southern Daily via CCP News, October 7, 2017, https://archive.fo/jFRuZ.

45. "深圳华大基因股份有限公司投资者关系活动记录表" [BGI Investor Relations Report], BGI, 2019, https://archive.ph/3oPnX; and "深圳华大基因股份有限公司2018年度社会责任报告" [BGI 2018 Social Responsibility Report], BGI, https://web.archive.org/web/20190701182701/https://www.bgi.com/wp-content/uploads/2019/04/%E5%8D%8E%E5%A4%A7%E5%9F%BA%E5%9B%A0%EF%BC%9A2018%E5%B9%B4%E5%BA%A6%E7%A4%BE%E4%BC%9A%E8%B4%A3%E4%BB%BB%E6%8A%A5%E5%91%8A.pdf.

46. "药明康德上交所挂牌 "回A"" [WuXi Biologics Listing "Returns to A"], *People's Daily*, May 8, 2018, http://archive.today/GrEvH.

47. "WuXi AppTec Listing," Bloomberg, https://www.bloomberg.com/quote/2359:HK; "【看点】2020年中国医药工业百强榜发布" [China's 2020 Top 100 Pharmaceutical Companies List Released], Sohu, July 23, 2021, http://archive.today/cCE9P; "Global Offering," WuXi AppTec, https://www1.hkexnews.hk/listedco/listconews/sehk/2018/1203/ltn20181203003.pdf; and "Fortune Future 50 2021 List," *Fortune*, https://fortune.com/future-50/2021/search.

48. "关于我们" [About Us], Communist Party Member Net, http://archive.today/0Q7Jd; and "甘当创新发展"催化剂"——记药明康德众党员" [WuXi Biologics Party Members—A Catalyst for Innovation and Development], Communist Party Member Net, May 25, 2013, http://archive.today/tJFvS.

49. “【云客厅】当药明生物周伟昌遇上默克Daniel Stamm” [WuXi Biologics’ Zhou Weicheng Met Merck’s Daniel Stamm], Antpedia, November 20, 2019, http://archive.today/kaKjn; “建立国际水平的生物药一体化平台推动全球医药创新：生物药中国“智”造的故事” [Building an International-Standard Integrated Platform for Biologics to Promote Global Pharmaceutical Innovation: The Story of Chinese “Smart” Biologic Manufacturing], Tsinghua University Department of Chemical Engineering, May 28, 2018, http://archive.today/F1NHs; “陈薇、陈智胜为本科新生讲授“生物医药与健康产业” [Chen Wei and Chen Zhisheng Lectured to Undergraduate Students on Biomedical and Health Industries], Tsinghua University News, December 26, 2018, http://archive.today/mIlhU; “关于成立“重大新药创制”和“艾滋病和病毒性肝炎等重大传染病防治”两个科技重大专项“十三五”总体组的通知” [Notice on the Establishment of Two Major Science and Technology Advisory Committees for the 13th Five-Year Plan: “Major Drug Innovation” and “AIDS, Hepatitis, and Major Infectious Diseases Prevention and Treatment”], National Health Commission of the People’s Republic of China, November 25, 2016, http://archive.today/ipCfJ; “上海留学人员人才网” [Shanghai Overseas Returned Scholars Association Website], archived December 2, 2021, http://archive.today/9njNi; Alex Joske, “Hunting the Phoenix,” Australian Strategic Policy Institute, https://www.aspi.org.au/report/hunting-phoenix; ““千人计划” 专家联谊会成立” [Thousand Talents Expert Association Established], January 16, 2011, npc.gov.cn, http://archive.today/6e5MM; “【人物肖像】杖黎行歌, 积健为雄——记总会理事, 药明康德副总裁黎健” [Profile: Jian Lai, a Member of the Board of Directors of WuXi Biologics and Vice President of WuXi Biologics], Shanghai Overseas Returned Scholars Association, June 2, 2016, http://archive.today/ojp2j; China Pharmaceutical Innovation and Research Development Association, 2015-2016 Association Journal, archived August 17, 2018, via https://web.archive.org/web/20190309210752/http://www.phirda.com/upload/download/%E4%B8%AD%E5%9B%BD%E8%8D%AF%E4%BF%83%E4%BC%9A2015-2016%E4%BC%9A%E5%88%8A.pdf; and “中国医药创新促进会章程” [Bylaws of the China Pharmaceutical Innovation and Research Development Association], archived August 12, 2020, https://web.archive.org/web/20200812020003/http://www.phirda.com/about_2.html.

50. “Huawei and WuXi Join Forces to Create China Precision Medicine Cloud Platform,” WXPress, March 17, 2016, http://archive.today/qTcrK.

51. “明码云助精准医疗走进现实” [Cloud Helps Bring Precision Medicine to Life], Huawei website, archived November 30, 2021, http://archive.today/jPrlV.

52. “国家重点研发计划“精准医学大数据处理和利用的标准化技术体系建设”,“精准医学大数据管理和共享技术平台”联合召开项目启动会” [The National Key Research and Development Program of China Projects on “Standardized Technical System Construction for Processing and Utilization of Precision Medicine Big Data” and “Platforms for Management and Sharing of Precision Medicine Big Data” Held a Joint Project Kickoff Meeting], Beijing Institute of Genomics, Chinese Academy of Sciences, December 8, 2016, http://archive.today/yoy5X.

53. “中电数据服务有限公司” [CEC Data Services], accessed March 16, 2023, https://aiqicha.baidu.com/company_detail_30265579092520; and “中国国有企业结构调整基金股份有限公司” [China State-Owned Enterprise Structure Adjustment Fund], accessed March 16, 2023, https://aiqicha.baidu.com/company_detail_15743248697725.

54. “China Electronics Data and WuXi AppTec Form CW Data, a Joint Venture to Offer One-Stop Healthcare Big Data Solutions,” WuXi AppTec, October 22, 2018, http://archive.today/H2ek3.

55. Office of Foreign Assets Control, “Non-SDN Chinese Military-Industrial Complex Companies List,” Department of the Treasury, December 16, 2021, https://www.treasury.gov/ofac/downloads/ccmc/nscmiclist.pdf.

56. “Protecting Critical and Emerging US Technologies from Foreign Threats,” National Counterintelligence and Security Center, October 2021, https://www.dni.gov/files/NCSC/documents/SafeguardingOurFuture/FINAL_NCSC_Emerging%20Technologies_Factsheet_10_22_2021.pdf.

57. Julian E. Barnes, “US Warns of Efforts by China to Collect Genetic Data,” *New York Times*, October 22, 2021, https://www.nytimes.com/2021/10/22/us/politics/china-genetic-data-collection.html.

58. “2021 Annual Report to Congress,” US-China Economic and Security Review Commission, November 2021, https://www.uscc.gov/annual-report/2021-annual-report-congress, 178, 252.

59. ByteDance website, https://www.bytedance.com/en.

60. “抖音有限公司” [Douyin Co., Ltd.], Baidu Aiqicha, archived June 10, 2022, https://archive.ph/NU1jC.

61. “Beijing Owns Stakes in ByteDance, Weibo Domestic Entities, Records Show,” Reuters, August 16, 2021, https://www.nasdaq.com/articles/beijing-owns-stakes-in-bytedance-weibo-domestic-entities-records-show-2021-08-17.

62. “抖音抖出违规问题线索, 中纪委机关报：群众是最强的监督力量” [Douyin Shakes Out Clues to Irregularities, the Central Committee for Discipline Inspection Reports: The Masses Are the Strongest Supervisory Force], China Discipline Inspection News, November 11, 2020, https://archive.ph/iks9K; and “抖音抖出线索群众监督给力” [Douyin Shakes Out Clues to Give Power to Mass Supervision], Central Committee for Discipline Inspection, November 11, 2020, https://archive.ph/2v4N2.

63. “重磅! 公安部与抖音正式合作” [Important: Ministry of Public Security and Douyin Formally Collaborate], Southern Network, April 26, 2019, https://archive.ph/TM7E5.

64. “字节跳动党委书记张辅评: 抖音打造 “警务亲民” 新模式” [ByteDance Party Secretary Zhang Fuping: ByteDance Initiates New Program to Warn the Police on Behalf of the People], Guangming Online, September 14, 2018, https://archive.ph/VRNBJ.

65. Emily Baker-White, “TikTok Is Bleeding US Execs because China Is Still Calling the Shots, Ex-employees Say,” Forbes, September 21, 2022, https://www.forbes.com/sites/emilybaker-white/2022/09/21/tiktok-bleeding-us-execs-china-control-bytedance.

66. Emily Baker-White, “LinkedIn Profiles Indicate 300 Current TikTok and ByteDance Employees Used to Work for Chinese State,” Forbes, August 11, 2022, https://www.forbes.com/sites/emilybaker-white/2022/08/10/bytedance-tiktok-china-state-media-propaganda.

67. Emily Baker-White, “Leaked Audio from 80 Internal TikTok Meetings Shows that US User Data Has Been Repeatedly Accessed from China,” BuzzFeed News, June 17, 2022, https://www.buzzfeednews.com/article/emilybakerwhite/tiktok-tapes-us-user-data-china-bytedance-access.

68. “TikTok, Snapchat, YouTube Executives Testify in Senate Hearing about Kids’ Safety Online,” PBS NewsHour, October 26, 2021, https://www.youtube.com/watch?v=HnH6HuFU6hI&ab_channel=PBSNewsHour.

69. Letter from TikTok to US Senators Marsha Blackburn, John Thune, Ted Cruz, Shelley Moore Capito, Steve Daines, Roger Wicker, Roy Blunt, Jerry Moran, and Cynthia Lummis, June 30, 2022, https://www.blackburn.senate.gov/services/files/A5027CD8-73DE-4571-95B0-AA7064F707C1.

70. “北京成立智源人工智能研究院” [Beijing Establishes Artificial Intelligence Research Institute], People’s Network, November 14, 2018, https://archive.ph/RgMuO; “Addition of Certain Entities to the Entity List,” Industry and Security Bureau via Federal Register, October 9, 2019, https://archive.ph/HhyU6; and “Treasury Identifies Eight Chinese Tech Firms as Part of the Chinese Military-Industrial Complex,” US Department of the Treasury, December 16, 2021, https://home.treasury.gov/news/press-releases/jy0538.

71. “Treasury Identifies Eight Chinese Tech Firms”; and “Addition of Certain Entities to the Entity List.”

72. Felix Krause, “iOS Privacy: Announcing InAppBrowser.com,” blog post, August 18, 2022, https://krausefx.com/blog/announcing-inappbrowsercom-see-what-javascript-commands-get-executed-in-an-in-app-browser.

73. “TikTok Admits Tracking FT Journalist in Leaks Investigation,” *Financial Times*, December 23, 2022, https://www.ft.com/content/e873b98a-9623-45b3-b97c-444a2fde5874; and Emily Baker-White, “EXCLUSIVE: TikTok Spied on Forbes Journalists,” *Forbes*, December 22, 2022, https://www.forbes.com/sites/emilybaker-white/2022/12/22/tiktok-tracks-forbes-journalists-bytedance/?sh=24c71c2e7da5.

74. "Worldwide Threats to the Homeland," House Homeland Security Committee, November 15, 2022, https://docs.house.gov/Committee/Calendar/ByEvent.aspx?EventID=115183.

75. "Fireside Chat with DNI Haines at the Reagan National Defense Forum," Office of the Director of National Intelligence, December 12, 2022, https://www.dni.gov/index.php/newsroom/news-articles/news-articles-2022/item/2346-fireside-chat-with-dni-haines-at-the-reagan-national-defense-forum.

76. Baker-White, "Leaked Audio from 80 Internal TikTok Meetings"; and Lauren Hirsch, David McCabe, Katie Benner, and Glenn Thrush, "TikTok Seen Moving toward US Security Deal, but Hurdles Remain," *New York Times*, September 26, 2022, https://www.nytimes.com/2022/09/26/technology/tiktok-national-security-china.html.

77. Brendan Bordelon and Gavin Bade, "Senate, White House Push New Bipartisan Bill that Could Ban TikTok," Politico, March 7, 2023, https://www.politico.com/news/2023/03/07/senate-white-house-tiktok-ban-00085998.

78. *Global Drone Market Report 2022–2030*, Drone Industry Insights, March 14, 2023, https://droneii.com/product/drone-market-report.

79. "Game of Drones: Drone Startup Funding Hits High. Have Raised More in 2015 than Last 3 Years Combined," CB Insights, May 31, 2015, https://www.cbinsights.com/research/drone-startup-venture-capital.

80. Wang Ying, "DJI Sees Jump in Revenue," *China Daily*, December 13, 2016, https://www.chinadaily.com.cn/business/tech/2016-12/13/content_27649387.htm.

81. Cate Cadell, "Drone Company DJI Obscured Ties to Chinese State Funding, Documents Show," *Washington Post*, February 1, 2022, https://www.washingtonpost.com/national-security/2022/02/01/china-funding-drones-dji-us-regulators.

82. "Global Commercial Drones Market Report 2022: Favourable Government Policies and Guidelines Present Opportunities," Research and Markets, Global Newswire, Yahoo.com, November 21, 2022, https://www.yahoo.com/now/global-commercial-drones-market-report-104800958.html.

83. Gina Chon, "DJI Is a More Elusive US Target than Huawei," Reuters, December 16, 2021, https://www.reuters.com/markets/asia/dji-is-more-elusive-us-target-than-huawei-2021-12-17; and David Benowitz, "2021 Drone Market Sector Report," DroneAnalyst, n.d., https://da21-summary.netlify.app.

84. "深圳市道通智能航空技术股份有限公司" [Shenzhen Daotong Intelligent Aviation Technology Co., Ltd.], accessed March 16, 2023, https://aiqicha.baidu.com/company_detail_99343256093607.

85. "会员单位" [Member Units], Shenzhen UAV Industry Association, July 1–3, 2022, https://web.archive.org/web/20220606200415/http://www.szuavia.org/vip_cen.php?cid=30.

86. "会长致词" [Association President's Greetings], Shenzhen UAV Industry Association, archived March 28, 2023, https://archive.ph/yn1XD.

87. "组织机构" [Organizational Structure], 2022 China International UAV Systems Industry Exhibition, archived September 14, 2022, https://archive.ph/uMraN.

88. "同期举办民营无人机企业参军建设交流会" [An Exchange Meeting for Private UAV Enterprises to 'Join the Army' Will Be Held], 2022 China International UAV Systems Industry Exhibition, archived September 14, 2022, https://archive.ph/QdHB8.

89. "深圳南山 党组织建在产业链上 无人机产业飞得更高" [Shenzhen Nanshan Party Organizations Built in the Industry Chain—The Drone Industry Flies Higher], Tencent, December 22, 2021, https://archive.ph/wLopv.

90. Hannah Leyva, "Wrightsville Beach to Begin Using a Drone for Emergency Responses," *Port City Daily*, September 9, 2016, https://portcitydaily.com/local-news/2016/09/09/wrightsville-beach-to-begin-using-a-drone-for-emergency-responses.

91. Zachary Evans, "Chinese Company Suspected of Spying on US Citizens Donates Police Drones to 22 States," *National Review*, April 20, 2020, https://www.nationalreview.com/news/chinese-company-suspected-of-spying-on-u-s-citizens-donates-police-drones-to-22-states.

92. Dan Gettinger, "Public Safety Drones, 3rd Edition," Center for the Study of the Drone at Bard College, March 2020, https://dronecenter.bard.edu/files/2020/03/CSD-Public-Safety-Drones-3rd-Edition-Web.pdf.

93. Jeff Daniels, "US Army Reportedly Bans Chinese-Made Drone, Citing 'Cyber Vulnerabilities,'" CNBC, August 4, 2017, updated August 5, 2017, https://www.cnbc.com/2017/08/04/us-army-bans-chinese-made-drone-citing-cyber-vulnerabilities.html.

94. Brian Naylor, "'We're Not Being Paranoid': US Warns of Spy Dangers of Chinese-Made Drones," NPR, May 29, 2019, https://www.npr.org/2019/05/29/727612692/we-re-not-being-paranoid-u-s-warns-of-spy-dangers-of-chinese-made-drones.

95. "DJI Refuses to Apply Geofencing in Ukraine," UAS Vision, n.d., https://www.uasvision.com/2022/03/23/dji-refuses-to-apply-geofencing-in-ukraine.

96. "Russland verhandelt offenbar mit China über die Lieferung von Kamikazedrohnen" [Russia Apparently Negotiating with China on the Supply of Kamikaze Drones], *Der Spiegel*, February 23, 2023, https://archive.ph/hCoWS.

97. "DJI AeroScope," DJI, n.d., https://www.dji.com/aeroscope.

98. Sean Hollister, "DJI Insisted Drone-Tracking AeroScope Signals Were Encrypted—Now It Admits They Aren't," *The Verge*, April 28, 2022, https://www.theverge.com/2022/4/28/23046916/dji-aeroscope-signals-not-encrypted-drone-tracking; and Lars Erik Schönander, "The US Government Is Funding Chinese Spy Technology in America's Backyard," *Tablet*, January 29, 2023, https://www.tabletmag.com/sections/news/articles/government-funds-chinese-spy-technology-americas-backyard.

99. Jamie Tarabay and Coco Liu, "Obscure Cyber Agency Becomes Nemesis of China's Tech Giants," Bloomberg, July 13, 2021, https://www.bloomberg.com/news/articles/2021-07-13/xi-elevates-an-obscure-china-regulator-to-take-on-didi-big-tech.

100. "China Plans to Ban Overseas IPOs for Tech Firms with Data Security Risks—Source," Reuters, August 27, 2021, https://www.reuters.com/technology/china-plans-ban-us-ipos-data-heavy-tech-firms-wsj-2021-08-27.

101. Xinmei Shen and Coco Feng, "Data Privacy in China: Beijing to Define Data that Will Not Be Allowed to Leave the Country Easily," *South China Morning Post*, August 2, 2021, https://www.scmp.com/tech/policy/article/3143532/data-privacy-china-beijing-define-data-will-not-be-allow-leave-country; and "网络安全审查办公室关于对 "滴滴出行" 启动网络安全审查的公告" [Announcement on the Start of the Internet Security Investigation into "DiDi" by the Cybersecurity Review Office], CAC, July 2, 2021, https://archive.md/vvHEx.

102. "网络安全审查办公室关于对 "运满满" "货车帮" "BOSS直聘" 启动网络安全审查的公告" [Announcement on the Start of the Internet Security Investigation into "Full Truck Alliance" and "BOSS Zhipin" by the Cybersecurity Review Office], CAC, July 5, 2021, https://archive.md/c6Tfq.

103. "五部门联合约谈11家网约车平台公司" [Five Departments Jointly Interview 11 Online Car Platform Companies], Ministry of Transport via CAC, September 2, 2021, https://archive.md/nm6YL.

104. "关于印发《关于加强互联网信息服务算法综合治理的指导意见》的通知" [Notice on the Issuance of the "Guidance on Strengthening the Comprehensive Governance of the Internet Information Service Algorithm"], CAC, September 29, 2021, https://archive.ph/Jx0Tq.

105. "工业和信息化部 国家互联网信息办公室 公安部关于印发网络产品安全漏洞管理规定的通知" [Notice of the Ministry of Industry and Information Technology, Cyberspace Administration of China, and the Ministry of Public Security on the Issuance of Regulations on the Management of Security Vulnerabilities in Network Products], CAC, July 13, 2021, https://archive.md/9cL8j.

106. Juro Osawa and Shai Oster, "Beijing Tightens Grip on ByteDance by Quietly Taking Stake, China Board Seat," The Information, August 16, 2021, https://www.theinformation.com/articles/beijing-tightens-grip-on-bytedance-by-quietly-taking-stake-china-board-seat.

107. Yingzhi Yang and Brenda Goh, "Beijing Took Stake and Board Seat in Key ByteDance Domestic Entity This Year," Reuters, August 17, 2021, https://www.reuters.com/world/china/beijing-owns-stakes-bytedance-weibo-domestic-entities-records-show-2021-08-17.

108. "习近平在全国网络安全和信息化工作会议上强调 敏锐抓住信息化发展历史机遇 自主创新推进网络强国建设" [Xi Jinping Stressed at the National Conference on Network Security and Informatization that It Is Important to Seize the Historic Opportunity of Information Development and Promote the Construction of a Strong Network through Independent Innovation], Xinhua, April 21, 2018, https://archive.md/Ic8TQ.

109. "国家互联网信息办公室" [Cyberspace Administration of China], CAC, August 1, 2014, https://archive.md/ZQ5GI.

110. Other Xi-chaired commissions created in 2018 include the Central Comprehensively Deepening Reform Commission, the Central Financial and Economic Affairs Commission, and the Central External Affairs Work Commission.

111. "国家数据局成立在即" [The Establishment of the National Data Bureau Is Imminent], Sohu, March 14, 2023, https://web.archive.org/web/20230316235948/https://www.sohu.com/a/654016886_137462.

112. "习近平在中共中央政治局第三十四次集体学习时强调 把握数字经济发展趋势和规律 推动我国数字经济健康发展" [At the 34th Collective Study Meeting of the Politburo Xi Jinping Emphasized Grasping the Development Trends and Laws of the Digital Economy and Promoting the Healthy Development of China's Digital Economy], Xinhua, October 19, 2021, https://archive.ph/s9gZN.

113. See, e.g., "'三高' 全面发展进行时：必须发挥新型举国体制优势" [The "Three Highs" Comprehensive Development Is Underway: We Must Give Play to the Advantages of the New National System], China Aerospace Science and Technology Corporation, June 17, 2022, https://archive.ph/bCXID.

114. "习近平在中共中央政治局第三十四次集体学习时强调 把握数字经济发展趋势和规律 推动我国数字经济健康发展" [At the 34th Collective Study Meeting of the Politburo Xi Jinping Emphasized Grasping the Development Trends and Laws of the Digital Economy and Promoting the Healthy Development of China's Digital Economy], Xinhua, October 19, 2021, https://archive.ph/s9gZN (emphasis added).

115. "商务部 中央网信办 发展改革委关于印发《"十四五"电子商务发展规划》的通知" [Ministry of Commerce, Central Cybersecurity and Informatization Commission Office, and National Development and Reform Commission Notice on Issuance of the 14th Five-Year Plan Electronic Commerce Development Plan], Ministry of Commerce via CAC, October 26, 2021, http://www.cac.gov.cn/2021-10/26/c_1636843216727631.htm.

116. China's "social credit system" (社会信用体系) is a data-driven tool of social management whose existence has been verified repeatedly by experts on the Party's Leninist control systems, despite contravening claims that its construction at the national level remains hypothetical or incomplete. See Samantha Hoffman, "Social Credit: Technology-Enhanced Authoritarian Control with Global Consequences," Australian Strategic Policy Institute, 2018, https://s3-ap-southeast-2.amazonaws.com/ad-aspi/2018-06/Social%20credit_1.pdf?VersionId=O3X2xnkGONvJFjK4Z57Xbf06lget_MID.

117. "商务部 中央网信办 发展改革委, "'十四五' 电子商务发展规划" [14th Five-Year Plan Electronic Commerce Development Plan].

118. "江苏省商务厅贯彻 "十四五" 电子商务发展规划实施方案" [Jiangsu Provincial Department of Commerce to Implement the 14th Five-Year Plan for the Development and Implementation of Electronic Commerce"], Jiangsu Commercial Office, July 20, 2022, https://archive.ph/iidel; "重庆市商务委员会关于印发重庆市 "十四五" 电子商务发展规划的通知" [Chongqing Municipal Commission of Commerce on the Issuance of Chongqing 14th Five-Year Plan E-commerce Development Plan Notice], Chongqing Commercial Committee, December 31, 2021, https://archive.ph/FQdCj; and "湖南省商务厅关于印发《湖南省 "十四五" 电子商务发展规划》的通知" [Hunan Provincial Department of Commerce on the Issuance of the 14th Five-Year Plan E-commerce Development Plan of Hunan Province], Hunan Commercial Office, January 21, 2022, https://archive.ph/oZoau.

119. “中央网络安全和信息化领导小组第一次会议召开” [The First Meeting of the Central Cybersecurity and Informatization Leading Small Group Was Held], Xinhua, February 27, 2014, https://archive.ph/sSBbx.

120. “习近平的6个“互联网思维”” [Xi Jinping’s Six “Internet Mind-Sets”], *People’s Daily*, November 20, 2014, http://archive.today/w2dDF.

121. “在贵州调研时的讲话” [Speech during Investigation in Guizhou], *People’s Daily*, June 19, 2015, https://web.archive.org/web/20200525171229/http://scitech.people.com.cn/n1/2016/0304/c1007-28171614.html.

122. See also Rogier Creemers et al., “Lexicon: 网络强国 Wǎngluò Qiángguó,” DigiChina, Stanford University, May 31, 2018, https://digichina.stanford.edu/work/lexicon-%E7%BD%91%E7%BB%9C%E5%BC%BA%E5%9B%BD-wangluo-qiangguo.

123. “习近平在网信工作座谈会上的讲话全文发表” [Full Text of Xi Jinping’s Speech at the Symposium on Cybersecurity and Informatization Work] (speech given April 19, 2016), Xinhua, April 25, 2016, https://archive.ph/hnnFI.

124. “习近平: 加快推进网络信息技术自主创新 朝着建设网络强国目标不懈努力” [Xi Jinping: Accelerate Promoting the Independent Innovation of Network Information Technology, and Make Tireless Efforts toward the Goal of Building a Network Great Power], Xinhua, October 9, 2016, https://archive.ph/tBTNY.

125. See, e.g., James Kynge and Sun Yu, “China and Big Tech: Xi’s Blueprint for a Digital Dictatorship,” *Financial Times*, September 7, 2021, https://www.ft.com/content/9ef38be2-9b4d-49a4-a812-97ad6d70ea6f.

126. See David Dorman and John Hemmings, “Digital China: The Strategy and Its Geopolitical Implications,” Pacific Forum International, February 2023, https://pacforum.org/wp-content/uploads/2023/02/IssuesandInsights_VOL23_WP2.pdf.

127. “习近平: 实施国家大数据战略加快建设数字中国” [Xi Jinping: Implement the National Big Data Strategy and Accelerate Construction of Digital China], Xinhua, December 9, 2017, https://archive.ph/yprSS.

128. “这四次中央政治局集体学习, 主题非常 “前沿”” [For These Four Politburo Collective Study Meetings, the Topic Is Very “Cutting-Edge”], Qiushi Net, March 19, 2021, https://archive.ph/uv402.

129. “习近平出席全国网络安全和信息化工作会议并发表重要讲话” [Xi Jinping Delivers an Important Speech at the Cyberspace Administration of China Meeting], Xinhua, April 21, 2018, https://archive.ph/hkCni.

130. The key policy frame that dissolves these distinctions is “top-level planning.” See, e.g., “MIIT Calls for Improvements to Top-Level Planning of Big Data Industry Development in China,” China Banking News, November 26, 2021, https://www.chinabankingnews.com/2021/11/26/miit-calls-for-improvements-to-top-level-planning-of-big-data-industry-development-in-china.

131. See, e.g., “习近平: 实施国家大数据战略加快建设数字中国” [Xi Jinping: The Implementation of the National Big Data Strategy to Accelerate the Construction of Digital China] (speech given December 8, 2017), Xinhua, December 9, 2017, https://archive.ph/TaSpA. According to an official interpretation of the meeting released by Party broadcaster CCTV, these statements signified that data was a “new factor of production, a basic and strategic resource, and an important productive force.” See “习近平带政治局集体学习 领导干部要学懂用好大数据” [Xi Jinping Led Politburo Self-Study Session on Using and Understanding Big Data], CCTV, December 10, 2017, http://archive.today/MzOKh.

132. “中共中央关于坚持和完善中国特色社会主义制度推进国家治理体系和治理能力现代化若干重大问题的决定” [Resolution of the CCP Central Committee on Several Major Issues concerning Adhering to and Perfecting the Socialist System with Chinese Characteristics and Advancing Modernization of the National Governance System and Governance Capacity], Xinhua, November 5, 2019, https://archive.ph/uWEnD.

133. “中共中央关于制定国民经济和社会发展第十四个五年规划和二〇三五年远景目标的建议” [Recommendation of the CCP Central Committee concerning Formulation of the National Economic and Social Development 14th Five-Year Plan and 2035 Long-Range Goals], Xinhua, November 3, 2020, https://archive.ph/r7AbQ.

134. “中华人民共和国国民经济和社会发展第十四个五年规划和2035年远景目标纲要” [Outline of the People’s Republic of China National Economic and Social Development 14th Five-Year Plan and 2035 Long-Range Goals], Xinhua, March 13, 2021, https://archive.ph/ZTF2U.

135. The State Strategic Advisory Committee, “Roadmap.”

136. “习近平出席二十国集团领导人第十六次峰会第一阶段会议并发表重要讲话” [Xi Jinping Attended the First Phase of the 16th G20 Leaders’ Summit and Delivered an Important Speech], *People’s Daily*, October 31, 2021, https://archive.ph/blwRs.

137. “全球数据安全倡议” [Global Data Security Initiative], PRC Ministry of Foreign Affairs, September 8, 2020, https://archive.ph/1eOtz.

138. “中方提出《全球数据安全倡议》” [China Proposes Global Data Security Initiative], PRC Ministry of Foreign Affairs, September 8, 2020, https://archive.ph/YZfbs.

139. See, e.g., Ryan Browne, “UK Bans Installation of Huawei 5G Equipment from September,” CNBC, November 30, 2020, https://www.cnbc.com/2020/11/30/uk-bans-installation-of-huawei-5g-equipment-from-september.html.

140. “The Clean Network,” US Department of State, n.d., https://2017-2021.state.gov/the-clean-network/index.html; see also “从《全球数据安全倡议》看当前的网络空间国际治理进程” [The Current Process of International Governance in Cyberspace from the Perspective of the Global Data Security Initiative], CICIR via Chinese People’s Institute of Foreign Affairs, September 2020, https://archive.ph/azeDC.

141. “中国与阿盟《中阿数据安全合作倡议》全文发布” [Full Text of the China-Arab Data Security Cooperation Initiative between China and League of Arab States Released], Trade Law Connection (China Council for the Promotion of International Trade), April 2, 2021, https://archive.ph/FlhmL.

142. “中方发起 “中非携手构建网络空间命运共同体倡议”” [China Launches “China-Africa Initiative on Building a Community of Destiny in Cyberspace Together”], CAC, August 25, 2021, https://archive.ph/mQ4KZ.

143. “Digital Economy Partnership Agreement (DEPA),” Singapore Ministry of Trade and Industry, n.d., https://www.mti.gov.sg/Trade/Digital-Economy-Agreements/The-Digital-Economy-Partnership-Agreement; and “Digital Economy Partnership Agreement (DEPA),” New Zealand Ministry of Foreign Affairs and Trade, n.d., https://www.mfat.govt.nz/en/trade/free-trade-agreements/free-trade-agreements-in-force/digital-economy-partnership-agreement-depa.

144. Rahul Nath Choudhury, “China’s Road to DEPA Is a Bumpy One,” Geopolitical Monitor, November 2, 2021, https://www.geopoliticalmonitor.com/chinas-road-to-depa-is-a-bumpy-one.

145. “中方正式提出申请加入《数字经济伙伴关系协定》(DEPA)” [China Formally Applies to Join the Digital Economy Partnership Agreement (DEPA)], China Financial News, November 1, 2021, https://archive.ph/RRqPL; and “中方正式提出申请加入数字经济伙伴关系协定” [China Formally Files Application to Join Digital Economy Partnership Agreement], Securities Times, November 2, 2021, https://archive.ph/ESwmm.

146. “Commerce Ministry: China Advancing Negotiations on Joining DEPA,” Xinhua, August 23, 2022, https://archive.ph/gtkPp; and Ovais Subhani, “S’pore, NZ, Chile to Formally Discuss China’s Accession to Digital Trade Pact,” The Straits Times, August 18, 2022, https://www.straitstimes.com/business/economy/singapore-new-zealand-chile-to-formally-discuss-chinas-accession-to-digital-trade-agreement.

147. “The Regional Comprehensive Economic Partnership (RCEP) is a free trade agreement (FTA) between the ten member states of the Association of Southeast Asian Nations (ASEAN) (Brunei, Cambodia, Indonesia, Laos, Malaysia, Myanmar, the Philippines, Singapore, Thailand, Vietnam) and its five FTA partners (Australia, China, Japan, New Zealand and Republic of Korea).” See RCEP, “Regional Comprehensive Economic Partnership (RCEP) Agreement to Enter

into Force on 1 January 2022," https://rcepsec.org; "商务部国际司负责人谈RCEP即将正式生效有关情况" [The Head of the Ministry of Commerce International Department Talks about Conditions Related to RCEP Becoming Formally Effective], PRC Ministry of Commerce, November 7, 2021, http://www.gov.cn/xinwen/2021-11/07/content_5649610.htm; and Jean-Marc F. Blanchard and Wei Liang, "Reassessing RCEP's Implications for Digital Trade and E-commerce," *The Diplomat*, May 4, 2022, https://thediplomat.com/2022/05/reassessing-rceps-implications-for-digital-trade-and-e-commerce.

148. See, e.g., "Trans-Pacific Partnership Agreement," Australian Government, last updated December 7, 2016, https://www.dfat.gov.au/sites/default/files/electronic-commerce.PDF; and Mireya Solís, "China Moves to Join the CPTPP, but Don't Expect a Fast Pass," Brookings, September 23, 2021, https://www.brookings.edu/blog/order-from-chaos/2021/09/23/china-moves-to-join-the-cptpp-but-dont-expect-a-fast-pass.

149. Jeffrey J. Schott, "China's CPTPP Bid Puts Biden on the Spot," Peterson Institute for International Economics, September 23, 2021, https://www.piie.com/blogs/trade-and-investment-policy-watch/chinas-cptpp-bid-puts-biden-spot.

150. "中华人民共和国国家安全法 (主席令第二十九号) " [PRC National Security Law (Presidential Order No. 29)], Xinhua, July 1, 2015, https://archive.ph/FHxrv; on the Party's view of "economic security," see "经济安全" 缘何被视为国家安全基础" [Why "Economic Security" Is Regarded as a Foundation of National Security], Qiushi, April 22, 2014, https://archive.ph/o7N8v.

151. "中华人民共和国国家情报法" [PRC National Intelligence Law (revised)], National People's Congress, June 12, 2018, https://archive.ph/6zb0B.

152. "中华人民共和国网络安全法" [PRC Cybersecurity Law], Xinhua, November 7, 2016, https://archive.ph/IwrOs. See also "China Cybersecurity: No Place to Hide," China Law Blog, Harris Bricken, October 11, 2020, last modified February 24, 2023, https://harrisbricken.com/chinalawblog/china-cybersecurity-no-place-to-hide/; and "China's New Cybersecurity System: There Is NO Place to Hide," China Law Blog, Harris Bricken, October 7, 2019, https://harrisbricken.com/chinalawblog/chinas-new-cybersecurity-system-there-is-no-place-to-hide.

153. "中华人民共和国密码法" [PRC Encryption Law], PRC National People's Congress, October 26, 2019, https://archive.ph/aBPwB.

154. "中华人民共和国数据安全法" [PRC Data Security Law], PRC National People's Congress, June 10, 2021, https://archive.ph/IMQL0.

155. "中华人民共和国数据安全法" [PRC Data Security Law]. According to the Ministry of Industry and Information Technology, core data is information that "poses a serious threat" to China's "politics, territory, economy, culture, society, science and technology, cyberspace, ecosystem, resources, and nuclear security"; has a "serious impact" on China's overseas interests, biosphere, space, polar regions, deep ocean, artificial intelligence, and other key domains of national security"; has a "serious impact" on "important backbone enterprises, critical information infrastructure, and important resources" in the industrial and telecommunications sectors; or which could "greatly damage" normal operation and services related to industrial production, telecommunications, or the internet. See "工业和信息化领域数据安全管理办法 (试行) (公开征求意见稿) " [Data Security Management Measures in the Domains of Industry and Informatization (for Trial Implementation) (Draft for Public Comment)], PRC Central People's Government, February 2022, https://archive.ph/MaF2K.

156. "中华人民共和国个人信息保护法" [PRC Personal Information Protection Law], PRC National People's Government, August 20, 2021, https://archive.ph/2cifD.

157. "中共中央关于坚持和完善中国特色社会主义制度 推进国家治理体系和治理能力现代化若干重大问题的决定" [Resolution of the CCP Central Committee on Several Major Issues concerning Adhering to and Perfecting the Socialist System with Chinese Characteristics and Advancing Modernization of the National Governance System and Governance Capacity], Xinhua, November 5, 2019, https://archive.ph/uWEnD.

158. "中共中央关于制定国民经济和社会发展第十四个五年规划和二〇三五年远景目标的建议" [Recommendation of the CCP Central Committee].

159. “全力提升科技创新要素整合力” [Fully Enhance the Integration of Science and Technology Innovation Factors], Economic Daily, October 2, 2020, https://archive.ph/qHDx3.

160. “中华人民共和国国民经济和社会发展第十四个五年规划和2035年远景目标纲要” [Outline of the People’s Republic of China National Economic and Social Development 14th Five-Year Plan and 2035 Long-Range Goals], Xinhua, March 13, 2021, https://archive.ph/ZTF2U.

161. Lu Zhenhua, “Party Calls on Private Sector to Break US Tech Blockade,” Caixin, January 25, 2021, https://www.caixinglobal.com/2021-01-25/party-calls-on-private-sector-to-break-us-tech-blockade-101655472.html.

162. “江金权：把握构建国内大循环的着力点” [Jiang Jinquan: Grasp the Focal Point of Building a Domestic “Big Cycle”], *Study Times*, January 25, 2021, http://www.rmlt.com.cn/2021/0125/606101.shtml.

163. “中国共产党章程” [Chinese Communist Party Charter], Article 30, revised October 24, 2017, https://archive.vn/pDFsG.

164. “中华人民共和国公司法” [People’s Republic of China Company Law], China National People’s Congress, revised October 26, 2018, https://archive.ph/32D6j.

165. “中央网信办召开互联网企业党建工作现场会” [Cyberspace Administration of China Held a Meeting on Party Building in Internet Corporations], Office of the Central Cyberspace Affairs Commission, October 26, 2016, https://archive.vn/Lvs8W.

166. “中国共产党章程” [Chinese Communist Party Charter].

167. “中国共产党章程” [Chinese Communist Party Charter].

168. Yan Xiaojun and Jie Huang, “Navigating Unknown Waters: The Chinese Communist Party’s New Presence in the Private Sector,” *China Review* 17, no. 2 (2017): 37–63.

169. See, e.g., “中共中央 国务院关于新时代加快完善社会主义市场经济体制的意见” [Opinions of the CCP Central Committee and State Council on Accelerating the Improvement of the Socialist Market Economic System in the New Era], Xinhua, May 18, 2020, https://archive.ph/9DhxI.

170. “习近平在企业家座谈会上的讲话” [Xi Jinping’s Speech at the Entrepreneurs Symposium], *People’s Daily*, July 21, 2020, https://archive.vn/8zSVJ (emphasis added).

171. Wei Qi, “Chinese President Takes On New Role to Spearhead Civilian-Military Tech Transfer,” *South China Morning Post*, January 23, 2017, https://www.scmp.com/news/china/diplomacy-defence/article/2064461/chinese-president-takes-new-role-spearhead-civilian.

172. “习近平：扎扎实实推进军民融合深度发展 为实现中国梦强军梦提供强大动力和战略支撑” [Xi Jinping: Solidly Promote the Deep Development of Military-Civil Integration to Achieve the China Dream and Strong Military Dream of Providing Strong Power and Strategic Support], Xinhua, March 12, 2018, https://archive.ph/vVwBi.

173. “Huawei and Its Siblings, the Chinese Tech Giants: National Security and Foreign Policy Implications,” US Department of State, September 11, 2019, https://2017-2021.state.gov/huawei-and-its-siblings-the-chinese-tech-giants-national-security-and-foreign-policy-implications/index.html.

174. “中共中央 国务院 中央军委印发《关于经济建设和国防建设融合发展的意见》” [CCP Central Committee, State Council, and Central Military Commission, “Opinions on the Fused Development of Economic Construction and National Defense Construction”], Xinhua, July 21, 2016, https://archive.ph/GsM2I.

175. “习近平：开创新时代军民融合深度发展新局面” [Xi Jinping: Open Up a New Era of In-Depth Development and a New Situation in Military-Civil Fusion], Xinhua, March 2, 2018, https://archive.ph/WI21s.

176. “China Outlines Vision for Four Mega Data Centre Clusters,” Reuters, December 31, 2021, https://www.reuters.com/technology/china-approves-building-four-data-centre-clusters-2021-12-29.

177. “职能配置与内设机构” [Functional Configuration and Internal Structure], NDRC, n.d., https://archive.ph/t5Iba.

178. Original: 创新和高技术发展司 [Department of Innovation and High-Tech Development]; and "职能配置与内设机构" [Functional Configuration and Internal Structure].

179. "大数据协同安全技术国家工程研究中心概述" [Overview of the National Engineering Research Center for Collaborative Security Technologies for Big Data], National Engineering Research Center for Big Data Collaborative Security Technology, accessed August 15, 2022, http://archive.today/ZSckY; and "工程中心成员单位" [Engineering Center Member Units], National Engineering Research Center for Big Data Collaborative Security Technology, accessed August 17, 2022, http://archive.today/zdyGx.

180. "什么是"东数西算"? 你想知道的都在这儿" [What Is "East Data, West Compute"? Here's What You Want to Know], Xinhua, February 18, 2022, https://web.archive.org/web/20230411012708/http://finance.people.com.cn/n1/2022/0218/c1004-32354691.html; and "东数西算" [East Data, West Compute], NDRC, https://archive.ph/CpeNC.

181. "什么是"东数西算"? 你想知道的都在这儿" [What Is "East Data, West Compute"?].

182. "八个算力枢纽，十大数字中心集群! 国家级「东数西算」工程解读" [Eight Computing Hubs, Ten Digital Center Clusters! National-Level "East Data, West Computing" Project Explained], 51CTO, February 19, 2022, https://archive.ph/MFBDP; and "工业和信息化部关于印发《新型数据中心发展三年行动计划（2021-2023年）》的通知" [Notice Concerning MIIT Issuance of the "New-Style Data Center Development Three-Year Action Plan (2021-2023)"], Ministry of Industry and Information Technology, July 4, 2021, https://archive.ph/ZNHR0.

183. "加快资源布局 中国电信加速织就全国算力"一张网"" [China Telecom Accelerates the Layout of Resources to Weave a "One Network" of National Computing Power], China Telecom, February 19, 2022, https://archive.ph/MFBDP; and "中国联通：将全面承接国家"东数西算"工程" [China Unicom: Will Fully Undertake the "East Data, West Computing" Project], China Securities Journal, February 23, 2022, https://archive.ph/Ah9i8.

184. "透视东数西算 | "东数西算"工程具有四大意义，中兴通讯赋能产业转型升级" [Deep Dive on East Data, West Computing—The "East Data, West Computing" Project Has Four Significances, ZTE Empowers Industrial Transformation and Upgrading], Sina Technology, March 11, 2022, https://archive.ph/GO4Yy; and "阿里、腾讯、华为加紧布局，"东数西算"这股东风利好哪些版块？" [Alibaba, Tencent, and Huawei to Step Up the Layout, "East Data, West Computing," This Wind Is Favorable to Which Part?], Sohu, February 22, 2022, https://archive.ph/QOudv.

185. 商务部 中央网信办 发展改革委, "'十四五' 电子商务发展规划" [Ministry of Commerce, CAC, and NDRC, 14th Five-Year Plan Digital Commerce Development Plan], October 2021, http://www.cac.gov.cn/2021-10/26/c_1636843216727631.htm.

186. "科学技术部关于公开征求《人类遗传资源管理条例实施细则（征求意见稿）》意见的通知" [Notice of the Ministry of Science and Technology on Public Consultation of Opinion on "Implementing Rules of the Regulations on Human Genetic Resources Management (Draft for Comments)"], March 22, 2022, https://archive.ph/d6IGP.

187. "习近平在中央政治局第十八次集体学习时强调 把区块链作为核心技术自主创新重要突破口 加快推动区块链技术和产业创新发展" [Xi Jinping Emphasized during the 18th Collective Study of the Politburo to Take Blockchain as an Important Breakthrough in Independent Innovation of Core Technologies to Accelerate the Development of Blockchain Technology and Industrial Innovation], Xinhua, October 25, 2019, https://archive.ph/UpDa8.

188. See "Knowledge Base: Blockchain-Based Service Network," DigiChina, Stanford University, July 2, 2021, https://digichina.stanford.edu/work/knowledge-base-blockchain-based-service-network-bsn-%E5%8C%BA%E5%9D%97%E9%93%BE%E6%9C%8D%E5%8A%A1%E7%BD%91%E7%BB%9C.

189. Michael D. Bordo, "Digital Currency and the Future," Hoover Institution, March 18, 2022, https://www.hoover.org/research/digital-currency-and-future.

190. "Central Banks of China and United Arab Emirates Join Digital Currency Project for Cross-Border Payments," press release, BIS, February 23, 2021, https://www.bis.org/press/p210223.htm.

191. "十四五" 现代流通体系建设规划" [14th Five-Year Plan Modern Circulation System Construction Plan], NDRC, January 13, 2022, https://archive.ph/55Mg9.

192. "关于印发《智能汽车创新发展战略》的通知" [Notice on the Issuance of the "Strategy for the Innovative Development of Intelligent Vehicles"], NDRC, February 10, 2021, https://web.archive.org/web/20220605172121/https://www.ndrc.gov.cn/xxgk/zcfb/tz/202002/P020200224573058971435.pdf.

193. "Securing the Information and Communications Technology and Services Supply Chain," Federal Register, National Archives, January 19, 2021, https://www.federalregister.gov/documents/2021/01/19/2021-01234/securing-the-information-and-communications-technology-and-services-supply-chain.

194. "Securing the Information and Communications Technology."

195. John D. McKinnon, "US to Impose Sweeping Rule Aimed at China Technology Threats," *Wall Street Journal*, February 26, 2021, https://www.wsj.com/articles/u-s-to-impose-sweeping-rule-aimed-at-china-technology-threats-11614362435.

196. Gina M. Raimondo, "US Secretary of Commerce Gina Raimondo Statement on Actions Taken under ICTS Supply Chain Executive Order," US Department of Commerce, March 17, 2021, https://www.commerce.gov/news/press-releases/2021/03/us-secretary-commerce-gina-raimondo-statement-actions-taken-under-icts; and Ben Brody, "A Secretive US Security Program Has Its Sights on DiDi," Protocol, March 23, 2022, https://www.protocol.com/policy/didi-commerce-icts.

197. "Securing the Information and Communications Technology and Services Supply Chain; Connected Software Applications," Federal Register, National Archives, November 26, 2021, https://www.federalregister.gov/documents/2021/11/26/2021-25329/securing-the-information-and-communications-technology-and-services-supply-chain-connected-software.

198. "Securing the Information and Communications Technology and Services Supply Chain," Federal Register, National Archives, May 15, 2019, https://www.federalregister.gov/documents/2019/05/17/2019-10538/securing-the-information-and-communications-technology-and-services-supply-chain.

199. "Executive Order on Protecting Americans' Sensitive Data from Foreign Adversaries," The White House, June 9, 2021, https://www.whitehouse.gov/briefing-room/presidential-actions/2021/06/09/executive-order-on-protecting-americans-sensitive-data-from-foreign-adversaries/ (emphasis added).

200. Emily Kilcrease, "Using a Sanctions Framework to Fix the ICTS Executive Order," Lawfare, December 17, 2021, https://www.lawfareblog.com/using-sanctions-framework-fix-icts-executive-order.

201. Notable examples of companies already subject to CFIUS review include TuSimple ("TuSimple Adds Independent Directors to Government Security Committee," Cision PR Newswire, January 17, 2023, https://www.prnewswire.com/news-releases/tusimple-adds-independent-directors-to-government-security-committee-301723837.html) and TikTok (Ashley Gold, "TikTok's 'Death Star' Dangers," Axios, January 9, 2023, https://www.axios.com/2023/01/09/tiktok-washington-china-cfius-bans).

202. James Pearson and Sarah N. Lynch, "US Launches 'Disruptive Technology' Strike Force to Target National Security Threats," Reuters, February 16, 2023, https://www.reuters.com/world/us/us-launches-disruptive-technology-strike-force-target-national-security-threats-2023-02-16.

203. "Executive Order on America's Supply Chains," The White House, February 24, 2021, https://www.whitehouse.gov/briefing-room/presidential-actions/2021/02/24/executive-order-on-americas-supply-chains.

204. See report on Safeguarding Science/Research Security, The National Counterintelligence and Security Center, n.d., https://www.dni.gov/index.php/safeguarding-science/research-security.

205. David Feith, "Opportunities and Challenges for Trade Policy in the Digital Economy," Testimony before the US Senate Committee on Finance, November 30, 2022, https://www.finance.senate.gov/imo/media/doc/David%20Feith%20testimony%20to%20Senate%20Finance%20subcommittee%20on%20digital%20trade%202022%2011%2030.pdf.

206. “Non-SDN Chinese Military-Industrial Complex Companies List (NS-CMIC List), US Department of the Treasury, last updated December 16, 2021, https://ofac.treasury.gov/consolidated-sanctions-list/ns-cmic-list; and “Executive Order: Addressing the Threat from Securities Investments that Finance Certain Companies of the People’s Republic of China,” US Department of the Treasury, n.d., https://ofac.treasury.gov/media/99111/download?inline.

207. “国务院关于印发促进大数据发展行动纲要的通知” [Notice on State Council Issuance of the Big Data Development Action Plan], PRC Central People’s Government, September 5, 2015, https://archive.ph/p6U7g; and CCP General Office and State Council General Office, “国家信息化发展战略纲要” [National Informatization Development Strategic Outline], Xinhua, July 27, 2016, https://archive.ph/YJm6d. On government use of big data for supervision and enterprise services, including data security, social credit, and credit reporting, see State Council General Office, “国务院办公厅关于运用大数据加强对市场主体服务和监管的若干意见” [Several Opinions on Using Big Data to Strengthen Service and Supervision of Market Entities], MIIT, July 2, 2015, https://web.archive.org/web/20180213232922/http://www.miit.gov.cn/n1146290/n1146392/c3299036/content.html.

208. “工业和信息化部关于印发大数据产业发展规划 (2016-2020年) 的通知” [Notice Concerning MIIT Issuance of the Big Data Industry Development Plan (2016-2020)], MIIT, January 17, 2017, https://archive.ph/qa4Zx.

209. “‘十四五’大数据产业发展规划” [14th Five-Year Plan Big Data Industry Development Plan], MIIT, November 2021, https://archive.ph/hhRHt.

28 27 26 25 24 23 7 6 5 4 3 2 1

ABOUT THE AUTHOR

MATTHEW JOHNSON

Matthew Johnson is a visiting fellow at the Hoover Institution and research director at Garnaut Global. His expertise covers China's elite politics, strategic thinking, and political control over the financial sector and private economy. Previously a lecturer in the history and politics of modern China at the University of Oxford, he has published on propaganda, CCP ideology, cultural security, state-society relations, and the Cold War.

China's Global Sharp Power
A Hoover Institution Project

The Hoover Institution's project on China's Global Sharp Power (CGSP) tracks, documents, and analyzes how China's Communist Party-state shapes and controls information flows, coerces governments and corporations, infiltrates and corrupts political systems, and exploits, disrupts, and debases civic institutions, particularly in open and democratic societies. Through its research and global partnerships, CGSP produces papers, lectures, conferences, workshops, publications, and web-accessible resources to educate opinion leaders and policy makers so that they may pursue diverse, balanced, and vigilant relationships with China, tailored to their circumstances.

For more information about this Hoover Institution project, visit us online at www.hoover.org/research-teams/chinas-global-sharp-power-project.

ASIA SOCIETY CENTER ON U.S.-CHINA RELATIONS

The Asia Society Center on U.S.-China Relations was founded in 2006 and is based at Asia Society's New York headquarters. In the years to come, an open and collaborative relationship between the United States and China will be essential to global peace, security, balanced economic growth, and environmental sustainability. In seeking new ways of building mutual understanding between the United States and China, the center undertakes projects and events that explore areas of common interest and divergent views between the two countries, focusing on policy, culture, business, media, economics, energy, and the environment.

Hoover Institution, Stanford University
434 Galvez Mall
Stanford, CA 94305-6003
650-723-1754

Hoover Institution in Washington
1399 New York Avenue NW, Suite 500
Washington, DC 20005
202-760-3200

HOOVER INSTITUTION