BRITISH CHAMBER OF COMMERCE IN CHINA
中国英国商会

LexisNexis®

CROSS-BORDER DATA AND INNOVATION

2021

CONTENTS

CHAIR'S FOREWORD

Our ability to service our customers, manage our daily operations and work efficiently depends on the ability to store and process information. The foundations of business are built on data and, for many companies trading, investing and operating in China, that foundation extends to the ability to transfer information across borders. Our ability to assess market trends and to develop new products and services all depends on our ability to pool and analyse data safely, securely and efficiently, often across regions and geographies. For many, it is a source of competitive advantage.

Policy makers around the world are faced with a common dilemma: how to ensure the integrity of data and digital infrastructure, protect users, consumers and individuals in a digital-first world, without restricting or slowing the free-flow of information necessary for business to operate, invest, innovate and grow. As China moves to protect cyber, data security and personal information, many companies here are faced with uncertainty over definitions, data classifications and the processes they must follow to remain compliant. This is most notable when it comes to cross-border data transfers.

Uncertainty over cybersecurity and data protection requirements consistently feature as two of the most significant concerns voiced by British companies operating in China. Companies are wrestling to understand the evolving legal and regulatory landscape and take adequate measures to ensure compliance. Whether data are classified as important, personal or sensitive matters, as do the requirements for auditing, disclosure and the assurances needed from information managers and data handlers located outside of China.

This report by the British Chamber of Commerce in China provides the latest assessment of the regulatory landscape and perspectives from across the British business community in China. It is timely, coming just as China's new Data Security and Personal Information Protection laws come into effect and the draft External Security Assessment Measures for Cross-Border Data are published. The recommendations contained here are needed to ensure business can manage their systems and data in China.

JULIAN MACCORMAC
Chair, British Chamber of Commerce in China

EXECUTIVE SUMMARY

The flow of data, like the air we breathe, is essential for business. Without it our vitality is restricted and our ability to function soon declines. Like air, it is easy to take data for granted. We expect the systems and information our businesses rely on will be available and accessible 24 hours a day.

Data flows across borders allow business to connect and pool data across regions. They provide clients access to services and expertise from across the world and enable companies operating here to centralise processing, increase workflow efficiency, and monitor and improve product performance efficiently. We all depend on the ability readily to transfer and access data safely and securely across borders.

British companies in China are worried about new rules on cross-border data transfers and are struggling to understand the consequences from China's cyber, data and personal information protection laws. Many have serious concerns over the impact on current business operating procedures, future product development and innovation. Their supply of air, so to speak, has become uncertain.

THE ECONOMIC BENEFITS OF CROSS-BORDER DATA FLOWS

One company's breakthrough lifts the whole market. The work of UK life science start-up Ziylo on glucose-binding molecules is now being used by Danish pharmaceutical leader Novo Nordisk to develop 'smart insulin' that could help diabetes become a completely manageable condition.

This example of cross-border innovation could not happen without access to data. Cross-border data flows:

- allow experts in companies to **connect data points** from a market halfway across the world and share this knowledge with partners.
- streamline company workflows, minimising costs and **creating more resources** for R&D.
- facilitate digital trade in a range of sectors, **unlocking opportunities** for commerce and cooperation in new areas.
- improve the business environment, **strengthening investor confidence** and drawing greater inflows of foreign investment.

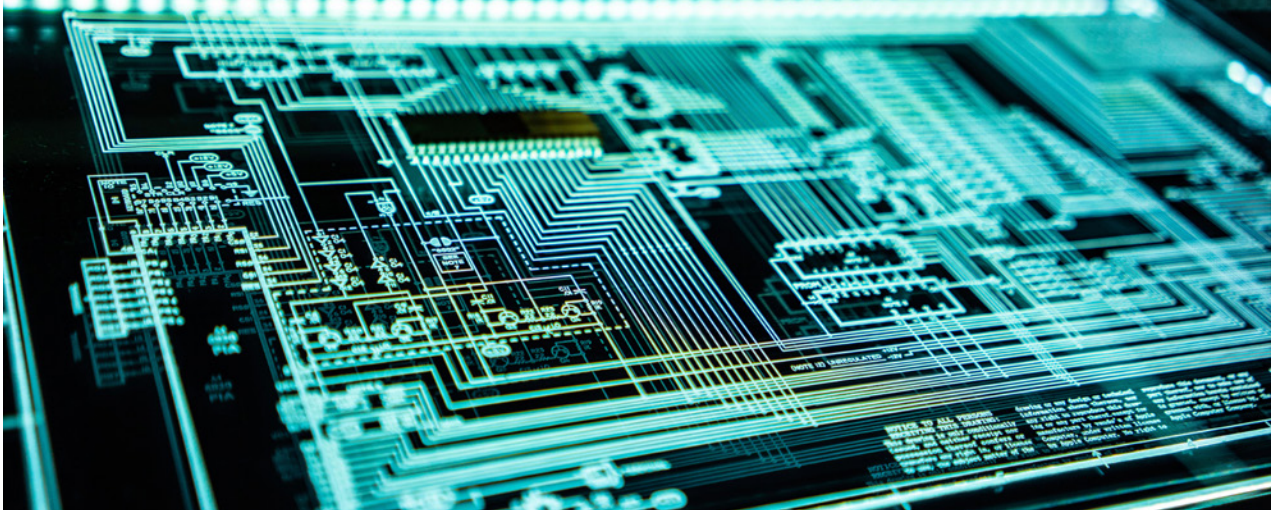
Greater data localisation, by contrast, increases friction for companies when dynamism and experimentation is key, and limits opportunities for partnership and exchange.

IMPROVEMENTS ON THE HORIZON, BUT FRAMEWORK LACKS CLARITY

The British Chamber of Commerce calls for clarity. British companies have raised uncertainty over data security and compliance since our inaugural Business Sentiment Survey in 2018. Our members welcome recent announcements from Beijing, Shanghai and other regions that may ensure that companies can continue to send low-risk data across borders under certain circumstances with relative ease. However, the landscape for cross-border data transfer currently remains unclear. Companies seek assurance. Faced with uncertainty and compliance concerns, some have delayed or cancelled projects. Others have felt compelled to downgrade or deny access to services for Chinese clients.

Compliance is the primary question businesses need to ask when faced with new laws and regulations. In China, ambiguity or uncertainty is common when new rules emerge but, in the case of data security, the consequences of new rules could be profound to how they operate and do business. Penalties for non-compliance are well-known, but we do not yet know the scope of information to which the rules apply. Recent draft laws have provided some clues about the shape of future cross-border data flows but there remains considerable anxiety around what might be classified as important data, and many questions over practicalities concerning data transfers assessment.

Requirements for cross-border data transfer must be practical, transparent and conducive to market-led innovation. Without this, businesses will face higher costs and struggle to realise their full potential to innovate and grow in the Chinese market.



1 CHINA'S INNOVATION LANDSCAPE

Very few could argue that China has not come a long way already in terms of innovation. China rose from ranking 29th in the Global Innovation Index to 12th between 2011 and 2021, driven in particular by increased global corporate spending on R&D, greater business sophistication and a focus on science, technology, engineering and mathematics (STEM) education. However, a relatively challenging business environment (39th), restrictive regulatory environment (106th) and year-on-year decrease in the value of innovative outputs between 2019 and 2021 (from 5th to 7th) precluded China from entering the top ten most innovative nations.[1]

Gross domestic spending on R&D reached RMB 2.4 trillion (GBP 280 billion) in 2020, or roughly 2.4% of GDP.[2] Three quarters of this was generated by business – both private and state-owned.[3] In 2019, Huawei R&D spend exceeded the total R&D spend of 25 of China's provinces.[4] While estimates vary, China has anywhere between 139[5] and 264[6] unicorn companies, dominated by tech giants.

Exports of high-tech products reached USD 777 billion (GBP 577 billion or RMB 5 trillion) in 2020. Industry is also leading on employment in innovation: 49 million people were employed in R&D roles in 2020, three-quarters of which were provided by businesses.[7]

1 'Global Innovation Index 2021: Tracking Innovation Through the COVID-19 Crisis', World Intellectual Property Organisation, September 2021.

2 'China's R&D Spending Rises 10% to Record $378 Billion in 2020', Bloomberg, March 2021.

3 'China Science & Technology Statistics Data Book', Ministry of Science and Technology, March 2021.

4 'Huawei R&D Spending Surpasses That of Each of 25 Provinces in China', Global Times, September 2020.

5 'Complete List of Unicorn Companies 2021', Eqvista, June 2021.

6 'China Has 264 Unicorn Firms, US Has 240: Together They Take 80% of Global Total', China Money Network, February 2021.

7 'China Science & Technology Statistics Data Book', Ministry of Science and Technology, March 2021.

LEADERSHIP RECOGNISES NEED FOR FOREIGN PARTICIPATION IN INNOVATION

Countries around the world should "strengthen open cooperation around developing innovation capability, create linkages across the land and seas ... [and] develop mechanisms for mutual assistance between the east and west", said President Xi Jinping at the the 19th Party Congress in 2017.

This is by no means an unusual statement from China's senior leadership. In 2019, Premier Li Keqiang told the World Economic Forum that "No country can single-handedly provide all the resources and factors of innovation for producers, or offer all the needed goods and services to consumers. Nor can any country sustain its development in isolation from the global system. ... The world economy stands to benefit from a more open China."

China's leaders have called for international cooperation across a variety of areas, from green technology to COVID-19 vaccines. UK-China cooperation on innovation, particularly in science and technology, has historically been strong. The UK-China Research and Innovation Partnership Fund funded over 1,000 individual partnerships between 2014 and 2020, tackling global challenges through innovations in antimicrobial resistance, atmospheric pollution, education technology, digitalising agriculture and more. The UK is China's second-largest science partner in terms of co-publication of papers, and data suggest that papers the UK and China collaborate on are much more impactful than papers authored by researchers from one country alone.[8]

A recent dialogue between the Ministry of Science and Technology in China and the UK's Department for Business, Energy and Industrial Strategy noted the importance of cooperation in science and technology in contributing to improving the UK-China relationship, and discussed future cooperation, particularly around environmental sustainability.[9] The UK-China Joint Strategy for Science, Technology and Innovation Cooperation,[10] signed between the two departments in 2017, included open access to 'non-proprietary' data as one of the many necessary areas of cooperation to boost innovation. The UK and China as such both recognise the importance of cooperation and connectivity when it comes to data and innovation.

LIMITED FOCUS ON CROSS-BORDER DATA IN CHINA'S INNOVATION POLICY

It is therefore troubling that China's innovation policy has only very recently begun to account for the need for facilitating flows of information between businesses in China and businesses overseas, and even then little detail has been provided. The recent swirl of technology spats with the United States may have exacerbated concerns about exposure to external shocks, but many of the domestically-oriented underpinnings of China's innovation strategy, and foreign companies' place within it, have been long-established.

The concept of localising innovation has been a significant element of China's industrial policy since the unveiling of the *National Medium to Long-term Plan for the Development of Science and Technology* in 2006. This was the one of the first documents to explicitly state the importance of indigenous, market-driven innovation to China's economic development:

> *"The guiding principles for our [science and technology] undertakings over the next 15 years are: "indigenous innovation, leapfrogging in priority fields, enabling development, and leading the future". Indigenous innovation refers to enhancing original innovation, integrated innovation, and re-innovation based on assimilation and absorption of imported technology,[11] in order improve our national innovation capability."*

Foreign multinational companies would be encouraged to establish R&D centres in China and technology transfers, which favoured domestic firms over their foreign business partners, were to be "perfected".

Made in China 2025 sustained this policy trajectory. One of its key aims was to ensure that China's manufacturing industry was of a significantly higher quality and more

8 'UK Science & Innovation Network Country Snapshot: China', UK Science & Innovation Network, July 2020.

9 'The 10th Sino-British Joint Commission on Cooperation around Science, Technology and Innovation Successfully Held', Ministry of Science and Technology, May 2021.

10 'The UK and China Officially Launch the Science, Technology and Innovation Cooperation Strategy', Embassy of the People's Republic of China in the United Kingdom of Great Britain and Northern Ireland, December 2017.

11 'The National Medium- and Long-Term Program for Science and Technology Development (2006- 2020)', State Council, January 2006.

innovative by 2025.[12] Targets were set both for R&D expenditure and invention patents in manufacturing companies. The state would provide support for R&D, particularly for core technologies. While cross-border data do not feature in the plan, it did call for a stronger push to enhance data collection and data sharing, through the construction of data centres and the creation of data-sharing mechanisms. The focus on biopharma and medical devices in *Made in China 2025* is credited as a driver of the uptake of faster registration of innovative drugs, approval to use overseas clinical trial data and the development of a Market Authorisation Holder regime.

In practice, however, Made in China 2025 also created significant barriers for British companies in China. The role of state-owned enterprises is seen to have grown more entrenched due to their ability to meet state directives as market players, while at the same time the plan called for the creation of 'national champions' and for the strengthening of their ability to compete at a global level through state support. There are concerns that the emphasis on improving indigenous innovation in this way has limited opportunities for foreign firms in China, despite assurances from officials that *Made in China 2025* did not discriminate against foreign multinationals.[13] Credible reports have revealed that foreign companies were less likely to be considered as recipients of incentives to develop R&D capacity in key technologies,[14] while procurement and technology transfers have strongly favoured domestic firms.

THE 14TH FIVE YEAR PLAN

While Made in China 2025 is no longer explicitly on the agenda, innovation remains at the core of modernisation in China.[15] The 14th Five-Year Plan, released amidst acrimonious US-China relations and global economic uncertainty due to COVID-19, dedicated a full chapter to innovation – the first Five-Year Plan to do so. A greater capacity for innovation was listed as one of the main objectives of the plan, alongside economic growth and a stronger domestic market.

Three core metrics will be used to judge the success of its drive for innovation by 2025:

- A growth in investment in R&D across society.
- 12 high-value invention patents per 10,000 people.
- Value-added of core industries in the digital economy comprising 10% of GDP.

China will prioritise strategically important areas for policy support, such as biomedicine, energy, network communication, quantum information, integrated circuits and artificial intelligence.

In practice, China's recent innovation policies can be categorised into one of several themes:

- **The allocation of resources directly from the government** e.g. direct procurement, government funding through science and technology programmes, dedicated spend on basic research.
- **The allocation of resources through financial markets** e.g. encouraging banks to lend to innovative SMEs, creating technology-focused boards on stock exchanges.
- **The development of human capital** e.g. a stronger focus on science and technology in education, incentives for foreign scientists and engineers to come to China.
- **The use of fiscal policy to incentivise innovation** e.g. 75-100% tax write-offs for R&D spend, corporate income tax exemptions for strategically important sectors.
- **The improvement of evaluation of output metrics** e.g. reforming evaluation and reward mechanisms for science and technology R&D, enhancing evaluation and third-party assessment of pilot programmes.
- **The development of digital infrastructure** e.g. growing data centre compute to 200 exaflops by 2023, setting a minimum urban internet speed, encouraging the expansion of broadband connectivity across China.
- **Creating interlinked hubs for innovation** e.g. granting Shenzhen and Shanghai greater autonomy to design attractive policies for innovative companies, creating infrastructure that links growing business hubs.
- **The improvement of the business environment** e.g. strengthening protection of IP rights, increasing market access, streamlined business licence application processes.

12 'Notice on the Publication of "Made in China 2025"', State Council, May 2015.

13 'Upgrade role for foreign companies', State Council, May 2017, and 'What Signal does Li Keqiang's Visit to the China-Europe Centre in Chengdu Send?', State Council, April 2021.

14 'Made in China 2025: Is Your Business Ready?', Control Risks, February 2019.

15 'Outline of the Objectives of the 14th Five Year Plan and Long-term Vision for 2035 for Economic and Social Development', National Development and Reform Commission, March 2021.

However, China is only beginning to acknowledge the important role of cross-border data transfers and international knowledge diffusion for expanding innovation. Instead, cross-border data have been primarily linked to national security, oversimplifying its function and importance to both UK-China trade and China's economic growth.

WHY FACILITATING CROSS-BORDER DATA TRANSFERS IS ESSENTIAL TO IMPROVING INNOVATION

Data and digitalisation are now inextricable parts of daily life and doing business. From buying groceries at the supermarket to coordinating the operations of a global company, data underpin our every action and decision. This has only become more true in the age of COVID-19, lockdowns and restricted travel, where digital solutions have helped people stay connected with loved ones overseas, helped international teams coordinate on work and helped companies engage with overseas clients.

Data's potential to enhance human development is limitless. 2.5 billion gigabytes of data are generated every day.[16] These data form the basis behind discoveries of more effective life-saving drugs, more efficient modes of transport, more accessible paths for financing and cleaner methods of generating energy. While large multinationals have clear needs for optimised cross-border data flows for everything from handling employee payrolls to fuelling global R&D, small companies also benefit from affordable access to global systems, markets and datasets, helping them to compete with larger companies as they position their offerings for different markets and develop a global strategy alongside a local one.

Ensuring that the flow of data is unimpeded is vital for both trade and domestic economic growth. However, China's cross-border data activity is relatively limited. In 2017, the year that China's *Cybersecurity Law* came into effect, 704 terabits of data were transferred across borders globally every second.[17] Only 6% of this activity occurred in China.[18] By contrast, the United States, Germany and the UK – the three countries with the most cross-border data activity – saw flows of 202, 167 and 151 terabits of data every second respectively. While volume does not necessarily equate to value, the contrast remains stark.

British companies have consistently reported that navigating cybersecurity and IT restrictions, including but not limited to cross-border data transfers, is the most challenging aspect of China's regulatory environment. Data localisation requirements are already adding costs, not only in terms of building a data centre or leasing server space, but also in terms of separating and restructuring existing global and local datasets to meet new regulatory demands.

Many expect the direction of travel for China's cybersecurity and data security landscape to continue along its current, relatively restrictive trajectory. If this should happen, there will be a tangible impact on trade. An EU study found that, if the EU and China's cross-border data regulations became more restrictive, bilateral trade would drop by EUR 8 billion (GBP 7 billion or RMB 58 billion, a reduction of 1.7%), while relaxation would grow imports by over EUR 10 billion (GBP 8 billion or RMB 73 billion, a growth of 2.1%).[19] Meanwhile, a 2014 study calculated that China's enacted or proposed data legislation would shrink GDP by 1.1%, shrink domestic investment by 1.8% and shrink exports by 1.7%.[20] The World Bank similarly found that productivity would grow by 4.5% and trade in services by 5% if restrictive data policies were removed.[21]

The added costs and missed opportunities caused by data localisation have a real impact on people's livelihoods, at the expense of roughly 13% of the average worker's salary.[22] But beyond that, they drain the innovation potential of China's business environment. Slowing or limiting cross-border knowledge diffusion restricts the ability of companies to understand the performance of their products in China as compared to other markets, and create new technologies or services to build on their strengths or fix their weaknesses. Added administrative costs for complying with data localisation requirements or conducting security assessments drain capital from R&D functions. These challenges fundamentally undermine the ecosystem of innovation that China is attempting to build.

16 'Cross-Border Data Transfer Facts and Figures', Global Data Alliance, July 2021.

17 'Globalization in Transition: The Future of Trade and Value Chains', McKinsey & Company, January 2019.

18 'China and the World: Inside the Dynamics of a Changing Relationship', McKinsey Global Institute, June 2019.

19 'The Value of Cross-Border Data Flows to Europe: Risks and Opportunities', Frontier Economics, June 2021.

20 'The Costs of Data Localisation: Friendly Fire on Economic Recovery', European Centre for International Political Economy, December 2014.

21 'World Development Report 2020: Trading for Development in the Age of Global Value Chains', The World Bank, November 2019.

22 'The Costs of Data Localisation: Friendly Fire on Economic Recovery', European Centre for International Political Economy, December 2014.

2 THE CURRENT FRAMEWORK FOR CROSS-BORDER DATA TRANSFERS

The Cybersecurity Law (CSL), Data Security Law (DSL) and Personal Information Protection Law (PIPL) are the three pillars of China's cybersecurity and data protection framework. While the CSL, effective since September 2017, focuses on network security, the DSL and the PIPL put emphasis on ensuring data safety and strengthening data protection, especially important data and personal information. Currently the DSL, has been effective since 1st September 2021 while the PIPL, passed in August, came into force on 1st November 2021. The three laws represent China's development of a more robust and comprehensive data security regime.

Overview of the CSL, the DSL and the PIPL

	CYBERSECURITY LAW (CSL)	DATA SECURITY LAW (DSL)	PERSONAL INFORMATION PROTECTION LAW (PIPL)
Focus	Applicable to the construction, operation, maintenance and use of networks, as well as to cybersecurity supervision and management within the Chinese mainland.	Applicable to data handling activities and ensuring data security within the Chinese mainland. The law focuses on maintaining national and social security.	Applicable to the processing of personal information of natural persons within the Chinese mainland, and outside the Chinese mainland under certain circumstances.

Although the establishment of a regulatory system for cross-border transfers of data has gathered pace since the introduction of the CSL, requirements to localise certain types of data actually predate it. For example, a notice issued by the People's Bank of China (PBOC) in 2011 required the banking sector to store, process and analyse personal financial information of Chinese citizens or institutions within China.[23] Similarly, the State Council passed a regulation two years later that requires credit investigation companies to organise, store and process information collected in China within China's borders.[24]

Nevertheless, the CSL is the first law to outline general legal requirements for cross-border data transfers,[25] requiring that personal information and important data gathered or generated in China by critical information infrastructure operators (CIIOs) be stored in China, and that security assessments be carried out if data need to be transferred overseas for business reasons.[26] Since then, an increasingly large number of administrative measures, department rules and guidelines have been released that either echo or expand on these requirements.

23 'Notice to Banks and Financial Institutions on Protecting Personal Financial Information', People's Bank of China, January 2011.

24 'Regulations of the Administration of the Credit Investigation Industry', State Council, January 2013.

25 'Cross-Border Data Transfer: A China Perspective', Covington, February 2017.

26 'Cybersecurity Law', National People's Congress, November 2016.

The Cybersecurity Administration of China (CAC) is the primary regulator in this process, leading the drafting processes of a range of implementation regulations around cybersecurity, including on CIIOs, security assessment requirements for cross-border transfers of important and personal data, and managing data security for network operators. Most of these regulations on cross-border data transfers remain in draft form, although the *Provision for Protecting CIIOs* was passed by the State Council in August 2021. However, in certain cases industry-specific legislation will be drafted either by the CAC in partnership with another industry regulator or independently published by that industry regulator.

Moreover, as China has become increasingly wary about cross-border transfers of data in general, a number of other laws regulating specific industries have also included cross-border flows in their remit. For example, the *Biosecurity Law* requires domestic organisations that plan to share data relating to human genetic resources with foreign parties to report to and submit records to relevant regulators in space of science and technology.[27] Information deemed as sensitive to national interests and security is also subject to export control, according to the *Export Control Law*.[28] However, despite the considerable number of laws and measures released so far, as most of them either still lack implementation details or remain in draft form, businesses are still waiting for more clarity to understand how to ensure compliance when transferring data across borders.

27 'Biosecurity Law', National People's Congress, October 2020.

28 'Export Control Law', National People's Congress, October 2020.

Different regulators' responsibilities regarding cybersecurity and data protection:

REGULATORS	RESPONSIBILITIES	DRAFT LEGISLATION OF NOTE
Cybersecurity Administration of China (CAC)	Coordinating with other regulators and leading the drafting process of specific cybersecurity, data and personal information legislation, such as outlining the process for conducting security assessments for cross-border data transfers.	Revised Draft Cybersecurity Review Measures 《网络安全审查办法 (修订草案征求意见稿) 》 Draft Measures on Security Assessment for Cross-border Data Transfers 《数据出境安全评估办法 (征求意见稿) 》 Draft Administrative Measures on Network Data Security 《网络数据安全管理条例 (征求意见稿) 》
Ministry of Public Security	Supervising and administering the security of public information systems and enforcing the multiple-level protection scheme.	Provisions for the Cybersecurity Multi-level Protection System 《网络安全等级保护条例》
Ministry of Industry and Information Technology	Supervising cybersecurity and data protection in the telecommunications and internet technology sectors.	Opinions on Strengthening the Administration of the Access of Intelligent Connected Vehicle Producers and Products 《关于加强智能网联汽车生产企业及产品准入管理的意见》
Ministry of Science and Technology (MOST)	Supervising the management and cross-border transfers of human genetic data.	Provisions for the Management of Human Genetic Materials 《人类遗传资源管理条例》
Regulators of specific industries (e.g. National Health Commission, PBOC, China Banking and Insurance Regulatory Commission (CBIRC), China Securities Regulatory Commission)	Supervising data protection in the industries under their remit.	Administrative Measures on National Health Data Standards, Security and Services (Trial Implementation) 《国家健康医疗大数据标准、安全和服务管理办法 (试行) 》 Draft Administrative Measures for Credit Investigation Services 《征信业务管理办法 (征求意见稿2021年) 》

Meanwhile, the National Information Security Standardisation Technical Committee (TC260) – a subcommittee of the Standardisation Administration of China that sits under the State Administration for Market Regulation – also plays an important role in shaping the regulatory landscape. TC 260 establishes detailed standards and best practices for all market entities, through the *Guidelines on Security Assessments for Cross-Border Data Transfers*,[29] the *Information Security Technology – Guidance for Personal Information Security Impact Assessments (GB/T 39335-2020)*, and an upcoming identification guide for important data, among others. Although these are in principle recommended standards, rather than mandatory ones, they are largely taken as indicators for the direction of future regulatory updates, and are generally closely followed by industry participants.

29 'Draft Guidelines on Security Assessment for Cross-Border Data Transfers', TC 260, May 2017.

Some of the draft guidelines and measures that could indicate future compliance standards:

TITLE	REGULATOR	RELEASE DATE	IMPORTANCE
Draft Measures on Cross-border Transfers of Personal information and Important Data 《个人信息和重要数据出境安全评估办法 (征求意见稿) 》	CAC	November 2017	The first measure regarding the security assessments of cross-border data transfers published after the implementation of the CSL. Outlines steps for conducting self-assessments and external security assessments before transferring important data and personal information across borders, listing what would be assessed and criteria for what would trigger external security assessments.
Draft Guidelines on Security Assessment for Cross-Border Data Transfers (hereafter 'Draft Guidelines for Cross-Border Data Transfers') 《信息安全技术 - 数据出境安全评估指南 (草案) 》	TC 260	May 2017	Establishes detailed procedures and criteria for security assessments for transferring data across borders, applicable to both self-assessments and external assessments. While there are overlaps between the draft guidelines by TC 260 and the draft measures released by CAC, the level of detail in the guidelines is greater. It also contains an important data identification guide in the appendix.
Draft Measures on Security Assessment for Cross-border Data Transfers 《数据出境安全评估办法 (征求意见稿) 》	CAC	October 2021	The latest draft measures regarding security assessments for cross-border data transfers released by the CAC. One of the key differences between this and previous iterations is the change to the criteria that would trigger external assessments. The draft measures also state that processing times may be as long as 45 to 60 days.
Draft Administrative Measures on Network Data Security 《网络数据安全管理条例 (征求意见稿) 》	CAC	November 2021	Focuses on ways to ensure data security in order to protect personal information, national security and the public interest. In terms of cross-border data transfers, it stipulates that important data and data processed by CIIOs and processors that have handled over one million people's personal information need to be externally assessed before being transferred across borders.

PROMISING POCKETS OF CROSS-BORDER DATA FACILITATION

However, there are also indications that certain segments of the policymaking apparatus are recognising the benefits and necessity of cross-border data transfers. Some documents, such as the 14th Five-Year Plan for Developing E-Commerce,[30] state an aim to speeding up cross-border data transfers. China has also applied to join the Digital Economic Partnership Agreement, which recognises the importance of allowing businesses to transfer information across borders. Cities including Beijing and Shanghai have expressed a goal to facilitate cross-border data transfers in order to promote the development of service industries, including digital services, financial services and healthcare.

Shanghai, for instance, released an implementation plan in November 2020 to comprehensively promote its trade in services.[31] The plan includes setting up pilot schemes in the Lingang New Area on conducting security assessments of cross-border data transfers in the automotive industry and in medical research (excluding research that involves human genetic materials), amongst other areas. It also plans to allow the China branches of foreign financial institutions to transfer data to their global headquarters.

In September, the Shanghai Municipal People's Congress also released the draft *Shanghai Data Provisions*, Article 67 of which requires that a catalogue of low-risk data for cross-border data transfers be created to promote the safe and free flow of data across borders. Similarly, the Beijing municipal government released an implementation plan in 2020 stating that Beijing will explore innovative mechanisms that facilitates cross-border data transfers while also ensuring data security.[32]

These are positive first steps, and the Chinese government must ensure that it promotes a holistic policy push that ensures these goals are successfully achieved, and can be implemented nationally.

30 'The 14th Five-Year Plan for the Development of E-Commerce', Ministry of Commerce, October 2021.

31 'Implementation Plan to Enhance Innovation in Trade in Services Pilot Programme in Shanghai', Shanghai Municipal People's Government, November 2020.

32 'Implementation Plan to Enhance Innovation in Trade in Services Pilot Programme in Beijing', Beijing Economic-Technological Development Area, November 2021.

3 LACK OF CLARITY HAMPERING BUSINESS DECISION-MAKING

The lack of clarity around cross-border data transfers is the key challenge businesses face in the current legislative framework. This is particularly true for requirements to localise data. Significant confusion remains as to which data are subject to localisation requirements, and how companies can send this data overseas if they need to.

3.1 WHICH DATA AND WHAT COMPANIES ARE AFFECTED BY 'DATA LOCALISATION'?

The CSL, DSL and PIPL have slightly different focuses in terms of which data need to be localised and which are subject to external security assessments if they are being transferred overseas for legitimate reasons:

LAW	DATA
The CSL	Personal information and important data collected and generated by CIIOs within Chinese mainland.
The DSL	Important data collected and generated by CIIOs and non-CIIO processors within Chinese mainland.
The PIPL	Personal information collected and generated within Chinese mainland by ▪ CIIOs, or ▪ non-CIIOs if their processed personal information reaches a certain amount.

There is a high degree of ambiguity around the exact definitions of the key concepts, including CIIOs and important data. The DSL defines critical information infrastructure as infrastructure in telecommunications and internet services, finance, energy, transportation, public services, digital governance and other such sectors, which once damaged or whose data once leaked will severely affect national security, people's livelihoods and the public interest. This definition nevertheless remains too vague to be helpful for businesses trying to remain compliant and develop business strategies.

The broad definition of important data – data that are closely linked with issues concerning national security, economic development and the public interest[33] – is also unhelpful for businesses attempting to understand how much of their day-to-day operations are affected by related requirements. References have been made in the DSL to the development of important data catalogues by regional governments and various government departments. However, it is uncertain when these catalogues might be released. In September 2021, TC 260 released a draft *Important Data Identification Guide* which, once finalised, would be used as a reference when local governments and national-level government departments draw up their own important data catalogues.[34] However, the document is also still in draft form. Ensuring that both the guideline and finalised important data catalogues are based on rational and practical principles, and released soon is key to resolving the current regulatory limbo and encouraging digital trade, particularly digital trade in services.

33 'Draft Measures on Cross-border Transfers of Personal information and Important Data', Cybersecurity Administration of China, April 2017.

34 'Draft Important Data Identification Guide', TC 260, September 2021.

For personal information processors specifically, there is also confusion over when personal data need to go through external assessments before being sent abroad. While the PIPL stipulates that, for non-CIIOs, only processed personal information datasets that reach a certain limit need to be assessed by the national cybersecurity authority,[35] companies are not entirely clear what the limit is.

The latest *Draft Security Assessment Measures on Cross-border Transfers of Data*,[36] in its Article 4, spells out several general situations where data processors need to file with regulators for cross-border data transfers. Apart from data collected and generated by CIIOs and important data, personal information has to be assessed externally if

1. they are sent by personal information processors that have handled over one million people's personal information in China
2. personal information handlers have sent over 100,000 people's personal information or over 10,000 people's sensitive information across borders cumulatively.

Nevertheless, there is ambiguity around how these numbers are calculated and some effective industry-level regulations have set different thresholds. For example, the *Several Provisions on Auto Data Security Management (Trial Implementation)* considers any information covering over 100,000 people as 'important data', subjecting it to stricter cross-border control.[37]

Understanding the definitions of CIIOs and important data as well as thresholds is the first step for starting the cross-border data transfer process. It is thus imperative that regulators provide more clarity on these questions as soon as possible.

3.2 WHAT FORM WILL THE SECURITY ASSESSMENT PROCESSES FOR CROSS-BORDER DATA TRANSFERS TAKE?

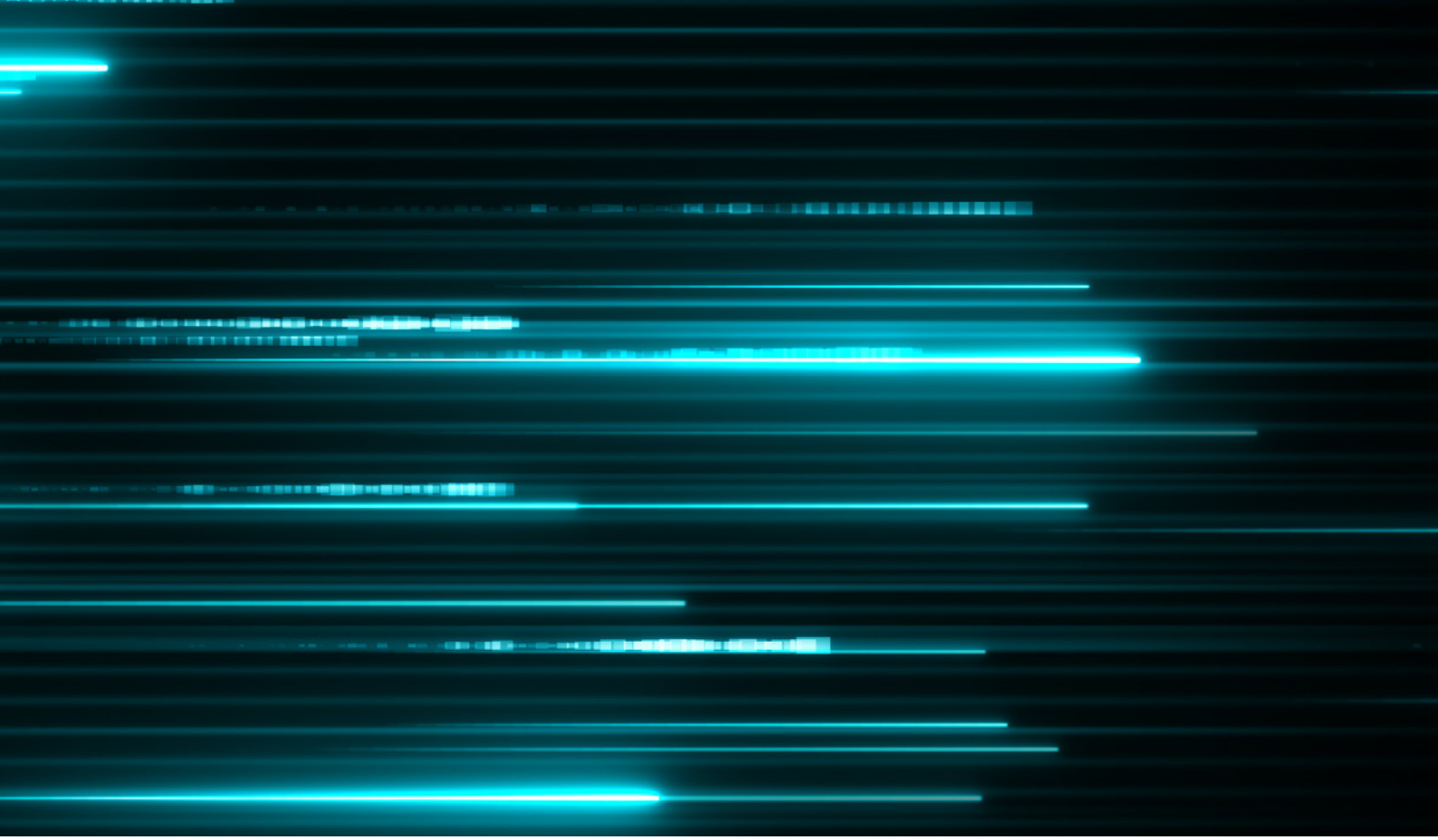
The requirements and form of the necessary security assessments also remain ambiguous. The CSL, the DSL and the PIPL authorise the national cyberspace authority and other relevant departments to further formulate relevant regulations on the security assessment. However, no rules have been finalised so far.

The CAC updated existing draft legislation on external security assessment measures for cross-border data

35 'Personal Information Protection Law', National People's Congress, August 2021.

36 'Draft Security Assessment Measures on Cross-border Transfers of Data', Cybersecurity Administration of China, October 2021.

37 'Several Provisions on Auto Data Security Management (Trial Implementation)', Cybersecurity Administration of China, August 2021.



transfers in October 2021. According to the new draft, to send personal information (once it reaches a yet-to-be-specified threshold) and important data overseas, relevant network operators need to first go through self-assessment. This determines the purpose, scope, means, legality, necessity and legitimacy of planned cross-border data transfers, amongst other things. Once data meet conditions that would trigger external assessments, the network operators in question also need to file applications, along with the results of their self-assessments with their primary regulators or supervisory authority for approval in order to send data overseas. Businesses hope that these key requirements regarding external cross-border security assessments will be confirmed as soon as possible.

Another question for companies is which regulators should conduct security assessments for cross-border data transfers. Some of the current draft measures and guidelines point to companies' primary regulators or corresponding supervisory authority, unless the relevant departments are not immediately clear, in which case the national cyberspace authority will be responsible. The *Several Provisions on Auto Data Security Management (Trial Implementation)* stipulates that these procedures will be carried out by the national cybersecurity authority in coordination with relevant departments under the State Council. The wording however, remains vague for businesses to understand which departments exactly are in charge. The latest *Draft Measures on Cross-border Data Transfers* released by the CAC also contradicts this by requiring data processors to submit applications to local-level cybersecurity authority.[38]

According to the *Draft Security Assessment Measures on Cross-border Transfers of Data*, data processers are also responsible for ensuring that the overseas data recipient securely and responsibly processes the data sent to them. However, companies are unsure what points are necessary for inclusion in agreements around data security responsibilities between the data processor and the data recipient, and would recommend that the CAC publishes a standard form of these contracts. For example, the measures state that the contract must include a binding and enforceable dispute resolution mechanism in case data recipients breach data security agreements. However, it is not clear what types of mechanisms could be considered such.

These gaps and ambiguous articles throughout China's cybersecurity legislation have created significant challenges for British companies in trying to ensure compliance, hampering their ability to use data to make business decisions at a local and global level. Greater clarity and consistency will ensure that companies can remain compliant and strengthen the attractiveness of the business environment.

38 'Draft Measures on Security Assessment for Cross-border Data Transfers', Cybersecurity Administration of China, October 2021.

4 THE IMPACT OF BURDENSOME DATA LEGISLATION ON BUSINESS OPERATIONS AND INNOVATION

Following the constraints placed on cross-border data transfers by the CSL and other draft regulations and guidelines, British businesses in China have been taking steps to identify and address gaps in compliance while closely following further legal developments.

Uncertainty around the scope of important data, CIIOs and security assessments for certain data to flow outside China is the greatest cause for concern. Even though many of the details regarding cross-border data transfers restrictions have yet to be fully formalised, businesses are already feeling knock-on effects. This is particularly true for companies in the telecommunications, finance, automotive, healthcare and energy sectors, where current regulations have, either directly or indirectly, impacted their ability to develop new products and services.

The following scenarios depict ways in which cross-border data flows are essential in order for businesses to improve efficiency and innovation, and which could be significantly impeded if current draft legislation is enacted without alteration. Without them, the threat of China offices becoming more isolated from their global headquarters and global R&D is a real possibility.

4.1 MEETING THE NEEDS OF CHINESE CONSUMERS

Companies cannot hope to understand their customers without data. Being able to access data from their customer base is crucial to identifying market trends and new areas of demand. The China offices of multinational companies must be able to ensure that customer bases' needs and preferences at the local level are being fully analysed, and they cannot do this without practical cross-border data transfer processes.

Many companies' global research centres rely on access to data in local markets in order to identify trends in various markets and to ensure that regional differences are accounted for during product development. A complete inability to access data from China would have a clear impact on the ability to test any new products' effectiveness for Chinese citizens, but delays in approving transfers of data across borders also diminish the speed with which adjustments to existing or new, innovative products can enter the market.

Currently, as industry participants await clarity around whether their data must undergo external security assessments before being sent across borders, the collection and transfer of biodata across borders already presents a significant challenge for international companies. For example, international medtech and cosmetic companies need to gather biodata of local consumers and integrate these data into their global datasets for in-depth analysis, in order to ensure the safety and effectiveness of products. However, they cannot transfer biodata outside China without MOST's permission, which requires a lengthy application process. This has caused serious disruptions and challenges for companies when conducting frontier research programs, such as polyculture and global cohort study, which provide critical insights into the effects of both existing and potential products on different populations

A range of regulations, and in particular the *Biosecurity Law*,[39] have made the cross-border transfers of biodata

39 'Biosecurity Law', National People's Congress, October 2020.

extremely restrictive. The *Biosecurity Law* requires foreign organisations that plan to conduct human genetic research to do so in partnership with a Chinese organisation. The Chinese organisation would then need to file for permission with MOST on their behalf, creating significant delays and uncertainty. The law also stipulates that companies that intend to share human genetic data with parties outside China need to first record the transfers with MOST. Companies find these processes very burdensome, particularly in terms of the sheer number of documents required, causing one company to abandon two of the three research programmes it had planned for 2021.

Considering the sensitivity of biometric data, companies often already have strict internal security policies in place. Nevertheless, it is important that data essential to facilitating R&D are allowed to be shared as long as it's secured, in order to drive innovation that ultimately benefits Chinese consumers. The burdensome application processes for conducting human genetic research and sharing related data prevent companies from pursuing innovative policies in China or developing products that deliver the best results for local patients.

4.2 HAVING A TRULY GLOBAL PICTURE

For businesses to plan their next moves, they need to be able to see the whole picture. The integration of datasets from their different offices in one central database helps decision-makers understand their business data at a global scale and therefore efficiently identify new solutions. The more complete the dataset, the better-informed business decisions will be. However, the lack of clarity around current draft regulations has raised concerns among some companies that even routine transfers of data regarding performance and internal management to headquarters may be restricted, severely inhibiting internal business performance monitoring. Without this information, it will be impossible for companies to understand how to improve efficiency and innovate for, the China market as a whole.

Meanwhile, a range of companies also rely on the information they receive from various markets to ensure they deliver high-quality products and services to customers. The reinsurance sector that helps insurance companies diversify financial risks, for instance, is highly dependent on access to personal data for risk accumulation. Cross-border data transfers allow international reinsurance companies to conduct risk accumulation on customers on the global level, which not only allows them to analyse policies customers purchase in the China market but also those outside China. This enables reinsurance companies to manage their own overall risk more effectively and arrange necessary risk diversification. Without cross-border data transfers, international insurance companies will not be able to operate efficiently and competitively in the China market.

A centralised dataset is also vital for companies that develop traditional or information infrastructure. Access to data on equipment performance sent from the device, information in fault tickets sent from clients and other sources of fault data from different markets allow them to identify key variations and adjust their products accordingly, while providing companies with a 'big picture' perspective and a more in-depth understanding of their equipment performance. Other companies prefer to produce a single, uniform product to their global client base and use global datasets in their offshore R&D centres in order to ensure such products meet all of their customers' needs, irrespective of the country in which country they are based. Reducing the speed with which data can be shared or requiring data localisation prevents companies from having a full understanding of their data. This artificially lowers their efficiency, limiting the extent to which companies can improve and innovate their products.

4.3 ENHANCING GLOBAL INTERCONNECTIVITY OF PEOPLE AND TECHNOLOGY

One of the major benefits of globalisation has been its ability to optimise the sharing of resources and ideas. With the free flow of data comes greater diffusion of expertise and knowledge across borders, rather than their concentration in a handful of countries. Whereas in the past experts and innovators had a limited sphere in which they could share new ideas, now knowledge can be shared across the world instantaneously, helping to spark new ideas and create new solutions.

Being able to consult talent from international offices in order to help local clients is a core strength of multinational companies, and technology has made this exchange easier than ever. Technology also streamlines internal workflows and operations, maximising efficiency.

For example, the China offices of a company specialising in organising English-language tests sends exam papers back to their UK headquarters to be marked and validated by a team of native English speakers. By necessity, these exams would need to include the personal information of test takers. However, this information is also crucial for companies to consider when developing new tests — which is a function the headquarters are best positioned to take on given the wider range of experts and resources available — in order to identify any weaknesses in the tests and ensure they are not missing any blind spots. If the processes needed to conduct cross-border data transfers are too burdensome, the company either would

be unable to deliver its basic business offerings or would have the quality of its services severely compromised. Many companies in the education space are therefore concerned about cross-border data transfer restrictions. Although the risk of such data transfers being banned completely is relatively low,

> *"it is hoped that clarity will be offered as soon as possible, and that processes for transferring this data will be simple and manageable."*

British engineering companies providing Chinese clients with clean energy solutions also rely on cross-border work teams to provide its regional offices with technical support from UK headquarters. However, it is essential that experts based outside of China fully understand the requirements of projects and the challenges clients in China are facing. Since 2015, one company has found its ability to share information with its global headquarters seriously restricted due to its state-owned clients' reluctance to share crucial data, as it was energy-related and therefore could be considered sensitive. As a result, when technical issues emerge with the project, technology specialists overseas could not immediately help with troubleshooting. Instead, the company has to send China-based engineers to the site, who can then only brief engineers back in the UK directly through an off-site video conference in order to find a solution. Even sending supporting written information overseas is no longer possible. This has not only significantly lowered the efficiency of workflows, but also dissuaded the company from importing new technologies to China, as the technologies are so new that only UK-based highly-specialised engineers can properly install and operate them.

Meanwhile, the Internet of Things (IoT) and digital interconnectivity of physical devices has revolutionised the way in which companies can monitor and optimise the performance of their products. Cross-border data transfers allow regional offices to access technical support from the headquarters, making sure devices run smoothly and effectively. For instance, medical devices companies that focus on treating complex diseases utilise IoT technology to analyse and fix machines deployed in regional markets remotely. When devices in regional markets become defective, a log of the issue can be uploaded to the central server in the headquarters, which will then help technicians in local markets to troubleshoot the problem. If the headquarters are not able to access information from a particular market, their ability to assist regional offices and ensure the stability and reliability of their products is compromised. In this case, it is ultimately the Chinese patient that will be most negatively impacted by these cross-border data transfer restrictions.

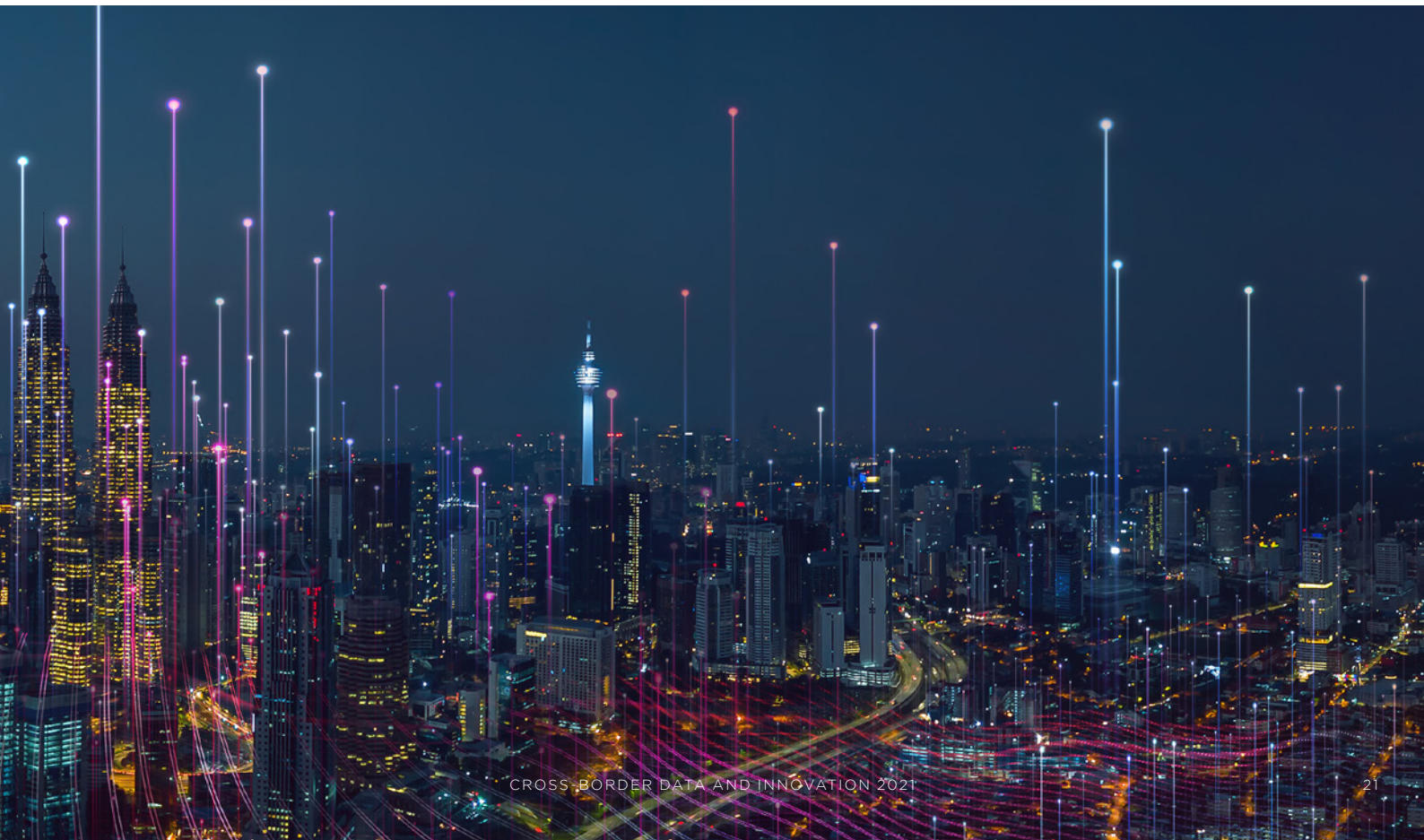
4.4 UNDERPINNING GROWTH IN FINANCIAL SERVICES

The operations of foreign financial and insurance institutions in China heavily involve cross-border transfers of clients' personal information. Not being able to access such information inhibits business activity while also making it challenging for companies to integrate their Chinese mainland datasets with those of other markets, weakening their ability to provide services and develop new products and platforms for clients that travel regularly and therefore need global financial support. Barriers to the free flow of data also inhibit the ability of multinational companies to deploy their global expertise in protection and retirement savings products to the benefit of Chinese mainland customers. This could, for example, undermine efforts to grow China's commercial pension sector, an important part of common prosperity efforts.

Solving the dilemma for businesses is crucial if China is to move ahead in its pursuit of higher level of opening-up in services sectors. Enhancing the capabilities of its financial industry has been a recent policy focus for China. Notable progress has already been made in financial services reforms and the launch of a number of pilot zones such as the Greater Bay Area (GBA). However, severe restrictions on cross-border data transfers risk defeating these goals. They are likely to slow down the development of services industries, including the insurance and reinsurance sectors, and dampen prospects for financial innovation in China, including insurance-related cross-border initiatives between the Chinese mainland and Hong Kong.

For example, the CBIRC is considering letting Hong Kong-based insurance companies establish post-sale service centres to service policyholders residing in the GBA. However, this plan can only proceed if customer data allowed to flow across the area, as the service centres would be dependent on receiving data on policyholders in real time in order to meet their needs, such as updating policy details or paying claims. Companies are unsure how feasible it would be to participate in the programme without the establishment of unimpeded data flows.

Encouragingly, the PBOC and the Hong Kong Monetary Authority (HKMA) signed a Memorandum of Understanding in October 2021 on fintech innovation supervisory co-operation in the GBA, linking up the PBOC's Fintech Innovation Regulatory Facility with the HKMA's Fintech Supervisory Sandbox in a 'network'. The arrangement aims to allow eligible financial institutions and technology firms to conduct pilot trials of cross-boundary fintech initiatives in the GBA. It represents a positive, practical attempt to facilitate financial institutions' cross-border data transfers and its successful implementation will lay a solid foundation for the integration of financial services market in the GBA. Developing a wider range of these arrangements for other sectors or between the UK and China would be significantly beneficial for bilateral trade and for greater partnership opportunities for British and Chinese businesses.



POLICY RECOMMENDATIONS

REGULATORY CHALLENGE	RECOMMENDATION
General challenges	▪ Ensure that the final scope of data considered to be important data is sufficiently broad to allow as much data exported for legitimate commercial reasons as possible to be shared without having to undergo external security assessments. ▪ Create avenues through which companies can share data with entities with which they have a legal relation, such as a sister office, parent company or subsidiary, without being required to conduct external security assessments. ▪ Streamline processes through which foreign companies can register R&D programmes, especially those involving human genetic data. ▪ Allow cities to provide broad whitelists of data that can be transferred across borders in any regional pilot zones, and implement those whitelists nationally should they prove effective. ▪ Provide clarity on how restrictions on cross-border data transfers synchronise with the regulatory arrangement on initiatives for the Greater Bay Area. ▪ Increase coordination between different regulators and ensure that industry participants are not required to go through security assessments with multiple regulators.
Difficulties understanding whether or not companies are CIIO	▪ Provide a clearer, more comprehensive definition of CIIO that allows companies to understand whether or not they would be classified as one. ▪ Publish the CIIO Catalogues. ▪ Allow a grace period for CIIOs to meet requirements after they are notified of being classified as one.

REGULATORY CHALLENGE	RECOMMENDATION
Lack of definition of important data	▪ Publish both the *Important Data Identification Guide* and subsequent Important Data Catalogues in a timely manner ▪ Refrain from including data of critical importance to commercial activities in important data catalogues.
Uncertainty around the form and requirements of external security assessments for cross-border data transfers	▪ Confirm key information regarding external cross-border security assessments, such as: 1. Which regulators will be responsible for overseeing external assessments. 2. How the size of datasets that will trigger external assessments are calculated. 3. The type of data that will be subject to assessments. 4. A comprehensive definition, including examples, of "binding and enforceable" dispute regulation mechanisms in the case of breaches of data security. ▪ Publish a standard contractual agreement between data processors and data recipients that companies can adapt. ▪ Raise the threshold of cumulative cross-border data transfers of sensitive personal information that triggers external security assessments from 10,000. ▪ Streamline the lead time for external security assessments to less than 20 working days.

ABOUT THE BRITISH CHAMBER OF COMMERCE IN CHINA

The British Chamber of Commerce in China provides advocacy, knowledge and community for British businesses in China. We operate as an independent, not-for-profit organisation with a strong and diverse membership, representing British companies across the country through our network in Beijing, Shanghai, Guangdong and Southwest China. With decades' worth of business experience in China, we are the independent voice of British business in China, bringing the British business community together and helping them thrive in one of the world's fastest growing markets.

As the voice of British business in China, BritCham advocates on behalf of our members to both the British and Chinese governments for the purpose of better directing trade relations. The dialogues we foster raise the core concerns of our members, making their voice heard in government and the wider China business environment.

Our major policy initiatives are our annual Position Paper and Business Sentiment Survey, two authoritative overviews of the needs of British businesses in the China market. Both documents examine the impact of China's regulatory system on the ability of BritCham members to thrive and provide a full range of products or services to market, and provides both policy recommendations and an overview of opportunities for British business in China. Other reports, such as the *Cross-Border Data and Innovation* report provide more focused analysis on particular facets of China's regulatory landscape. Through our engagement with the British and Chinese government we aim to foster a strong, resilient UK-China trade relationship.

ABOUT LEXISNEXIS

LexisNexis Legal & Professional is a global provider of content and technology solutions that enable professionals in legal, corporate, tax, academic and non-profit organizations to make informed decisions and achieve better business outcomes. As a digital pioneer, the company was the first to bring legal information online with its Lexis services. Today, LexisNexis Legal & Professional harnesses leading-edge technology and world-class content to help professionals work in faster, easier and more effective ways. Through close collaboration with its customers, the company ensures organizations can leverage its solutions to control risk, improve productivity, increase profitability and grow their business. LexisNexis Legal & Professional, which serves customers from all over the world with 10,000 employees worldwide, is part of RELX Group PLC, a world famous provider of information solutions for professional customers across industries.

Ever since its entry into Hong Kong in 1994, LexisNexis currently has set up Beijing, Shanghai and Guangzhou offices in mainland China. LexisNexis China collaborates with the team of experts with the practical experienced in China, relying on independent innovation technology and big data analysis, and has successively developed series of products of Lexis China and Lexis Practical Guidance. What we provide is a 360-degree solution that is a practical workflow close to legal practitioners and helping them deal with practical issues, to write legal documents, and conduct legal research efficiently, instead of merely a legal search tool.

ABOUT THE CROSS-BORDER DATA AND INNOVATION REPORT

The *Cross-Border Data and Innovation* report represents the views of members of British Chamber of Commerce in China on challenges particularly pertaining to exporting cross-border data to UK headquarters or global offices.

Navigating cybersecurity and IT regulations has been one of the top challenges facing member companies for the past three years. This report provides recommendations on how to address one aspect of this issue in order to support British businesses innovation in China and thereby boost the innovative potential of the market as a whole.

Analysis within the paper is drawn from interviews with a number of member companies. These were held with between June and July 2021, providing input from companies across industries, revenue profiles and years of experience in market.

The recommendations in this paper are indicative of priority areas as expressed by members during the data collection period and are not an exhaustive assessment of the issues faced by foreign businesses in China. The British Chamber of Commerce in China does not assume legal liability or responsibility for the accuracy and completeness of the information provided in this paper.

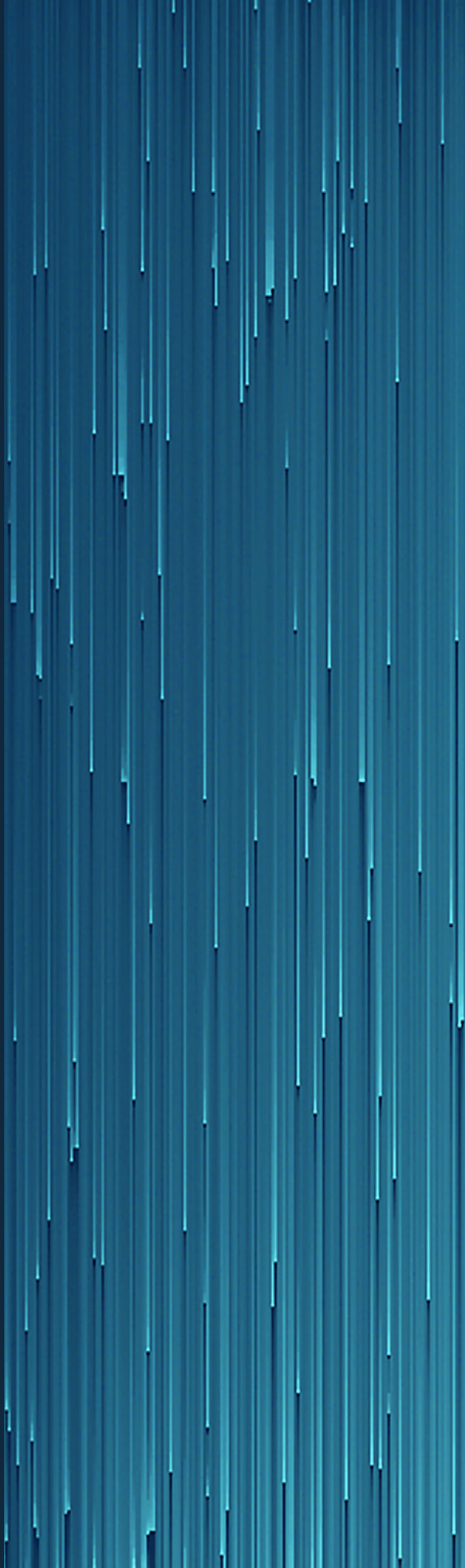
ACRONYMS

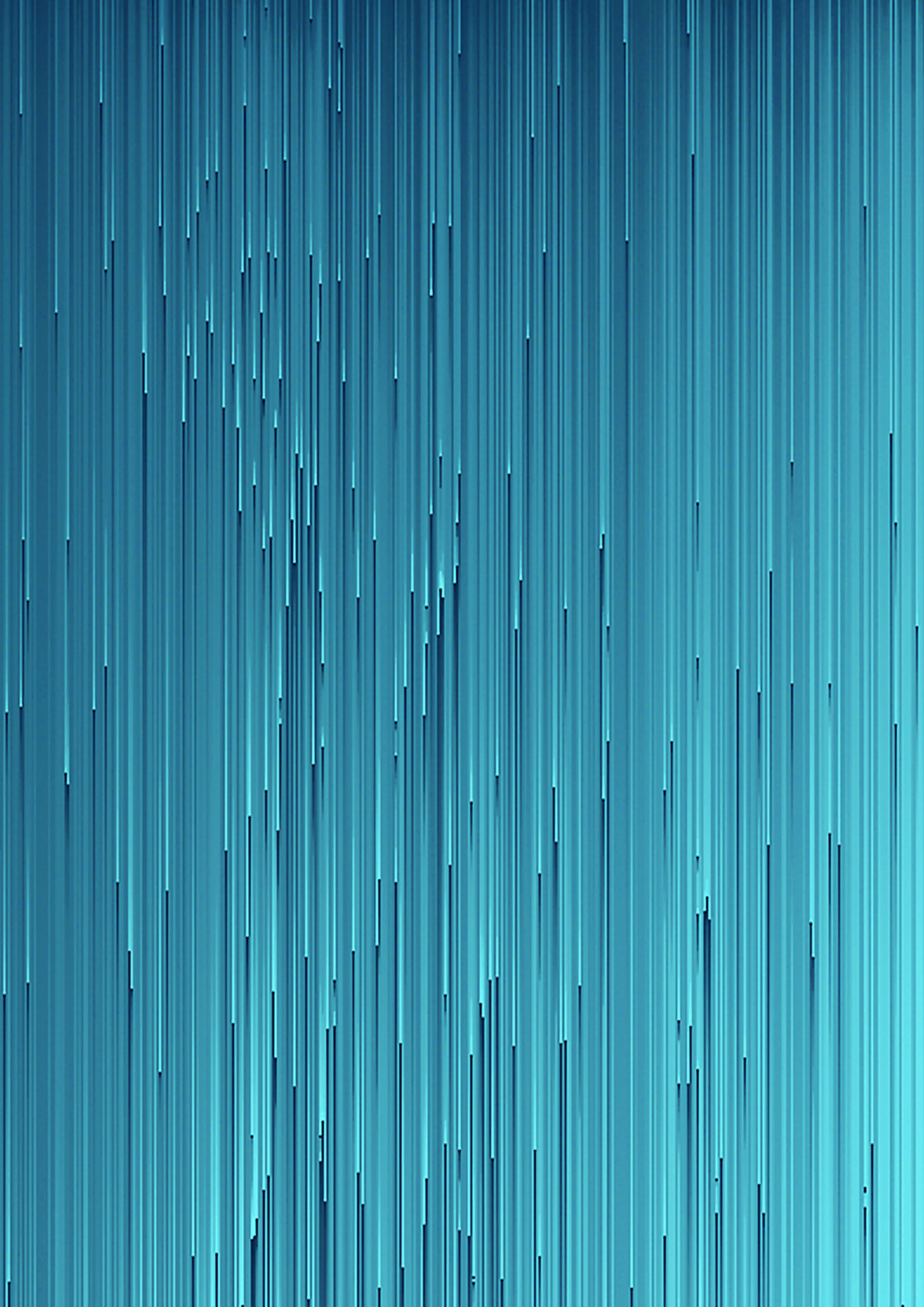
CAC	Cyberspace Administration of China
CBIRC	China Banking and Insurance Regulatory Commission
CIIO	Critical Information Infrastructure Operator
CSL	Cybersecurity Law
DSL	Data Security Law
EU	European Union
EUR	Euro
GBA	Greater Bay Area
GBP	Great British Pounds
GDP	Gross Domestic Product
HKMA	Hong Kong Monetary Authority
IOT	The Internet of Things
MOST	Ministry of Science and Technology
PIPL	Personal Information Protection Law
PBOC	People's Bank of China
R&D	Research and Development
RMB	Renminbi
STEM	Science, Technology, Engineering and Mathematics
TC 260	National Information Security Standardisation Technical Committee
USD	United States Dollars

ACKNOWLEDGEMENTS

- AUTHORS:
  Anika Patel
  Sally Xu
- DESIGN:
  Boglárka Miriszlai
- TRANSLATION:
  Practical Translations Ltd

The British Chamber of Commerce in China would like to thank our partners LexisNexis for their support during the course of producing this report, and to our contributing members for their time and insights.





NOVEMBER 2021

advocacy@britishchamber.cn

BRITISH CHAMBER OF COMMERCE IN CHINA

中 国 英 国 商 会

ADVOCACY | KNOWLEDGE | COMMUNITY