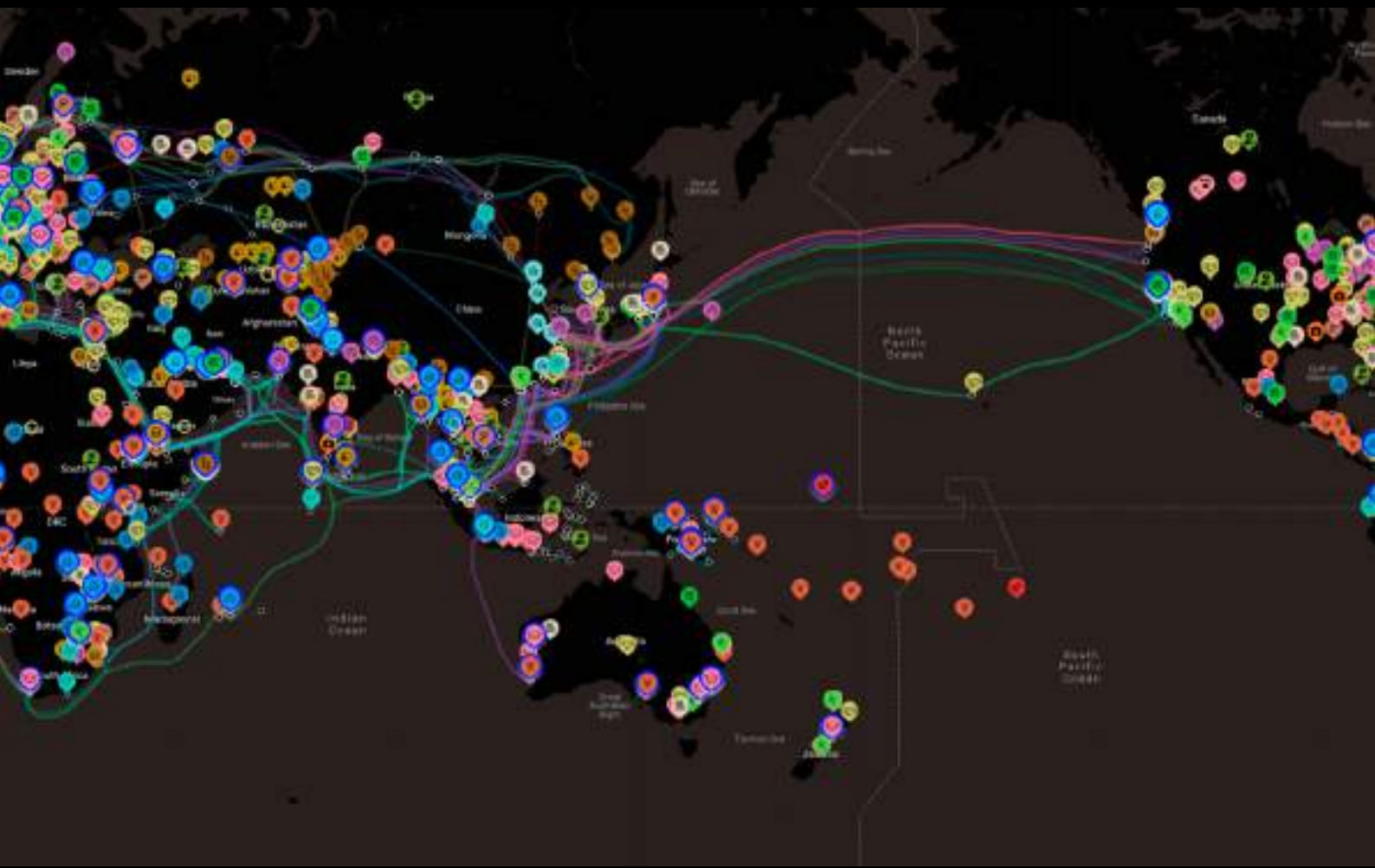
Mapping China's Technology Giants

Supply chains and the global data collection ecosystem

Dr Samantha Hoffman and Dr Nathan Attrill



ASPI AUSTRALIAN STRATEGIC POLICY INSTITUTE
INTERNATIONAL CYBER POLICY CENTRE
TWENTY YEARS OF ASPI STRATEGY 2001 - 2021

Policy Brief
Report No. 45/2021

About the authors

Dr Samantha Hoffman is a senior analyst with ASPI's International Cyber Policy Centre.

Dr Nathan Attrill is an analyst with ASPI's International Cyber Policy Centre.

Acknowledgements

Thank you to Danielle Cave and Cheryl Yu for all of their work on this project. We would like to also thank our external peer reviewers Lindsay Gorman, Kara Frederick and Chris Crowley. We're also grateful for the valuable comments and assistance provided by Peter Mattis, Tom Uren, Michael Shoebridge and Fergus Hanson.

This research report forms part of Mapping China's Technology Giants, which is a multi-year project mapping and analysing the overseas expansion of key Chinese technology companies. The project seeks to:

- analyse the global expansion of a key sample of China's tech giants by mapping their major points of overseas presence
- provide the public with analysis of the governance structures and party-state politics in which these companies have emerged, and are deeply entwined.

The Mapping China's Technology Giants project is produced by researchers at ASPI's International Cyber Policy Centre. The relaunch of this project, and associated research, was funded with a US$270,000 grant from the US State Department

What is ASPI?

The Australian Strategic Policy Institute was formed in 2001 as an independent, non-partisan think tank. Its core aim is to provide the Australian Government with fresh ideas on Australia's defence, security and strategic policy choices. ASPI is responsible for informing the public on a range of strategic issues, generating new thinking for government and harnessing strategic thinking internationally. ASPI's sources of funding are identified in our annual report, online at www.aspi.org.au and in the acknowledgements section of individual publications. ASPI remains independent in the content of the research and in all editorial judgements.

ASPI International Cyber Policy Centre

ASPI's International Cyber Policy Centre (ICPC) is a leading voice in global debates on cyber, emerging and critical technologies, issues related to information and foreign interference and focuses on the impact these issues have on broader strategic policy. The centre has a growing mixture of expertise and skills with teams of researchers who concentrate on policy, technical analysis, information operations and disinformation, critical and emerging technologies, cyber capacity building, satellite analysis, surveillance and China-related issues.

The ICPC informs public debate in the Indo-Pacific region and supports public policy development by producing original, empirical, data-driven research. The ICPC enriches regional debates by collaborating with research institutes from around the world and by bringing leading global experts to Australia, including through fellowships. To develop capability in Australia and across the Indo-Pacific region, the ICPC has a capacity building team that conducts workshops, training programs and large-scale exercises for the public and private sectors.

We would like to thank all of those who support and contribute to the ICPC with their time, intellect and passion for the topics we work on. If you would like to support the work of the centre please contact: icpc@aspi.org.au

Important disclaimer

ASPI

Tel +61 2 6270 5100
Email enquiries@aspi.org.au
www.aspi.org.au
www.aspistrategist.org.au
facebook.com/ASPI.org
@ASPI_ICPC

First published June 2021.

ISSN 2209-9689 (online),
ISSN 2209-9670 (print).

Cover image: ASPI ICPC, Nathan Attrill

ASPI AUSTRALIAN STRATEGIC POLICY INSTITUTE

INTERNATIONAL CYBER POLICY CENTRE

Funding for this report was provided by the US State Department.

Mapping China's Technology Giants

Supply chains and the global data collection ecosystem

Dr Samantha Hoffman and Dr Nathan Attrill

Policy Brief
Report No. 45/2021

Contents

What's the problem?

Most of the 27 companies tracked by our Mapping China's Technology Giants project are heavily involved in the collection and processing of vast quantities of personal and organisational data—everything from personal social media accounts, to smart cities data, to biomedical data.[1] Their business operations—and associated international collaborations—depend on the flow of vast amounts of data, often governed by the data privacy laws of multiple jurisdictions. Currently, however, existing global policy debates and subsequent policy responses concerning security in the digital supply chain miss the bigger picture because they typically prioritise the potential for disruption or malicious alterations of the supply chain. Yet, as we have defined it in this report, digital supply-chain risk starts at the design level (Figure 1).

For the People's Republic of China (PRC), the designer is the Chinese party-state, through expectations and agenda-setting in laws and policy documents and actions such as the mobilisation of state resources to achieve objectives such as the setting of technology standards. It's through those standards, policies and laws that the party-state is refining its capacity to exert control over companies' activities to ensure that it can derive strategic value and benefit from the companies' global operations. That includes leveraging data collection taking place through those companies' everyday global business activities, which ASPI's International Cyber Policy Centre (ICPC) described in the *Engineering global consent* report.[2] Technology isn't agnostic—who sets the standards and therefore the direction of the technology matters just as much as who manufactures the product. This will have major implications for the effectiveness of data protection laws and notions of digital supply-chain security.

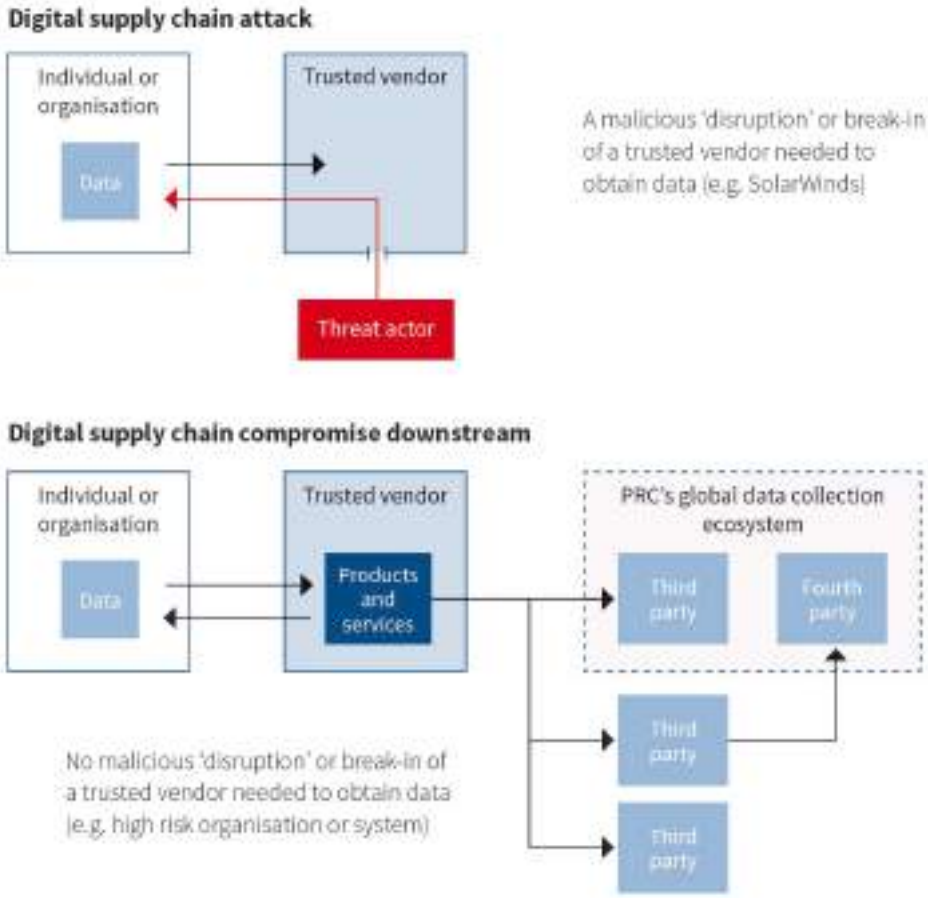
What's the solution?

This report recommends that governments, businesses and other organisations take a more multidisciplinary approach to due diligence. That approach needs to take into account the core strategic thinking that underlies the ways the Chinese party-state uses technology. It must also take into account the breadth of what's considered to be 'state security' in China and the ramifications of the PRC's cyber- and data-focused laws and regulations.

All governments should improve their regulatory frameworks for data security and privacy protection. Doing so will put them in better ethical and legal positions to take meaningful long-term policy actions on a whole suite of issues. However, those efforts in isolation won't solve all of the unique challenges posed by the Chinese party-state or other geopolitical challenges described in this report.

A more holistic approach, which would help to ensure that data is better protected, also requires a better definition of digital supply-chain risk and a reframing of global policy debates on these issues. There needs to be a greater understanding of how supply-chain risks manifest, including the intentional introduction of access and more subtle monitoring and information collection by malicious actors. Specific actions for managing potential data insecurity and privacy breaches in supply chains should include improving risk-based approaches to the regulation of data transfers.

Figure 1: Compromise of the digital supply chain without a malicious intrusion or alteration



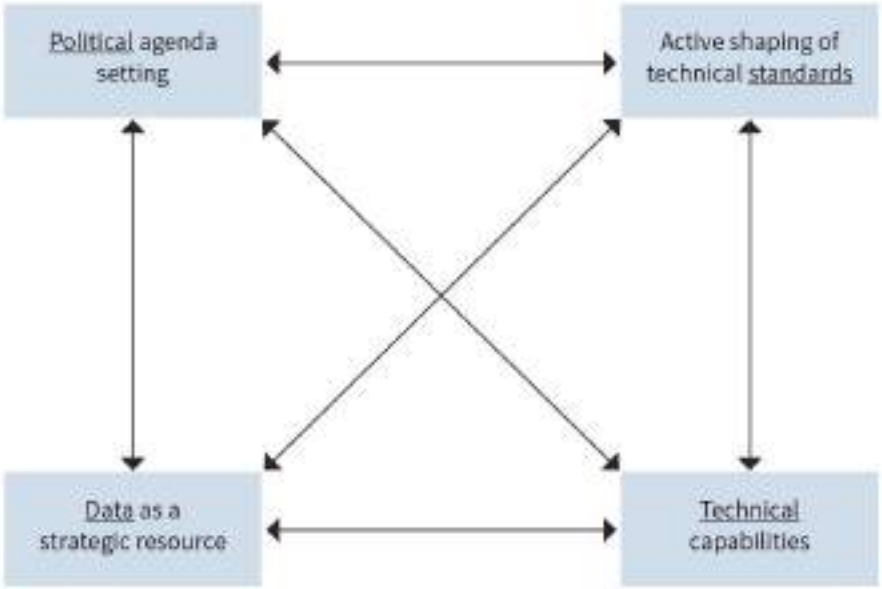
Source: ASPI authors' illustration.

1. The PRC's data ecosystem

The PRC's global data collection ecosystem was outlined in the ASPI ICPC policy report *Engineering global consent: the Chinese Communist Party's data-driven power expansion*.[3] In that report, we described ways the Chinese party-state directly and indirectly leveraged PRC-headquartered commercial enterprises to access troves of data that those enterprises' products help generate. That report was based on how the Chinese party-state articulated its objectives on data use and state security and a case study of the propaganda department–linked company Global Tone Communication Technology Co. Ltd (which we expand on in the 'Downstream data access' section of this report).

As part of the Mapping China's Technology Giants project, we have identified the need to further define the PRC's 'global data ecosystem' concept. In this section, we focus on the nature of interactions between political agenda-setting, active shaping of international technical standards, technical capabilities, and data as a strategic resource. This directly affects companies' business activities, both domestic and global (Figure 2).

Figure 2: The PRC's data ecosystem



Source: ASPI authors' illustration.

The PRC's data ecosystem begins with technical capability. That includes China's advanced cyber offensive skills, but also extends to its companies' normal business operations anywhere in the world providing access, collection, data processing or any combination of the three to the party-state.

The party-state's ability to obtain large amounts of personal information and intellectual property through its state-sponsored cyber operations has been widely reported in detail, including in indictments by the US Department of Justice.[4] However, the PRC's policies and legislation—purposefully shaped by the Chinese Communist Party (CCP)—mean that the party-state's ability to access data is extended even further than the normal operations of PRC-based companies with a global presence. It's also consequential that those globally influential PRC-based technology companies occupy every layer of the 'technology stack'.

In Table 1, we illustrate the 'technology stack' by using the ISO standard Open Systems Interconnection model as a reference (because it's used for networking and data exchange but can also be illustrative of the technology industry ecosystem).[5] We then charted it against the relevant companies in the Mapping China's Technology Giants project and their US counterparts, which for several decades have had a dominant presence in every layer.

Table 1: Technology business ecosystem, referencing a simplified Open Systems Interconnection model

	Software/hardware groupings	General examples	US-based companies	PRC-based companies
Application layer	Software applications	Internet platforms (e.g. social media, websites, mobile apps), machine-learning engines (from cloud providers), content handlers	Facebook, Google, Amazon, Apple, Microsoft, PayPal, Zoom, Salesforce, Adobe	Baidu, Alibaba, Tencent, JD.com, ByteDance, Ant Group, Megvii, iFlytek, CloudWalk, SenseTime, YITU, Ping An Tech, Inspur, Huawei, CETC
Network layer	Storage and software infrastructure	Content delivery networks, cloud storage and infrastructure	Cloudflare, Akamai, Google, Microsoft, Amazon, IBM, Oracle, Apple	Alibaba, Tencent, ByteDance, Ping An Tech, Inspur, Huawei, CETC
	Hardware	Satellite navigation, networking hardware, sensor hardware, semiconductors, mobile wireless networking equipment	Cisco, Juniper, Global Positioning System (GPS), Google, Amazon, Apple, Nvidia, AMD, Texas Instruments, Qualcomm, Broadcom, Intel, Microsoft, IBM	Huawei, ZTE, BeiDou, Nuctech, Meiya Pico, Hikvision, Uniview, Dahua, Megvii, iFlytek, SenseTime, DJI, Huawei's Hisilicon, SMIC, CETC
Physical layer	Carrier infrastructure	Submarine cables, fibre-optic networks, mobile wireless network carrier equipment (5G base stations)	AT&T, Sprint, Verizon, Cogent, Comcast, Facebook, Google, Amazon, Microsoft, T-Mobile US	Hengtong, China Mobile, China Telecom, China Unicom, PEACE cable Ltd, Huawei, CETC

Source: ASPI authors' illustration.

Technology companies everywhere are primarily driven by commercial interests. The difference between the US and China is that in China the way the state conceives of the usefulness of data goes beyond traditional intelligence collection. For the Chinese party-state, data and the information derived from it contribute to everything. Domestically, that ranges from solving policy problems to information control and state coercion. Globally, it ranges from expanding the PRC's role in the global economy to understanding how to shape and control its global operating environment. In the next two sections, we elaborate on how the Chinese party-state's laws, policies and actions, which apply to PRC-based technology companies, create an ecosystem that provides it with access to the data that those companies can obtain.

1.1 Who sets the standards matters

Technology isn't values-agnostic. It takes on the values of its creator. Therefore, who sets the standards, and consequently the direction of the technology, matters. We know, for instance, that artificial intelligence has a history of racial and socio-economic bias built in from the design stage, reflective of the inherent biases of the designers and the choice of data used to train the algorithms.[6] Technologies must be designed to be 'values-neutral'[7] to avoid those problems, but that aspiration might not ever be realistic.[8]

Liberal democracies don't agree on what 'values' mean in this context. The European Union, for example, is increasingly prioritising indigenous technology development not just because of strategic competitors such as the PRC but also because of the US. That requires navigating often complex relationships with US-based technology giants such as Google, Apple and Facebook.[9] Part of protecting values in any liberal democracy is about preventing the creep of illiberalism from sources both domestic and foreign. It's also about introducing regulations and standards that protect the norms and freedoms underpinning democratic values. When it comes to Europe and the digital economy, much of that effort is currently targeted towards holding US technology companies accountable.[10]

The Chinese party-state is creating mechanisms and power structures through which it can ensure its ultimate and maximum access to datasets both domestically and globally. This is apparent through its agenda-setting (articulated in party and policy documents), its expectation-setting (signalled through new laws) and communications from the CCP (such as speeches and state media reporting).

Part of the CCP's effort takes place through the PRC's attempts to set standards that guide the design of technologies. For example, PRC facial recognition systems are required to be designed to recognise 'Uyghur faces'.[11] Another example is big data platforms and systems designed to categorise individuals based on a politicised version of whom the CCP deems suspicious or potentially threatening (such as petitioners, Tibetans, Uyghurs or Falun Gong practitioners).[12] Within the PRC, technologies are already being researched and developed to meet the needs of the party-state (see section 'Data regulations: setting the standards'). When those technologies are exported, such design features can't be erased by the technology's end-user, whether it's a global company or a foreign government.

1.2 Harnessing the strategic value of data

The Chinese party-state has deliberately formulated a strategy to harness the strategic value of data and the power of information to grow the power of the CCP over society. In 2013, Xi Jinping was quoted as saying, 'big data is the "free" resource of the industrial society. Whoever has a hold of the data has the initiative.'[13]

In 2016, China's 13th Five-Year Plan pushed for the creation of a 'big data security management system' alongside efforts to improve cyberspace governance by building an international consensus around the PRC's ideas on cyberspace security.[14] The 14th Five-Year Plan, unveiled in 2021, continues the party-state's multifaceted priorities for the development and use of big data for economic and social governance and calls for building new data infrastructure and improving the rules governing data collection, storage and use.[15]

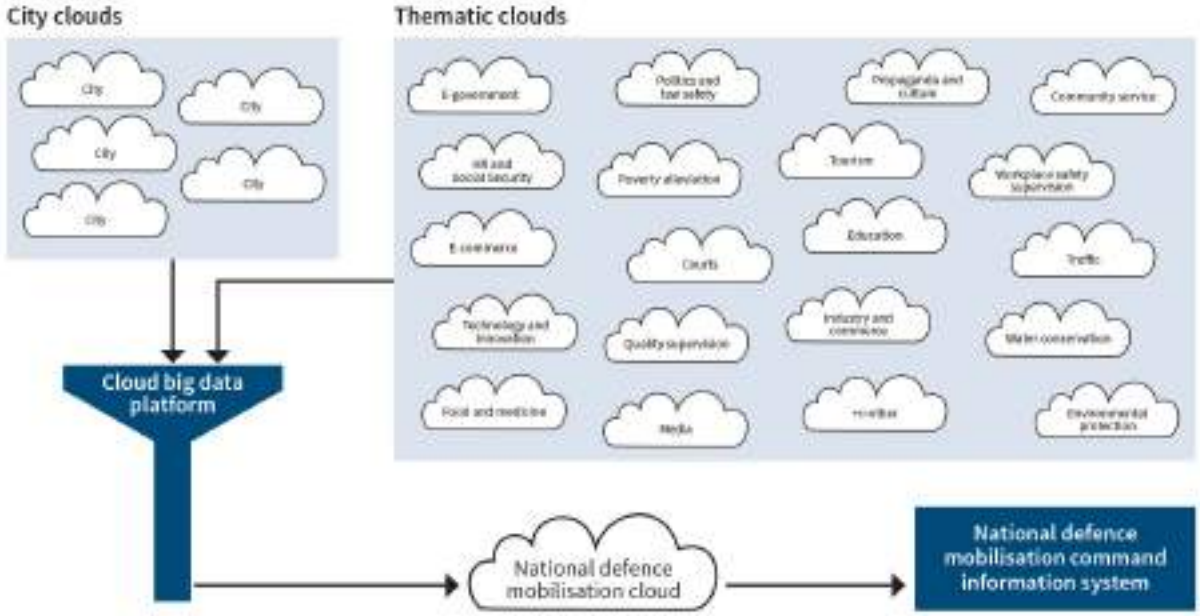
In addition to economic development, the party-state often describes big data technologies as contributing to 'social management' (also called 'social governance').[16] Social management covers a broad and overlapping list of agenda items, from creating capabilities to improve public service administration to strengthening 'public security'. Ultimately, social management refers to the party-state's management of *itself* as well as of society. This process relies on shaping, managing and controlling its operating environment through capabilities that enhance service provision and the capacity for risk management.[17]

New and emerging digital technologies are valued because they're viewed as a resource that can improve everyday governance capacity and facilitate problem-solving. In simplifying government service provision, the implementation of those technologies can in future facilitate communication across the PRC's sprawling government apparatus.[18] Digital and data-driven technologies obviously have multiple uses. For example, they can help streamline urban and social welfare services. In other respects, those same services can feed into the party-state's totalitarian model of governance and the way it identifies and responds to what it believes are emerging threats.

This use of data occurs in ways that provide both convenience and control. Routine services are intertwined with surveillance and coercive tools in ways that are often not legally possible in liberal democratic societies—or, when they do occur, can be genuinely challenged by the public, media and civil society. That distinction doesn't simply apply to the ways different PRC Government departments use similar technologies (such as ways the public security bureaus use technologies versus the ways industrial work safety offices use them).

One example is Human Rights Watch's findings on Xinjiang's Integrated Joint Operations Platform, which is used to centrally collect data on individual behaviours and flag 'those deemed potentially threatening'. One metric used to identify threats is energy usage from smart electricity meters: abnormally high energy use could indicate 'illegal' activity, but such meters in their normal use would also improve the accuracy of meter readings.[19] Another example is building datasets for use in the PRC's 'national defence mobilisation system' (a crisis response platform) using data sourced from a variety of government cloud networks, from smart cities to tourism-related cloud networks (Figure 3).[20]

Figure 3: The concept of defence mobilisation and smart cities data integration and processing



Source: ASPI authors' illustration.

Despite the benefits it can derive, the CCP also sees sources of harm emerging from technology and its use, and it realises that technology isn't an all-encompassing solution to its problems. Xi Jinping has described science and technology as a double-edged sword: 'On one hand, it can benefit society and the people. On the other hand, it can also be used by some people to damage the public interest and the interests of the people.'[21] Such risks could include companies or officials having the ability to exercise too much power with the aid of technology.[22] They could also include the use of technology by the CCP's political opponents to organise against the party-state, from either inside or outside the PRC.[23]

1.3 A global outlook

The PRC's plans to harness the strategic value of data and the power of information to grow state power are also globally oriented. The party-state sees its reliance on technologies originating in the West (especially the US) as a threat to state security, for fear of how foreign powers might exploit that reliance, especially in a crisis.[24] That fear helps drive the development of the PRC's indigenous technology capabilities.[25] Its capability effort includes planning on big data development to build an 'industry ecosystem' with 'globally oriented key enterprises and innovative small- and medium-sized enterprises with distinctive features'.[26] It also includes a plan to export PRC-originated technology standards, envisioned through the China Standards 2035 project.[27] Economic benefits and objectives are included in each plan, but through them the CCP also sets specific political ambitions.

As part of its global vision (see Figure 4), the Chinese party-state ensures that it's a part of the market-driven expansion and success of its global technology giants. Under Xi Jinping, the government has increasingly demonstrated the extraterritoriality inherent in PRC state security concepts and law. Moreover, the fact that companies have the right to do business in China at the party-state's discretion has become abundantly clear. The ability to harness the benefits of data would help to achieve the CCP's global vision because, through the processing and application of that data, the party can improve the sophistication of its efforts to shape, manage and control its global operating environment.

Figure 4: Explainer: The Chinese party-state's vision for the PRC in the world

Since its founding, the Chinese party-state has pursued the modernisation of the PRC with the goal of becoming both wealthy and powerful, and returning to what the party views as China's rightful place in the world [1].

The party-state's ambitions can be described as having three lines of effort:

1 The comprehensive modernisation of the PRC under the party-state's rule.
2 The unification and economic, social, and cultural assimilation of areas claimed by the party-state as 'China'.
3 Becoming a global power that shapes the international order and the ways in which nation-states interact.

Beijing's much-touted 'Belt and Road Initiative' (一带一路) is just one part of a larger vision for a 'new type of international relations (新型国际关系) and a 'community of common destiny for mankind' (人类命运共同体). In those concepts, the party-state has outlined a vision of international relations that more closely resembles the way the party-state exercises influence over the PRC and Chinese society [2]. In fact, there's also an international version of the social management concept that's been used to refer to a so-called 'deficit in social governance' due to the ineffectiveness of international institutions and the rules-based international order [3]. The party-state sees that a 'deficit' in international social management has not stopped 'the West' from having a strong discourse power [4]; therefore, the PRC needs to develop its own 'discourse power'—a concept that analyst Nadège Rolland has described as 'the ability to exert influence over the formulations and ideas that underpin the international order' [5].

Progress along each of these lines of effort may be uneven; however, these ambitious objectives can't be dismissed just because they appear unreachable or because the results appear fragmented today.

Sources: ASPI authors' illustration. See endnote for detailed citations.[28]

2. The PRC's developing data security framework

PRC legislation related to state security[29] provides reasons for foreign governments to be concerned about the exposure of any PRC-based commercial enterprise to the political demands of the party-state.[30] Recent state security laws, such as the 2017 Intelligence Law, haven't changed the longstanding *de facto* practice of state power in the PRC, but have further codified expectations in China that every citizen is responsible for state security.[31] Assessments of those risks have helped address what should be the obvious political and legal risks of doing business with PRC-based technology companies.

Some analysts have attempted to downplay the significance of such laws by claiming that the law is never black and white in the PRC and by describing compliance with PRC law as 'a negotiation'.[32] The latitude of officials to enforce the law and corporations' efforts to maintain their freedom of action leave open grey areas, but that claim, in the context in which it's being made, is false. Law may be a negotiation in the PRC, as it is elsewhere, but the party-state decides whether there's a negotiation at all, and where that negotiation ends.

Critically, the party-state itself isn't bound by the law when it's challenged or when its interests are threatened. A recent illustration of this is Alibaba and its founder, Jack Ma, who briefly 'disappeared' at the end of 2020 following his public criticism of PRC regulators' attitude towards big business, accusing them of having a 'pawnshop' mentality that stifled innovation.[33] In April 2021, it was announced that Alibaba would be fined US$2.8 billion after a probe determined that it had abused its market position for years.[34] Nobody in the PRC is too big or too powerful to be subject to the party-state's demands.[35]

PRC-based technology companies themselves have acknowledged their exposure to legal risks emanating from the PRC. It's standard practice for global companies to acknowledge in their privacy policies that user data may be transferred and governed by laws outside of their own jurisdiction. According to most privacy policies for websites and products of the 27 companies in our Mapping China's Technology Giants project, users who live outside the PRC may have their data transferred to and processed and stored in a country that isn't where they reside or have ordered services from, including the PRC, where all of the companies have business. When the data is transferred it will be governed by the law in that country's jurisdiction, not only the law in the place where the data originated (Figure 5).[36]

Figure 5: New *Mapping China's Technology Giants* product—'Thematic snapshots'

Source: Mapping China's Technology Giants project website, online.

Most of the 27 companies state that they're committed to protecting personal information, but acknowledge that they may be required to disclose personal data to meet law enforcement or state security requirements. The definition of what meets the threshold of being a national security or criminal case can be highly politicised in the PRC, and the process of definition isn't similar to those that occur in a liberal democracy.

The political system of the PRC creates this risk. Law in the PRC is first and foremost political and a governing tool that enforces political power. It's meant to be wielded by the party-state and to uphold and expand the power of the state. Its implementation is reliant on the CCP's leadership and is used to strengthen the party's governing capacity, but the law isn't above the party-state even if it's used to manage its members.[37] Nonetheless, the law is more than a blunt weapon of state power. It's important to think through the implications of the fact that the law also functions as a tool to set and communicate the state's expectations of its apparatuses, its entities and individuals.

New developments related to data collection, storage and transfer make these issues more apparent. The Chinese party-state is currently deliberating on a draft Data Security Law (DSL) and draft Personal Information Protection Law (PIPL).[38] In April 2021, second draft versions were issued publicly (see the appendix to this report for translations of the articles of the draft laws that we focus on in this

section). Both are expected to become law in 2021. The third and probably final version of the draft DSL is expected to be deliberated at a National People's Congress Standing Committee meeting on 7–10 June 2021.[39]

These laws don't exist in a vacuum. They should be read along with a suite of other relevant state security legislation, including, for example, the State Security Law (2015) and the Cybersecurity Law (2016).

2.1 Data regulations: limiting individuals and organisations while empowering the state

The draft DSL and draft PIPL should be read together. The main distinction is that the draft DSL lays out the responsibilities of the state in creating a data security system and in guaranteeing data security, whereas the draft PIPL defines the boundaries and personal information protection requirements for individuals and entities.[40]

What makes the framework unique, compared to any other country's laws regulating data security, is that data security is unambiguously part of the party-state's security strategy and is first about protecting the CCP's monopoly hold on power (Figure 6). The draft DSL says that the effort to guarantee data security must adhere to the party-state's 'comprehensive state security outlook'.[41] The draft establishes the state as the leader of the data security system, stating that the 'central state security leading mechanism' is 'responsible for decision making and overall coordination on data security work, and researching, drafting and guiding the implementation of national data security strategies and relevant major guidelines and policies.'[42]

Figure 6: Explainer: The PRC's state security concept

According to the State Security Law (2015), Article 3, 'All state security work shall adhere to the comprehensive state security outlook, regard people's security as the purpose, regard political security as the root, regard economic security as the foundation, regard military, cultural, and social security as the guarantors, [and] regard promoting international security as the dependent to maintain state security in all fields, build a state security system, and walk a path of state security with Chinese characteristics' [1].

According to the State Security Law (2015), Article 11, 'All citizens, state authorities, armed forces, political parties, people's groups, enterprises, public institutions, and other social organisations of the People's Republic of China shall have the responsibility and obligation to maintain state security ...' [2].

Figure 6 (continued): Explainer: The PRC's state security concept

The **comprehensive state security outlook (总体国家安全观)** is the phrase used under Xi Jinping to describe the concept of **state security (国家安全)**. While the phrase is new under Xi Jinping, the state security concept it describes is not; rather, it's part of the fabric of the political system. At the root of the concept is **political security (政治安全)**. It refers to the requirement to guarantee the CCP's leadership authority, and to protect the party-state from political threats that can emerge from *both inside and outside the party and inside and outside the PRC's geographical borders*. The state security concept also includes 'guarantors' such as **cultural security (文化安全)**, which is best summed up as the party-state's version of what is and is not 'China'. It also includes traditional components of national security such as **military security (军事安全)**, although this also carries political weight because the People's Liberation Army is the CCP's army [3].

Sources: ASPI authors' Illustration. See endnote for detailed citations.[43]

The law says not only that a party entity is in charge, but also that any significant policies will originate there. The term 'central state security leading mechanism' in legal documents is synonymous with the Central State Security Commission, which is a CCP body led by Xi Jinping.[44] Therefore, the activity of other state regulatory departments and public and state security organs responsible for implementing data security efforts would flow from the decision-making and strategy that the Central State Security Commission is tasked with overseeing and implementing.[45]

The draft DSL also applies to data-handling activities taking place 'outside the territory of the PRC', if those activities are seen to 'harm the state security, the public interest, or the lawful rights and interests of citizens' and organisations of the PRC, they are to be pursued for legal responsibility 'in accordance with law.' Existing law and practice illustrate the global application of such concepts.

Hong Kong's new National Security Law, passed in 2020, criminalises 'separatism', 'subversion', 'terrorism' and 'collusion' in addition to support for any of those activities by anyone, no matter where in the world they're located.[46]

The draft PIPL, meanwhile, is intended to regulate the power of individuals and entities who handle the personal data of PRC citizens both inside and outside the country. It establishes a more robust system for protecting individuals' data privacy from individuals and companies.[47] It applies to activities outside the PRC involving the handling of personal information of natural persons within the territory of the PRC when those outside actors are providing products or services to persons within the PRC, analysing and assessing the conduct of natural persons within PRC or 'other situations provided for by law or administrative regulations'. Just like the draft DSL, it leaves open the potential that the law can be used as intended: to protect the CCP's power wherever necessary. Laws such as the Intelligence Law illustrate specific cases in which other legislation might be used to justify this reach, and a law such as the Hong Kong National Security Law illustrates the fact that political opponents of the party-state might also be targeted in vague 'other situations'.[48]

The draft PIPL also superficially applies to the state. For example, it says that any retrieval of personal information requires following 'legally prescribed duties' and must be done 'in accordance with the authority and procedures provided by laws'.[49] Yet, Article 19 establishes that:

> [W]hen personal information handlers handle personal information, where there are circumstances that laws and administrative regulations provide shall be kept confidential or need not be announced, it is acceptable not to notify the individual.

On the basis of that logic, any case in which the 2017 Intelligence Law applies could be excluded from the PIPL's protections. Article 7 of the Intelligence Law says that:

> [A]ny organisation and citizen shall in accordance with the law, support, provide assistance, and cooperate in national intelligence work, and guard the secrecy of any intelligence work they are aware of.[50]

The important takeaway is that digital technology can be applied in ways that expand the aforementioned capabilities of the party-state, but governance of its use can be managed in ways that restrict officials' discretion in applying it. This doesn't mean, however, that these regulations limit the party-state's influence. In reality, the regulations enhance their ultimate influence over digital technologies and the flow of data.

2.2 Data regulations: setting the standards

Both draft laws contain directives on how the party-state expects data security and data privacy regimes to develop. They establish that, in the PRC, data shall be collected, stored and processed in a manner that's consistent with the party-state's paramount security concepts and objectives. Especially given the party-state security concept guiding data security, it's notable that Xi Jinping has called for strengthening 'the Party's leadership over standardisation work' and has described standardisation as the 'commanding heights' of international economic and technological competition.[51]

Beyond establishing which institutions are in charge and who is responsible for data security, the draft DSL also establishes expectations about how the PRC's standardisation system is to function that are specific to data security. The draft DSL says that State Council administrative departments and other relevant State Council departments are responsible for organising 'the formulation and appropriate revision of standards related to technology and products for the development and use of data and to data security.'[52] The most relevant body under the State Council is the Standardisation Administration of China (SAC), which is an agency under the State Administration for Market Regulation. According to the revised 2017 Standardisation Law,[53] the SAC is required to oversee standards initiation and implementation. At the practical level, technical committees develop standards, which are then accredited by the SAC.[54]

The technical committees working on the standards consist of stakeholders that are mostly government entities, government-linked research institutes and commercial enterprises. Many standards they develop are mandatory requirements, which companies must also meet to successfully bid for a project domestically. A March 2021 report by *IPVM* pointed to documents such as 'GA/T1400.3—2017' on 'public security video image information application systems' developed by the Science and Technology Information Technology Bureau of the Ministry of Public Security in coordination with several companies included in the *Mapping China's Technology Giants* project, including Uniview, Hikvision and Dahua.[55]

As the standards develop domestically, they'll also be projected globally, not just through market activity but also as the PRC seeks to participate and shape international technology standards. The SAC is also responsible for representing the PRC at international standards-setting bodies.[56] Both the draft PIPL and the draft DSL have provisions stating that the state is required to participate in setting international rules and technology standards for data security and personal information protection.[57] The expansiveness of that expectation-setting creates normalised pathways for the PRC to exploit data-sharing downstream in ways that can undermine the security of other countries, as we describe in the next section.

3. Rethinking digital supply-chain vulnerability

Not all methods used to acquire data need to be intrusive, subversive, covert or even illegal—they can be part of normal business data exchanges. Figure 1 (on page 3) illustrates how a digital supply chain can be compromised without a malicious intrusion or alteration. The data-sharing relationships that bring commercial advantages are also the same ones that could compromise an organisation. Thinking about risk solely in terms of potential disruption ignores the ways in which supply-chain risk can emerge from normal processes, in which no disruption is required.

The vulnerability of supply chains was made apparent by the Covid-19 pandemic, which made supply-chain resilience even more important. As we become more digitally interconnected, the breadth of what's considered a risk to the supply chain has grown to include risks to the digital supply chain—the electronic products we rely on and the data that flows through them.

Discussions about digital supply-chain security typically prioritise the potential for disruption or malicious alterations of the supply chain. Examples include cyberattacks, altered components inserted into the supply chain and limited access to critical supplies such as semiconductors. That kind of risk from well-resourced state and non-state actors is already well understood by governments thinking about supply-chain security.[58] As we noted in the section on 'The PRC's data ecosystem', the PRC's sophisticated offensive cyber capability and its ability to obtain data through those methods are also well known. But a digital supply chain threat doesn't necessarily require malicious alterations or cyber intrusions into a network.

The SolarWinds supply-chain attack of 2020 is one example of a supply-chain cyberattack perpetrated through the malicious insertion of software. In that case, threat actors, probably of Russian origin,[59] compromised the software update service for the SolarWinds Orion platform to facilitate the distribution of malicious code to Orion customers.[60]

Another cybersecurity risk in the supply chain that's hidden in plain sight comes from 'white labelling' of original equipment manufacturer (OEM) products.[61] That was the case with US-headquartered Honeywell, which came under scrutiny in 2018 for selling Dahua cameras under its own brand, as Dahua was banned in the US under the National Defense Authorization Act.[62] A simple example of risk for customers in this situation is that they may be monitoring cybersecurity vulnerabilities for Honeywell products, not knowing that in fact they should also be monitoring vulnerabilities for the underlying Dahua product.

Other areas of discussion include vendor trustworthiness. The 5G vendor debate within Australia a few years ago brought to light the importance of the ownership and control of network infrastructure.[63] More broadly, it made organisations consider the risk of the vendors whose equipment their organisations' data would be passing through and the obligations that those vendors have to their 'home' governments.[64] Australia's lead cybersecurity agency, the Australian Cyber Security Centre, in its guidance to organisations on identifying digital supply-chain risks, addresses this need to take into consideration foreign control, influence and interference.[65]

While these discussions are likely to lead to important policy responses that address some digital supply-chain vulnerabilities, they don't capture the full scope of risk that currently exists. In the SolarWinds and Honeywell examples above, those charged with ensuring cybersecurity usually look for changes to normal activity as an indicator of a problem or threat. In cases where the risk lies within standard data exchange processes, therefore, it could be easily missed.

3.1 Downstream data access: the GTCOM case study

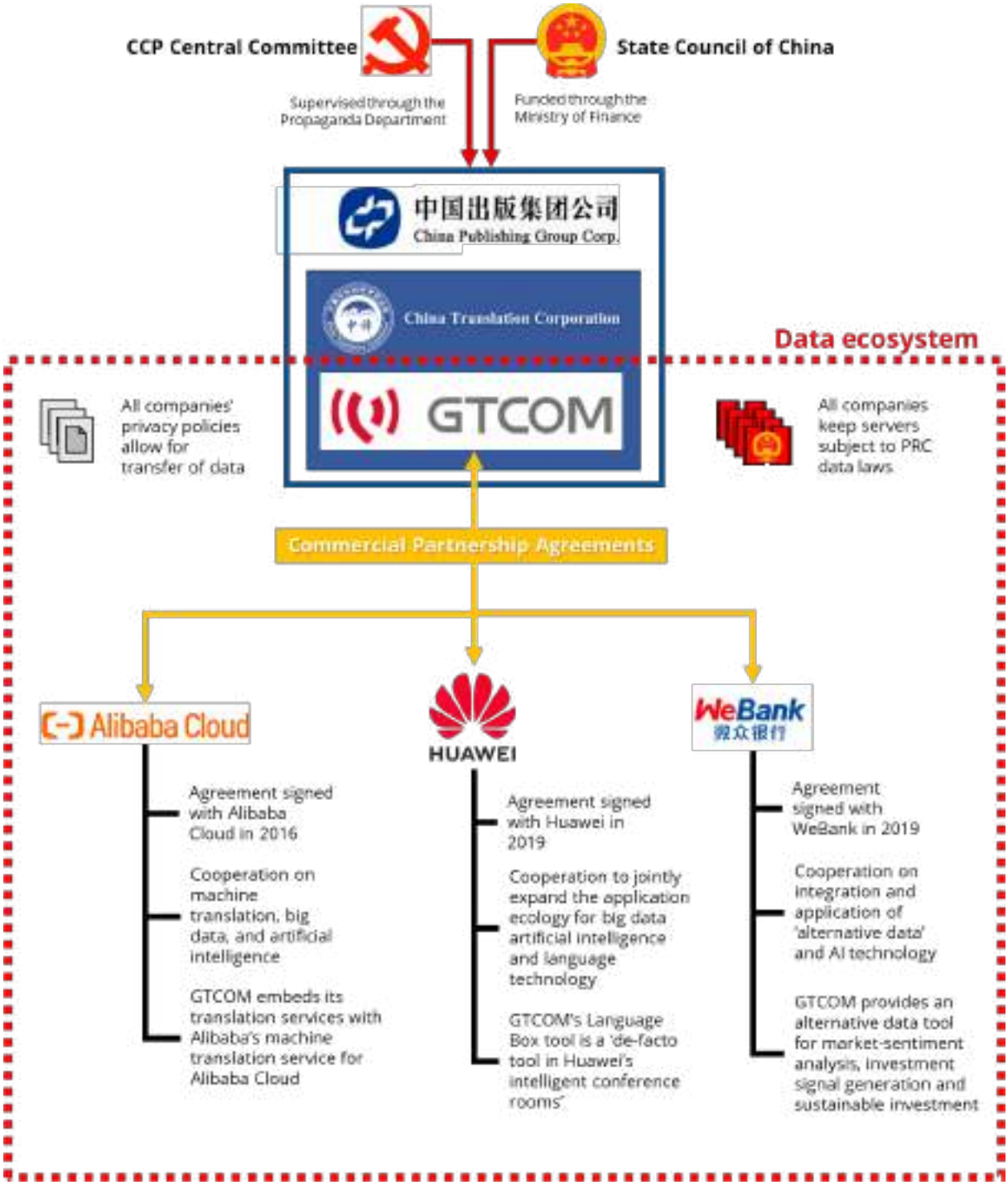
The ASPI ICPC policy brief *Engineering global consent* focused on Global Tone Communication Technology Co. Ltd (GTCOM), which is a subsidiary of a state-owned enterprise directly controlled by the Central Propaganda Department of the CCP that collects bulk data globally in support of the party-state's propaganda and state security objectives.[66] The data ecosystem emerging from GTCOM's commercial partnerships includes some of the PRC's largest and most important technology companies. For GTCOM, strategic cooperation with globally recognisable PRC-based companies—notably Huawei and Alibaba Cloud—provides assistance in two key areas in the form of:

- the opportunity to conduct bulk data collection by providing translation services to both companies, which have deeper market penetration
- the development of or access to capabilities that support its bulk data collection.

As Figure 7 shows, GTCOM has commercial partnership agreements that provide it with access to bulk data from other PRC-based technology companies.

Data transfers can occur through processes built directly into the ecosystem. A technology company such as GTCOM provides an important case study in how the data ecosystem could reach far beyond the PRC's data regulatory regime.

Figure 7: GTCOM and the global data collection ecosystem concept



Sources: ASPI authors' illustration.

3.2 Processing power

The party-state prioritises data collection domestically and globally. As we've described above, it's building an ecosystem that enables access to any bulk data collected through commercial enterprises. It further recognises that technology will eventually catch up to its ideas for processing and generating specific outputs. Being able to collect data is useful, but it's the ability to access and aggregate data for analysis and derive useful insights from it that's powerful.

The business model of internet giants such as Facebook, Google, ByteDance and Tencent heavily relies on data and the use of artificial intelligence. They collect large volumes and many varieties of data from users of their service platforms. For example, they may collect such things as user platform preferences, platform behaviours (such as how long it took an individual user to click from one page to another), how long the user stayed on a page, what products they put into their shopping cart and who their friends are, as well as real-world information such as the running routes of the user and the user's home location. The data is aggregated to generate profiles of individual users for marketing and advertising purposes, and also to improve the platform. That in turn leads to greater user engagement and provides additional opportunities to collect more data. Data brokers perform a similar aggregation and analysis task, but they usually use data that they've mined freely from the internet or purchased from other sources.

The concern isn't necessarily that data is being collected, but rather the ability to infer sensitive details about individuals from the aggregation of seemingly innocuous bits of data from a variety of sources. A single geolocation coordinate out of context isn't meaningful, but, using location data from a single mobile device collected over time, it's possible to identify an individual in a household and their pattern of life. All that's needed is to identify their three primary locations—home, work and one other regularly used location.

That kind of data can be used to target individuals, such as by identifying and tracking the movements of the US President,[67] and can identify sensitive military locations *en masse*,[68] but it can also be used to create convenience. Google Search results provide popular times, wait times and visit durations for all users searching for a local business by using 'aggregated and anonymised data from users who have opted in to Google Location History'.[69]

The use of big data analytics to monitor operations in smart cities can bring greater efficiency benefits to operations, facilitate data sharing and assist with decision-making and situational awareness overall. However, that same data, in the hands of adversaries, could give them macro-scale insights that would otherwise be difficult to obtain. If those systems are under the control of adversaries, the concern isn't just about others having access to the data but also about adversaries' ability to control or modify the data. As a consequence, the information used to create convenience, improve efficiency and enhance situational awareness is the same information that can be used by an adversary.

The ability of some PRC-based technology companies to process big data is sufficiently large. According to reporting in *Foreign Policy,* they've been used by the party-state to carry out intelligence tasks. According to 'current and former officials' cited in the report, this has included the acquisition of datasets from large data breaches, such as the 2014 cyber intrusion into the US Office of Personnel Management.[70] It's big data analysis like this that the US Central Intelligence Agency believes enabled

the exposure of its undercover officers in Africa and Europe.[71] The question that requires further research and analysis is why those PRC-based companies were chosen. For instance, were they chosen not just for their processing ability but also because, by ingesting the datasets and combining the data with their own holdings, they could enrich the information that could be derived from the data?

Commercial businesses aren't the only entities carrying out large-scale data processing in the PRC. The party-state is also doing it at the national level. The People's Bank of China has included a 'Big Data Analytics Centre' as part of the design of the PRC's 'Digital Currency / Electronic Payments' system. The bank's officials have said that the data collected through the system will be used to improve macroeconomic policy. The bank will 'analyse how money is being used, transacted, and stored; support tracking and surveillance using both static and real-time data; provide data and analysis inputs for monetary policy; and flag financial fraud'.[72]

Goals associated with harnessing the strategic power of data are a natural extension of long-enshrined goals in authoritative party-state documents and embedded in detailed economic policies and plans to ensure progress toward those goals.[73] However, the party-state's development of theory and policy is an iterative process and has always involved a degree of experimentation to ensure progress without too many unintended consequences.[74] Control or the preservation of the CCP's power isn't a goal unto itself, but rather a prerequisite for achieving those ambitions. The collection, storage and processing of big data will play an increasingly key role in those efforts in future.

4. Recommendations

Adequately evaluating the risks associated with doing business with PRC-based technology companies, or companies that rely on their technologies in their supply chains, requires an understanding of the Chinese party-state's articulation of its own intentions. It also requires an understanding of the implications of policy and legal documents that signal what steps will be taken to realise intended outcomes, as well as, of course, analysis of the party-state's actual behaviour (domestic and global).

We recommend as follows.

1. **Invest resources to better understand the PRC's and the CCP's articulation of their own intentions in order to set the tone for a more informed public debate that will generate targeted responses to the identified problems.**

   Incorrect assumptions are often made about the party-state's intent. In addition, what's being articulated and signalled through PRC policy and legal documents is too often ignored or not placed into the context in which it's being articulated or signalled (such as being placed in an appropriate political context) or being described (for example, in the light of the CCP's view that data security is a problem of state security, as the party-state defines 'state security').

2. **Recalibrate data security policy and privacy frameworks to account for the Chinese state's use of data to reinforce its political monopoly.**

   Companies and governments too often assume that other governments' data and privacy regulations share the same goals as their own. That isn't true when it comes to the Chinese party-state and PRC-based companies, even if common vocabularies are used or if some policy drivers are similar. In the PRC, unlike in liberal democracies, data security and privacy concepts (including draft legislation) reinforce the party-state's monopoly power. Companies and governments need to recognise this risk and calibrate their policies to account for it.

3. **Collaborate with like-minded countries to develop systems for improving risk-based approaches to improving the regulation of data transfers.**

   Organisations must assess the value of their data, as well as the value of that data to any potential party in their supply chain that may have access to it or that might be granted access. In an age in which information warfare and disinformation campaigns occur across social media platforms and are among the greatest threats to social cohesion, data that's about public sentiment is as strategically valuable as data about more traditional military targets. Risk needs to be understood in a way that keeps up with the current threat landscape, in which otherwise innocuous data can be aggregated to carry meaning that can undermine a society or individuals.

4. **Take a multidisciplinary approach to due diligence.**

   Governments, businesses and other organisations need to develop frameworks for conducting supply-chain reviews that take into account country-specific policy drivers**.** Developing such a framework shouldn't be limited to just assessing a vendor's risk of exposure to political risk. It should also include detailed analysis of the downstream actors who have access to the vendor's data (and must include analysis of things such as the broader data ecosystem they're a part of and the obligations those vendors have to their own governments). Taking this more holistic approach to due diligence will better ensure that data can be protected in an effective way.

Appendix: The draft Data Security Law and draft Personal Information Protection Law

Law	Article	Text
DSL	2	在中华人民共和国境内开展数据处理活动及其安全监管,适用本法。在中华人民共和国境外开展数据处理活动,损害中华人民共和国国家安全、公共利益或者公民、组织合法权益的,依法追究法律责任。 This law applies to data-handling activities and security regulation carried out within the territory of the People's Republic of China. Data-handling activities carried out outside the territory of the PRC that harm the state security, the public interest, or the lawful rights and interests of citizens' and organisations of the PRC, are to be pursued for legal responsibility in accordance with law.
DSL	4	维护数据安全,应当坚持总体国家安全观,建立健全数据安全治理体系,提高数据安全保障能力。 The preservation of data security shall adhere to the comprehensive state security outlook, establish and complete data security governance systems, and increase capacity to ensure data security.
DSL	5	国家保护个人、组织与数据有关的权益,鼓励数据依法合理有效利用,保障数据依法有序自由流动,促进以数据为关键要素的数字经济发展。 The state is to protect the rights and interests of individuals and organisations with regard to data; encourage the lawful, reasonable and effective use of data; ensure the lawful and orderly free flow of data; and promote the development of a digital economy with data as a key factor.
DSL	6	中央国家安全领导机构负责数据安全工作的决策和统筹协调,研究制定、指导实施国家数据安全战略和有关重大方针政策。 The central state security leading mechanism is responsible for decision-making and overall coordination on data security work, and researching, drafting and guiding the implementation of national data security strategies and relevant major guidelines and policies.
DSL	7	各地区、各部门对本地区、本部门工作中产生、汇总、加工的数据及数据安全负主体责任。工业、电信、交通、金融、自然资源、卫生健康、教育、科技等主管部门承担本行业、本领域数据安全监管职责。公安机关、国家安全机关等依照本法和有关法律、行政法规的规定,在各自职责范围内承担数据安全监管职责。国家网信部门依照本法和有关法律、行政法规的规定,负责统筹协调网络数据安全和相关监管工作。 Each region and department bears primary responsibility for that region's or department's efforts on data production, aggregation and processing, as well as data security. Regulatory departments such as for industry, telecommunications, communications, finance, natural resources, health, education, science and technology are to undertake data security regulatory duties in the corresponding sector. Public security organs, state security organs and so forth are to undertake data security regulation duties within the scope of their duties in accordance with the provisions of this Law, relevant laws and administrative regulations. The state cybersecurity and informatisation departments are to take responsibility for overall coordination of network data security and relevant regulatory efforts in accordance with this Law, relevant laws and administrative regulations.
DSL	11	国家积极开展数据领域国际交流与合作,参与数据安全相关国际规则和标准的制定,促进数据跨境安全、自由流动。 The state is to actively carry out international exchanges and cooperation in the data field, participate in the formulation of international rules and standards related to data security, and promote the cross-border secure and free flow of data.
DSL	14	国家实施大数据战略,推进数据基础设施建设, 鼓励和支持数据在各行业、各领域的创新应用。县级以上人民政府应当将数字经济发展纳入本级国民经济和社会发展规划,并根据需要制定数字经济发展规划。 The state is to implement a big data strategy, advancing the establishment of data infrastructure, and encouraging and supporting innovative applications of data in each industry and field. People's governments at the county level or higher shall include the development of the digital economy in the national economic and social development plans for that level, and draft development plans for the digital economy as needed.
DSL	15	国家支持数据开发利用和数据安全技术研究,鼓励数据开发利用和数据安全等领域的技术推广和商业创新,培育、发展数据开发利用和数据安全产品和产业体系。 The state is to support research into data use and development and data security techniques, encourage the spread and commercial innovation in areas such as the use and development of data and data security, and foster and develop the use and development of data, data security products and industrial systems.

Law	Article	Text
DSL	16	国家推进数据开发利用技术和数据安全标准体系建设。国务院标准化行政主管部门和国务院有关部门根据各自的职责,组织制定并适时修订有关数据开发利用技术、产品和数据安全相关标准。国家支持企业、社会团体和教育、科研机构等参与标准制定。 The state is to advance the establishment of a system of standards for data development and exploitation technologies and data security. Within the scope of their respective duties, the State Council administrative departments in charge of standardisation and other relevant State Council departments are to organise the formulation and appropriate revision of standards related to technology and products for the development and use of data and to data security. The state is to support enterprises and social groups, educational or research bodies and so forth participating in drafting standards.
DSL	19	国家支持高等学校、中等职业学校、科研机构和 企业等开展数据开发利用技术和数据安全相关教育和培训,采取 多种方式培养数据开发利用技术和数据安全专业人才,促进人才 交流。 The state is to support schools of higher education, secondary vocational schools, scientific research institutions, enterprises and so forth in carrying out education and training related to data use and development and data security, employing diverse methods to cultivate professional data use and development and data security talent, and promote professional exchanges.
DSL	34	公安机关、国家安全机关因依法维护国家安全或者侦查犯罪的需要调取数据,应当按照国家有关规定,经过严格的批准手续,依法进行,有关组织、个人应当予以配合。 Public security organs and state security organs retrieving data as necessary to lawfully preserve state security or investigate crimes shall follow relevant state provisions and complete strict approval formalities to do so in accordance with law, and relevant organisations and individuals shall cooperate.
DSL	51	开展涉及国家秘密的数据处理活动,适用 《中华人民共和国保守国家秘密法》等法律、行政法规的规定。开展涉及个人信息的数据处理活动,应当遵守个人信息保护法律、行政法规的规定。 The Law of the People's Republic of China on the Protection of State Secrets and other relevant laws and administrative regulations are to apply to carrying out data-handling activities involving state secrets. The carrying out of data-handling activities involving personal information shall comply with laws and administrative regulations on protecting personal information.
PIPL	3	组织、个人在中华人民共和国境内处理自然人个人信息的活动,适用本法。在中华人民共和国境外处理中华人民共和国境内自然人个人信息的活动,有下列情形之一的,也适用本法: (一)以向境内自然人提供产品或者服务为目的; (二)分析、评估境内自然人的行为; (三)法律、行政法规规定的其他情形。 This law applies to the activities of organisations and individuals handling the personal information of natural persons within the territory of the People's Republic of China. This law is also applicable to activities outside the PRC that handle the personal information of natural persons within the territory of the PRC, in any of the following circumstances: (1) for the purpose of providing products or services to natural persons within the territory; (2) to analyse and assess the conduct of natural persons within the territory; (3) in other situations provided for by law or administrative regulations.
PIPL	4	个人信息是以电子或者其他方式记录的与已识别或者可识别的自然人有关的各种信息,不包括匿名化处理后的信息。个人信息的处理包括个人信息的收集、存储、使用、加工、传输、提供、公开等。 Personal information is any type of information that identifies or can identify natural persons recorded electronically or by other means, but does not include anonymised information. Handling of personal information includes the collection, storage, use, processing, transmission, provision, disclosure etc. of personal information.
PIPL	12	国家积极参与个人信息保护国际规则的制定,促进个人信息保护方面的国际交流与合作,推动与其他国家、地区、国际组织之间的个人信息保护规则、标准等的互认。 The state is to actively participate in the formulation of international rules for personal information protection, promote international exchanges and cooperation on personal information protection, and promote mutual recognition of rules and standards for the personal information protection with other countries, regions and international organisations.

Law	Article	Text
PIPL	19	个人信息处理者处理个人信息,有法律、行政法规规定应当保密或者不需要告知的情形的,可以不向个人告知前条规定的事项。紧急情况下为保护自然人的生命健康和财产安全无法及时向个人告知的,个人信息处理者应当在紧急情况消除后及时告知。 When personal information handlers handle personal information, where there are circumstances that laws and administrative regulations provide shall be kept confidential or need not be announced, it is acceptable not to notify the individual of the matters specified in the preceding article. If an individual cannot be notified in time to protect the life, health and property safety of natural persons under an emergency, the personal information handler shall promptly notify the individual after the emergency is eliminated.
PIPL	34	国家机关为履行法定职责处理个人信息,应当依照法律、行政法规规定的权限、程序进行,不得超出履行法定职责所必需的范围和限度。 State organs handling personal information in order to perform their legally prescribed duties shall do so in accordance with the authority and procedures provided by laws and administrative regulations, and must not exceed the scope and limits necessary for performing their legally prescribed duties.
PIPL	35	国家机关为履行法定职责处理个人信息,应当依照本法规定向个人告知并取得其同意;法律、行政法规规定应当保密,或者告知、取得同意将妨碍国家机关履行法定职责的除外。 State organs handling personal information in order to perform their legally prescribed duties shall notify the individuals and obtain their consent as provided in this Law, except where laws and administrative regulations provide that it shall be confidential or where giving notice and obtaining consent would impede the performance of the state organs' legally prescribed duties.

Notes

1 Mapping China's Tech Giants, online.
2 Samantha Hoffman, *Engineering global consent: the Chinese Communist Party's data-driven power expansion*, ASPI, Canberra, 14 October 2019, online.
3 Hoffman, *Engineering global consent: the Chinese Communist Party's data-driven power expansion*.
4 'Two Chinese hackers working with the Ministry of State Security charged with global computer intrusion campaign targeting intellectual property and confidential business information, including COVID-19 research', news release, US Department of Justice, 21 July 2020, online; 'Chinese military personnel charged with computer fraud, economic espionage and wire fraud for hacking into credit reporting agency Equifax', news release, US Department of Justice, 10 February 2020, online.
5 The Open Systems Interconnection model provides a standard for systems to communicate with each other. It has several layers that data must pass through, from the user-facing 'application layer' and the 'physical layer', which is the physical medium that connects systems, in order to exchange data between systems. In between are layers that define how the data must be presented, packetised and sessionised in order to travel across the network.
6 Rebecca Heilweil, 'Why algorithms can be racist and sexist', *Vox*, 18 February 2020, online.
7 Jenny Darmody, 'For smart cities to work, they need to be "neutral and objective"', *Siliconrepublic*, 12 May 2021, online.
8 For instance, Karen Hao, 'This is how AI bias really happens—and why it's so hard to fix', *MIT Technology Review*, 4 February 2019, online.
9 Carla Hobbs, *Europe's digital sovereignty: from rulemaker to superpower in the age of US–China rivalry*, European Council On Foreign Relations, 30 July 2020, online.
10 Adam Satariano, Monika Pronczuk, 'Europe, overrun by foreign tech giants, wants to grow its own', *New York Times*, 19 February 2020, online.
11 'Dahua and Hikvision co-author racial and ethnic PRC police standards', *IPVM*, 30 March 2021, online; Leo Kelion, 'Huawei patent mentions use of Uighur-spotting tech', *BBC*, 13 January 2021, online.
12 Read about 'key personnel' in 'China: Police "big data" systems violate privacy, target dissent', *Human Rights Watch*, 19 November 2017, online.
13 '国家大数据战略' [National Big Data Strategy], *People's Daily*, 12 November 2015, online.
14 See Chapter 28, Section 2 in '中华人民共和国国民经济和社会发展' [Outline of the 13th Five-Year Plan for the National Economic and Social Development of the People's Republic of China], *Gov.cn*, 17 March 2016, online.
15 '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 14th Five-Year Plan for National Economic and Social Development and long-range objectives for 2035], PRC Government, 13 March 2021, online.
16 '共建 共治 共享——民进中央"提升基层治理效能·促进社会和谐稳定"重点考察调研综述' [Co-construction, co-governance, and co-sharing: Summary of Central Committee of the China Association for Promoting Democracy's key investigations on 'improving the effectiveness of grassroots governance and promoting harmony and stability of the society'], National Committee of the Chinese People's Political Consultative Conference, 9 September 2020, online; '国家大数据战略——习近平与"十三五"十四大战略' [National Big Data Strategy: Xi Jinping and the fourteen grand strategies of the '13th five-year-plan'], *Xinhua*, 12 November 2015, online; '第四届互联网大数据与社会治理南京智库峰会举行' [The 4th Internet Big Data and Social Governance Nanjing Think Tank Summit was held], *Xinhua*, 13 November 2020, online; Fengli Wang, Li Zhang, '大数据技术提升社会治理能力' [Big data technology enhances social governance capabilities], *China Social Science Net*, 10 June 2020, online.
17 Samantha Hoffman, 'Programming China: the Communist Party's autonomic approach to managing state security', PhD thesis, University of Nottingham, 29 September 2017.
18 For more on this topic, see the 'Service-oriented management' section in Samantha Hoffman, 'Grasping power with both hands: social credit, the mass line, and party control', *China Brief*, 10 October 2018, online.

19 Maya Wang, 'China's algorithms of repression: reverse engineering a Xinjiang police mass surveillance app', *Human Rights Watch*, May 2019, online.

20 For instance, the description of Guizhou's National Defense Mobilization Command Information System as being reliant on the 'Guizhou Cloud' big-data platform, which is described as being inclusive of dozens of 'thematic clouds' and clouds' prefecture-level administrative divisions. '国防动员 · 再不牵手大数据就晚了' [National defence mobilisation, it would be too late to hold hands with big data (if not doing it now)], *Xinhuanet*, 6 June 2016, online; '成功案例' [Successful cases], Cinasoft, online; '公司简介' [Company introduction], Cinasoft, online; Cheng Miao, Feng Xinyi, '贵州大数据智库平台 : 助推政府管理和社会治理创新' [Guizhou big data think tank platform: boosting government management and social governance innovation], *Xinhuanet*, 19 January 2018, online; Hu Xiao, '"云上贵州"平台上线 建设"7+N"多云' ['Guizhou Cloud' platform was launched, constructed '7+n' clouds], *People's Daily*, 20 October 2014, online; '贵州携阿里云造中国"数据之都' [Guizhou and Alibaba Cloud jointly build China's 'data capital'], *People's Daily*, 22 December 2014, online.

21 '透析国家安全视野中的大数据发展问题' [Analysis of the development of big data from the perspective of state security], *CPC News*, 9 November 2016, online.

22 Nigel Inkster, *China's cyber power*, Routledge, Adelphi, London, for the Institute of International and Strategic Studies, 2016, 24.

23 '拍案 | 看看这三个案例 · 青年学子可要绷紧国家安全这根弦' [Take a look a these three cases: young students must tighten the string of state security], *Xinhua*, 15 April 2021, online.

24 '委员 : 电脑操作系统太依赖进口 威胁国家安全' [Committee member: [Our] computer operating systems rely too much on imports, threatening national security], *China News*, 10 March 2009, online; '专家谈XP退休 : 严重依赖国外技术 中国信息安全形势严峻' [Experts discuss XP retirement: relying heavily on foreign technology, China's information security situation is severe], *People's Daily*, 8 April 2014, online; '人民日报整版讨论 : 抓住信息化发展的历史机遇' [*People's Daily* full-page discussion: Seize the historical opportunity of informatisation development], *People's Daily*, 12 April 2019, online.

25 Jianguo Hou, '把科技自立自强作为国家发展的战略支撑' [Taking self-reliance of science and technology as a strategic support for national development], *Qstheory*, 16 March 2021, online; '中共中央 国务院印发《国家创新驱动发展战略纲要》' [The Central Committee of the Communist Party of China and the State Council issued the 'Outline of the National Strategy of Innovation-Driven Development'], *Xinhua*, 19 May 2016, online.

26 See the 2015 'Notice from the State Council on issuing the action outline for promoting the development of big data', online.

27 'Chinese standards going global an unavoidable trend', *Global Times*, 28 April 2020, online.

28 The number in brackets corresponds with citations for claims in the graphic's text:
[1] Many of the party-state's founding generation shared with the PRC's other reformers and revolutionaries a vision of a modern China becoming both wealthy and strong. See John Delury, Orville Schell, *Wealth and power: China's long march to the twenty-first century*, Random House, 16 July 2013. Xi Jinping calls this the party's 'original aspiration'. In his speech to the 19th Party Congress, Xi stated that 'The original aspiration and the mission of Chinese Communists is to seek happiness for the Chinese people and rejuvenation for the Chinese nation.' See Xi Jinping, 'Secure a decisive victory in building a moderately prosperous society in all respects and strive for the great success of socialism with Chinese characteristics for a new era', *Xinhua*, 18 October 2017, online.
[2] Samantha Hoffman, *Engineering global consent: the Chinese Communist Party's data-driven power expansion*; Liza Tobin, 'Xi's vision for transforming global governance: a strategic challenge for Washington and its allies', *Texas National Security Review*, November 2018, 2(1), online.
[3] '新华国际时评 : 破解全球治理赤字难题需要新钥匙' [Xinhua international commentary: A new key is needed to solve the problem of global governance deficit], *Xinhua*, 24 January 2019, online.
[4] Fengrong Zuo, '全球治理中的国际话语权' [International discourse power in global governance], *China Worker Net*, 22 November 2019, online.
[5] Nadège Rolland, *China's vision for a new world order*, NBR special report no. 83, National Bureau of Asian Research, 27 January 2020, online.

29 The Counter Espionage Law (2014), the State Security Law (2015), the Foreign Non-governmental Organisation Management Law (2016), the Cybersecurity Law (2016) and the Intelligence Law (2017), among others.

30 The Australian Cyber Security Centre, in its guidance to organisations for identifying cyber supply-chain risks, covers this under 'Foreign control, influence and interference'. See *Identifying cyber supply chain risks*, Australian Cyber Security Centre, January 2021, online; Max Smolaks, 'No backdoor, no backdoor … you're a backdoor! Huawei won't spy for China or anyone else, exec tells MPs', *The Register*, 11 June 2019, online.

31 Samantha Hoffman, 'China's state security strategy: "Everyone is responsible"',*The Strategist*, 11 December 2017, online; '全民国家安全教育日 这20个法律知识你懂吗？' [National State Security Education Day: Do you understand these 20 legal trivia?]', *People's Liberation Army Daily*, 7 April 2017, online.

32 Samm Sacks, 'Data security and US–China tech entanglement', *Lawfare*, 2 April 2020, online.

33 Rob Davies, Helen Davidson, 'The strange case of Alibaba's Jack Ma and his three-month vanishing act', *The Guardian*, 23 January 2021, online.

34 Karishma Vaswani, 'Alibaba accepts record China fine and vows to change', *BBC*, 12 April 2021, online.

35 'Jack Ma shows why China's tycoons keep quiet', *New York Times*, 22 April 2021, online.

36 See 'Thematic snapshots' in the 'Analysis' section of the Mapping China's Technology Giants project. 'Thematic snapshot: Privacy policies' covers the publicly available privacy policies for the 27 companies tracked in the project, online.

37 '习近平谈法治最新金句 剖析高级干部走上犯罪道路原因' [Xi Jinping's latest key quotes on the rule of law analyse the reasons why senior cadres commit crimes], *CPC News*, 15 February 2019, online; Yixin Chen, '习近平法治思想是全面依法治国的行动指南' [Xi Jinping's thought on the rule of law is an action guide for comprehensively relying upon the law to rule the country], National People's Congress of the PRC, 14 May 2021, online; Jiafu Wang, '依法治国 · 建设社会主义法治国家' [Relying upon the law to rule the country to build a socialist country ruled by law], *Public Law*, 1997, online; '党的领导是推进全面依法治国的根本保证' [The leadership of the party is the fundamental guarantee for advancing the rule of law comprehensively], *Legal Daily*, 30 December 2020, online; Dalin Fu, '坚持党对全面依法治国的领导' [Persist in the party's leadership of comprehensively governing the country relying on law], *Qstheory*, 13 January 2021, online; Qingshan Qu, '正确认识和把握党和法的关系' [Correctly understand and handle the relationship between the party and the law], *Guangming Daily*, 16 February 2015, online.

38 中华人民共和国数据安全法 (草案) (二次审议稿) [Data Security Law of the People's Republic of China (draft) (second deliberation)], *NPC.gov.cn*, April 2021, online; 中华人民共和国个人信息保护法 (草案) (二次审议稿), [Personal Information Protection Law of the People's Republic of China (draft) (second deliberation)], *NPC.gov.cn*, April 2021, online.

39 'China's top legislature schedules standing committee session', *Xinhua*, 26 May 2021, online.

40 See Appendix: articles 2, 5, 6, 7, 14, 15, 16, 19 of the draft DSL and Article 3 of the draft PIPL; see also Chuanying Lu, '鲁传颖 : 数据安全立法 · 需平衡好各方诉求' [Lu Chuanying: Data security legislation needs to balance the demands of all parties], *Global Times*, 27 May 2020, online.

41 Draft DSL, Article 4.

42 Draft DSL, Article 6.

43 The number in brackets corresponds with citations for claims in the graphic's text.
[1] '中华人民共和国国家安全法' [State Security Law of the People's Republic of China], *Gov.cn*, 1 July 2015, online.
[2] '中华人民共和国国家安全法' [State Security Law of the People's Republic of China], *Gov.cn*, 1 July 2015, online.
[3] The concept of 'comprehensive state security outlook' articulated as it is today includes numerous component parts, in addition to those highlighted in the graphic. Rather than being new under Xi Jinping, the comprehensive state security outlook has most clearly come out of the CCP's conversation on its ability to respond to perceived threats, which has become increasingly distinct ever since the Tiananmen Massacre in 1989. By the late 1990s and early 2000s, many of the parts of state security included in Xi Jinping's 'outlook' were already being discussed as a part of state security. The 2001 Science of Military Strategy, for example, said that 'state security' is a key 'national interest' and is a 'combination of political, economic, military, cultural, information, energy and biological environment situations'. It added: 'While traditional security still exists, we cannot neglect the threat of economic, political and cultural fields. Security in non-traditional fields such as "economic security", "political security", culture and others are also important factors of state security.' One shift under Xi Jinping has been the removal of any ambiguity about the idea that every individual and entity is responsible for state security. An annual State Security Education Day is held on 15 April, In 2016, for instance, Xi Jinping emphasised that 'We must be proactive, take precautions, [react/learn] from clues that reveal a trend, nip [problems] in the bud, take the first move, take the initiative, and be prepared to deal with any forms of conflict, risk and challenge, do well at preparing for every kind of struggle [in the] economic, political, cultural, societal, diplomatic, military [realms]. All levels and everyone should take responsibility [for it].' See also '习近平这样谈总体国家安全' [Xi Jinping talks about comprehensive state security], *Science and Technology Daily*, 11 April 2020, online; Dazhi Yang, '政治安全是国家安全的根本' [Political security is the root of state security], *Qstheory*, 20 April 2018, online; Xiaofeng Yan, '人民安全是国家安全的基石' [The people's security is the cornerstone of state security], *PLA Daily*, 12 June 2020, online.
[4] Andrew S Erickson, Adam P Liff, 'Installing a safety on the "loaded gun"? China's institutional reforms, National Security Commission and Sino-Japanese crisis (in)stability', *Journal of Contemporary China*, 26 October 2015, 25(98), online; Weixing Hu, 'Xi Jinping's "big power diplomacy" and China's Central National Security Commission', *Journal of Contemporary China*, 8 December 2015, 25(98):163–177, online; David M Lampton, 'Xi Jinping and the National Security Commission: policy coordination and political power', *Journal of Contemporary China*, 18 March 2015, 24(95):759–777, online; Joel Wuthnow, 'Decoding China's new "National Security Commission"', *CNA Brief*, November 2013, online; Joel Wuthnow, 'China's much-heralded NSC has disappeared', *Foreign Policy*, 30 June 2016, online.
[5] '林铎在省委国家安全委员会第一次会议上强调全面贯彻落实总体国家安全观 努力推动国家安全工作上台阶唐仁健出席' [Lin Duo emphasised at the first meeting of the State Security Committee of the Provincial Party Committee to fully implement the overall state security concept and strive to promote state security work, Tang Renjian attended], *Gansu Daily*, 29 December 2018, online; '河南省级机构改革 : 设党委机构18个 政府机构42个' [Henan Provincial Institutional Reform: Set up 18 party committees and 42 government agencies], *Sina News*, 6 November 2018, online.
[6] '全民国家安全教育日 这20个法律知识你懂吗？' [National State Security Education Day: Do you understand these 20 legal trivia?], *People's Liberation Army Daily*, 7 April 2017, online; '中共中央印发《中国共产党政法工作条例》' [The Central Committee of the Communist Party of China issued the 'Regulations on the Political and Legal Work of the Communist Party of China'], *Xinhua*, 18 January 2019, online.
[7] Samantha Hoffman, Peter Mattis, 'Managing the power within: China's Central State Security Commission', *War on the Rocks*, 18 July 2016, online.

44 The term 'central state security leading mechanism' (中央国家安全领导机构) is used in legal documents to refer to the Central State Security Commission (CSSC; 中央国家安全委员会) because the CSSC is a party body. See '全民国家安全教育日 这20个法律知识你懂吗？' [State Security Education Day: Do you understand these 20 legal trivia?], *People's Liberation Army Daily*, 7 April 2017, online.

45 Draft DSL, Article 7.

46 Dominic Meagher, 'Has Hong Kong's national security law created secret police with Chinese characteristics?', *The Strategist*, 14 July 2020, online.

47 Draft PIPL, Article 3.

48 William Yang, 'Hong Kong: National security law targets overseas activists', *DW News*, 18 August 2020, online.

49 Draft PIPL, Article 34, also see Article 35 on notification requirements.

50 'Data security business advisory: Risks and considerations for businesses using data services and equipment from firms linked to the People's Republic of China', US Department of Homeland Security, 22 December 2020, online.

51 '开创我国标准化事业新局面——学习贯彻习近平同志关于标准化工作的重要论述' [Create a new situation in China's standardisation business—study and implement Comrade Xi Jinping's important exposition on standardisation], *People's Daily*, 6 September 2015, online.

52 Draft DSL, Article 16.

53 'Standardisation Law of the People's Republic of China', Standardisation Administration of China, 23 March 2018, online. The Standardisation Law was revised and adopted at a meeting of the Standing Committee of the National People's Congress in November 2017 and came into force on 1 January 2018.

54 'China—Standards for trade', *Export.gov*, 30 July 2019, online.

55 'Dahua and Hikvision co-author racial and ethnic PRC police standards', *IPVM*, 30 March 2021, online. See also Samantha Hoffman, *Double-edged sword: China's sharp power exploitation of emerging technologies*, National Endowment for Democracy, April 2021, online.

56 '组织机构' [Organisation], Standardisation Administration of China, online.

57 Draft DSL, Article 11; draft PIPL, Article 12.

58 For instance, see US President Biden's comments in a speech corresponding with the signing of an executive order on supply-chain security: 'Remarks by President Biden at signing of an executive order on supply chains', transcript, The White House, 24 February 2021, online.

59 Cyber Security & Infrastructure Security Agency, 'Joint Statement by the Federal Bureau Of Investigation (FBI), the Cybersecurity And Infrastructure Security Agency (CISA), the office of the Director of National Intelligence (ODNI), and the National Security Agency (NSA)', US Government, 5 January 2021, online; Andrew Roth, 'Code deployed in US cyber-attack linked to suspected Russian hackers', *The Guardian*, 11 January 2021, online.

60 The number of organisations known to have downloaded the malicious update was approximately 18,000, but the number affected could be much higher. They included both US Government and private networks and large corporations such as Microsoft, whose CEO, Brad Smith, called it 'the largest and most sophisticated attack the world has ever seen'. 'SolarWinds hack was "largest and most sophisticated attack" ever: Microsoft president', *Reuters*, 14 February 2021, online; David E Sanger, Nicole Perlroth, Julian E Barnes, 'As understanding of Russian hacking grows, so does alarm', *New York Times*, 2 January 2021, online.

61 An original equipment manufacturer (OEM) produces products or components and sells them more cheaply in bulk to another company, sometimes without its own company branding (white labelling). The product can then be branded by the purchasing company. See 'OEM software', *Looker*, no date, online; 'Original equipment manufacturer (OEM): introduction, pros & cons', *Intrepidsourcing*, no date, online.

62 'Dahua OEM directory', *IPVM*, 5 May 2021, online; John Honovich, 'Bosch dropping Dahua', *IPVM*, 13 February 2020, online; 'Honeywell hides selling US Gov banned Chinese video surveillance', *IPVM*, 10 October 2018, online; Chris Burt, 'Bosch considers dumping Dahua cameras after biometric ethnicity-warning revelations', *Biometric*, 19 February 2021, online; John Honovich, '3 weeks later, Honeywell still cannot say whether they are vulnerable to Dahua wiretapping [now admits]', *IPVM*, 27 August 2019, online.

63 Danielle Cave, Elsa Kania, Tom Uren, Fergus Hanson, Peter Jennings, Michael Shoebridge, Samantha Hoffman, Jessica Clarence, Greg Austin, *Huawei and Australia's 5G network*, ASPI, Canberra, 10 October 2018, online.

64 Danielle Cave, 'Huawei highlights China's expansion dilemma: espionage or profit?' *The Strategist*, 15 June 2018, online; Elsa Kania, 'Much ado about Huawei (Part 2)', *The Strategist,* 28 March 2018, online; Samantha Hoffman, 'China's state security strategy: "Everyone is responsible"', *The Strategist*, 11 December 2017, online; Samantha Hoffman, '"Dangerous love": China's all-encompassing security vision', *The National Interest*, 17 May 2016, online.

65 *Identifying cyber supply chain risks*, Australian Cyber Security Centre, January 2021, online.

66 Hoffman, *Engineering global consent: the Chinese Communist Party's data-driven power expansion*.

67 Stuart A Thompson, Charlie Warzel, 'How to track President Trump', *New York Times,* 20 December 2019, online.

68 Richard Pérez-Peña, Matthew Rosenberg, 'Strava fitness app can reveal military sites, analysts say', *New York Times*, 29 January 2018, online.

69 'Popular times, wait times, and visit duration', *Google My Business Help*, online.

70 Zach Dorfman, 'How China's tech giants are giving China a vital edge in espionage', *Foreign Policy*, 23 December 2020, online.

71 Zach Dorfman, 'China used stolen data to expose CIA operatives in Africa and Europe', *Foreign Policy,* 21 December 2020, online.

72 Samantha Hoffman, John Garnaut, Kayla Izenman, Matthew Johnson, Alexandra Pascoe, Fergus Ryan, Elise Thomas, *The flipside of China's central bank digital currency*, ASPI, Canberra, 14 October 2020, online.

73 Sebastian Heilmann, Oliver Melton, 'The reinvention of development planning in China, 1993–2012', *Modern China*, 24 August 2013, online; Dan Tobin, *How Xi Jinping's 'New Era' should have ended US debate on Beijing's ambitions*, Center for Strategic and International Studies, 8 May 2020, online.

74 Timothy R Heath, *China's new governing party parad*igm, Routledge, 28 February 2019; Sebastian Heilmann, Elizabeth J Perry (eds), *Mao's invisible hand: the political foundations of adaptive governance in Chi*na, Harvard Contemporary China Series 17, Harvard University Press, 1 May 2011.

Acronyms and abbreviations

CCP	Chinese Communist Party
DSL	Data Security Law
GTCOM	Global Tone Communication Technology Co. Ltd
ICPC	International Cyber Policy Centre
OEM	original equipment manufacturer
PIPL	Personal Information Protection Law
PRC	People's Republic of China
SAC	Standardisation Administration of China

Some previous ICPC publications

ASPI
AUSTRALIAN STRATEGIC POLICY INSTITUTE

INTERNATIONAL CYBER POLICY CENTRE

TWENTY YEARS OF ASPI STRATEGY
2001 - 2021