Leiden Journal of International Law (2026), **39**, 655–676
doi:10.1017/S0922156526100909

ORIGINAL ARTICLE

INTERNATIONAL LAW AND PRACTICE

Digital industrial policy through data security? – China's approach and security exceptions under trade agreements

Xiaomeng Qu[1] and Weihuan Zhou[2]*

[1]China-ASEAN Legal Research Center, School of International Law, Southwest University of Political Science & Law, Chongqing, China and [2]China International Business and Economic Law Centre (CIBEL), Faculty of Law & Justice, UNSW Sydney, Australia

Corresponding author: Weihuan Zhou; Email: weihuan.zhou@unsw.edu.au

Abstract

As industrial policy and national security become increasingly integrated, the extent to which national security may be abused to foster select economic sectors requires more dedicated studies. We make two major contributions in this paper. First, we offer a critical analysis of China's digital industrial policy, focusing on data security regulation and practices. We show that China has sought to maintain a balanced approach towards data liberalization and protection without compelling evidence to suggest abuses of national security to bolster its data sector. Yet, major loopholes remain in China's regulatory framework leaving room for discretion and abuse in deploying data security measures. As geopolitical tensions and strategic rivalries intensify, a data trade war in the name of national security is not a remote possibility. Second, we argue that the security exceptions under existing trade or digital economy agreements can hardly strike a desirable balance between data liberalization and security. Governments should join forces to modernize these exceptions, ideally via multilateral venues, by deliberating on data security goals and regulatory practices to build transparency and trust and lay the groundwork for negotiating more detailed exceptions for data security.

Keywords: China; data security; digital economy agreements; industrial policy; trade agreements

1. Introduction

Industrial policy is not new. For decades, governments have deployed such policies to foster the development of selected economic sectors or entities through a wide array of instruments.[1] Typical industrial policy instruments, such as subsidies, export restrictions, tariffs, and local content requirements, tend to generate considerable negative spillovers in both domestic and global

*The authors are grateful for constructive comments from Victor Crochet, Henry Gao, Deborah Healey, Simon Lacey, and Shin-yi Peng, Lucas Lixinski as well as for the editing assistance by Vinitika Vij.

[1]See generally D. Rodrik, 'Industrial Policy for the Twenty-First Century', (November 2004) *HKS Working Paper No. RWP04-047*, available at www.hks.harvard.edu/publications/industrial-policy-twenty-first-century; T. Nodd Tucker, 'Industrial Policy and Planning: What it is and How to Do It Better', *Roosevelt Institute*, July 2019, available at rooseveltinstitute.org/wp-content/uploads/2020/07/RI_Industrial-Policy-and-Planning-201707.pdf.

© The Author(s), 2026. Published by Cambridge University Press on behalf of The Foundation of the Leiden Journal of International Law in association with the Grotius Centre for International Law, Leiden University. This is an Open Access article, distributed under the terms of the Creative Commons Attribution licence (https://creativecommons.org/licenses/by/4.0/), which permits unrestricted re-use, distribution and reproduction, provided the original article is properly cited.

https://doi.org/10.1017/S0922156526100909 Published online by Cambridge University Press

markets due to their protective, discriminatory, and trade-distorting effects.[2] In the past, industrial policies served primarily economic goals (e.g., growing infant industries and boosting productivity and competitiveness of select industries for economic growth).[3] Recent years, however, have witnessed a dramatic shift whereby industrial policies are adopted predominantly for non-economic goals. For instance, the International Monetary Fund reported 2,500 new industrial policies around the globe in 2024: 71 per cent of them were trade-distorting while almost all were motivated by non-economic goals.[4] As Nobel laureate Professor Michael Spence has rightly observed, 'At a time of rising geopolitical tensions and supply-chain fragmentation – when national security considerations are shaping economic policy, and the risks of war seem to be intensifying – industrial policy is all but inevitable'.[5]

The new generation of industrial policy is no longer confined to consideration of economic competitiveness but embraces broader strategic, societal, and political goals. The definition of 'industrial policy' has evolved accordingly. Leading commentators have suggested that modern industrial policy involves 'those ... in pursuit of some public goal', as they are increasingly motivated by multiple non-economic objectives such as 'digitalization, the green transition ... and geopolitical imperatives'.[6]

The proliferation of modern industrial policies has gone hand in hand with the expansive use of 'national security' beyond military/defence-related interests to pursue wide-ranging economic interests.[7] Supply chain safety and technological leadership in strategic and frontier sectors, and economic competitiveness and industrialization in general, are widely viewed via a security lens,[8] rendering national security and industrial policy increasingly intertwined. In this context, governments are retreating from the conventional wisdom of free trade while using trade-distorting policies to advance domestic industrial and security interests.[9] This ongoing shift towards inward-oriented economic and security policies has exaggerated the longstanding tension between trade liberalization and domestic autonomy.

Against this backdrop, this paper explores so-called 'digital industrial policy' by focusing on data-related policies and regulation. As the world navigates the digital age, data regulation has rapidly fragmented. Governments have introduced and continue to experiment with a variety of regulatory approaches in pursuit of diverse and oftentimes competing policy goals. These range from promoting free flows of data for e-commerce, global business connectivity, and supply chains to protecting privacy and cybersecurity, fostering national digital capabilities, and pursuing

[2]See, e.g., W.C. Shih, 'The New Era of Industrial Policy Is Here. Are You Prepared?', *Harvard Business Review*, September-October 2023, available at hbr.org/2023/09/the-new-era-of-industrial-policy-is-here; IMF, OECD, World Bank and WTO, Subsidies, Trade, and International Cooperation, Analytical Notes No. 2022/001 (April 2022), available at www.imf.org/en/Publications/analytical-notes/Issues/2022/04/22/Subsidies-Trade-and-International-Cooperation-516660.

[3]See, e.g., C.P. Bown, 'Modern Industrial Policy and the WTO', (2024) 16 *Annual Review of Economics* 243, at 244–6; A. Ilyina, C. Pazarbasioglu, and M. Ruta, 'Industrial Policy is Back But the Bar to Get it Right Is High', *IMF Blog*, 12 April 2024, available at www.imf.org/en/Blogs/Articles/2024/04/12/industrial-policy-is-back-but-the-bar-to-get-it-right-is-high.

[4]S. Evenett et al., 'The Return of Industrial Policy in Data', (January 2024) *IMF Working Paper No. 2024/001*, available at www.imf.org/en/Publications/WP/Issues/2023/12/23/The-Return-of-Industrial-Policy-in-Data-542828; S. Evenett et al., 'Industrial Policy Since the Great Financial Crisis', (October 2025) *IMF Working Paper No. 2025/222*, available at www.imf.org/en/Publications/WP/Issues/2025/10/31/Industrial-Policy-Since-the-Great-Financial-Crisis-570816.

[5]M. Spence, 'In Defense of Industrial Policy', *Project Syndicate*, 5 May 2023, available at www.project-syndicate.org/commentary/industrial-policy-us-chips-and-science-act-debate-by-michael-spence-2023-05.

[6]R. Juhász et al., 'The New Economics of Industrial Policy', (2024) 16 *Annual Review of Economics* 213, at 216, 235.

[7]See, generally, H.G. Cohen, 'Nations and Markets', (2020) 23 *Journal of International Economic Law* 793.

[8]See W. Zhou et al., 'Trade vs. Security: Recent Developments of Global Trade Rules and China's Policy and Regulatory Responses from Defensive to Proactive', (2023) *World Trade Review* 193, at 193–4.

[9]U.S. economic and security policies are driving this paradigm shift and reshaping the global economic order. See, e.g., M. Fasteau and I. Fletcher, *Industrial Policy for the United States: Winning the Competition for Good Jobs and High-Value Industries* (2024). For a summary of recent rounds of U.S. tariffs and bilateral agreements with major partners for economic and security goals, see, e.g., The White House, 'Further Modifying the Reciprocal Tariff Rates', Executive Order, 31 July 2025, available at www.whitehouse.gov/presidential-actions/2025/07/further-modifying-the-reciprocal-tariff-rates/.

https://doi.org/10.1017/S0922156526100909 Published online by Cambridge University Press

strategic competition for technological supremacy. In particular, as states increasingly assert 'digital sovereignty', the intersection of industrial policy and national security has entered a new phase of legal complexity. This convergence not only challenges the integrity and predictability of the global trade regime. More broadly, it also raises systemic and fresh questions as to how to rethink security interests and their interaction with economic interests under public international law.

To contribute to the already voluminous literature on data policies and regulation, this paper focuses on examining the growing interaction between digital industrial policy and national security, using China as a case study. As explained in Section 2, digital industrial policies in major economies have been designed increasingly through a security lens. This trend generates concerns about the extent to which national security may be abused to protect or advance domestic digital industries at the cost of foreign competitors. Section 3 reviews the evolution of China's digital industrial policy with a focus on security-related data policies and regulation. After a careful analysis of China's data security laws and practices, particularly those relating to cross-border data transfers and data localization, we find no compelling evidence to suggest that China has used security-based measures to bolster its data sector. Rather, we show that China has sought to maintain a balanced approach by ensuring that data restrictive measures target genuine security risks and do not cause unnecessary burdens on business operations. However, the existence of major ambiguities in China's data security laws, the well-known lack of transparency in China's regulatory practices, etc. may provide room for abuses of national security as industrial policy in practice. To address the systemic challenges posed by the growing integration between (digital) industrial policy and national security, Section 4 discusses the inadequacies of security exceptions in existing trade or digital economy agreements in dealing with data security, focusing on the Comprehensive and Progressive Agreement for Trans-Pacific Partnership (CPTPP), the United States–Mexico–Canada Agreement (USMCA), the Digital Economy Partnership Agreement (DEPA), the Regional Comprehensive Economic Partnership (RCEP) and the Joint Statement Initiative on E-commerce (JSI) under the World Trade Organization (WTO). We then propose ways to facilitate negotiations on data security issues with the aim of modernizing the security exceptions to strike a proper balance between data liberalization and security. Section 5 sets forth the conclusion.

2. Digital industrial policy via a security lens

The rapid evolution of, and intense competition in, the digital transition worldwide have led to the development of a comprehensive digital ecosystem that ranges from enabling technologies, semiconductors, digital infrastructure and networks, and data spaces to downstream applications.[10] In this intensified digital race, '[p]olicymakers are flying blind as they shape and nurture the digital domain' through industrial policies to foster selected, domestic digital sectors and firms.[11] As a critical part of the new paradigm of industrial policy described above, digital industrial policy has been adopted for a mix of economic and non-economic goals. While in many cases such policies are driven by economic imperatives to bridge the digital divide between developed and developing economies and promote digital industrialization, they are also considered to be crucial for advancing strategic and security interests.[12] Accordingly, the term 'digital security' is no longer confined to tackling security risks in digital infrastructure, platforms,

[10]See, e.g., World Bank, *Digital Progress and Trends Report 2023* (2024), available at openknowledge.worldbank.org/server/api/core/bitstreams/95fe55e9-f110-4ba8-933f-e65572e05395/content.

[11]S. Evenett and J. Fritz, *Emergent Digital Fragmentation: The Perils of Unilateralism* (2022), at 5, 14–15, available at www.hinrichfoundation.com/research/wp/digital/emergent-digital-fragmentation-the-perils-of-unilateralism/.

[12]See, e.g., P. J. Singh, 'Digital Industrialisation in Developing Countries: A Review of the Business and Policy Landscape', (December 2017) *IT for Change Research Paper*, available at itforchange.net/sites/default/files/1468/Digital-industrialisation-May-2018.pdf; M. Musoni et al., 'Global Approaches to Digital Sovereignty: Competing Definitions and Contrasting Policy',

https://doi.org/10.1017/S0922156526100909 Published online by Cambridge University Press

networks, technologies, and products.[13] Supply chain safety, digital sovereignty, strategic autonomy, technological leadership, etc. are now integral parts of (economic) security considerations ingrained in digital industrial policies.[14] This evolving reality adds greater uncertainty and complexity to the task of disentangling protectionist industrial policies from those underpinned by genuine security concerns.

While governments pursue different policy priorities, a common area of regulatory effort has been data[15] due to the pivotal role data plays in digital transformation. Various forms of regulatory interventions have been introduced to build data-related capabilities such as subsidizing R&D, digital start-ups and the establishment of data infrastructures, and enhancing enabling regulatory frameworks for data-based digital businesses.[16] Such interventions have also been used to foster the competitiveness of national tech companies through mobilizing local data collection, restricting cross-border data flows, mandating data localization, promoting outbound foreign investment, etc.[17] Notably, the growing claim for data sovereignty can potentially become an all-encompassing policy that enables the deployment of industrial policy for a diverse range of economic and non-economic goals.[18]

There is abundant evidence to show strengthened regulatory linkages between digital industrial policy and national security, including in the data sector. One major example concerns the surge of US industrial policy in recent times to promote US global competitiveness in critical sectors, technologies, and manufacturing capabilities.[19] These industrial policies, officially labelled as the 'modern American industrial strategy', have been developing noticeably through a security lens, which may involve all matters related to economic prosperity and opportunity, democratic values, US global leadership, and strategic and geopolitical competition with China.[20] To remain the world leader in critical and frontier technologies, the US industrial strategy is determined to promote advanced manufacturing where data is the backbone of many

(May 2023) *ECDPM Discussion Paper No. 344*, available at ecdpm.org/application/files/7816/8485/0476/Global-approaches-digital-sovereignty-competing-definitions-contrasting-policy-ECDPM-Discussion-Paper-344-2023.pdf.

[13]OECD, *Economic Security in a Changing World, New Approaches to Economic Challenges* (2025), Ch. 6, available at https://doi.org/10.1787/4eac89c7-en.

[14]See, e.g., Ibid., Chs. 1–3; P. Timmers, Digital Industrial Policy for Europe, Centre on Regulation in Europe Report (December 2022), available at cerre.eu/wp-content/uploads/2022/12/Digital-Industrial-Policy-for-Europe.pdf; M. Szczepański, The Geopolitics of Technology: Charting the EU's Path in a Competitive World, European Parliamentary Research Service Briefing, PE 762.384 (September 2024), available at www.europarl.europa.eu/RegData/etudes/BRIE/2024/762384/EPRS_BRI(2024)762384_EN.pdf; IDC, 'AI Sovereignty: National Economic Competitiveness and Security', 12 February 2025, available at www.idc.com/resource-center/blog/ai-sovereignty-national-economic-competitiveness-and-security/.

[15]See Evenett and Fritz, *supra* note 11, at 21.

[16]See Singh, *supra* note 12.

[17]Ibid. For a comprehensive discussion of digital policies and transformation in the US, China, and the EU, see generally A. Bradford, *Digital Empires: The Global Battle to Regulate Technology* (2023).

[18]See Musoni et al., *supra* note 12; A. Chander and H. Sun, 'Introduction: Sovereignty 2.0', in A. Chander and H. Sun (eds.), *Data Sovereignty: From the Digital Silk Road to the Return of the State* (2023), 1.

[19]See generally S. Lincicome, 'Made in America: The Boom in U.S. Manufacturing Investment', testimony before the Joint Economic Committee of the United States Congress, 12 June 2024, available at www.cato.org/testimony/made-america-boom-us-manufacturing-investment; A. Siripurapu and N. Berman, 'Is Industrial Policy Making a Comeback?', *Council on Foreign Relations*, 18 September 2023, available at www.cfr.org/backgrounders/industrial-policy-making-comeback.

[20]See, generally, The White House, National Security Strategy (October 2022), available at bidenwhitehouse.archives.gov/wp-content/uploads/2022/10/Biden-Harris-Administrations-National-Security-Strategy-10.2022.pdf; WITA, 'Remarks on Executing a Modern American Industrial Strategy by NEC Director Brian Deese', 13 October 2022, available at www.wita.org/trade-news/remarks-on-industrial-strategy/; The American Presidency Project, 'Remarks by National Security Advisor Jake Sullivan on Renewing American Economic Leadership at the Brookings Institution', 27 April 2023, available at www.presidency.ucsb.edu/documents/remarks-national-security-advisor-jake-sullivan-renewing-american-economic-leadership-the; U.S. Department of the Treasury, 'Remarks by Secretary of the Treasury Janet L. Yellen on the U.S.-China Economic Relationship at Johns Hopkins School of Advanced International Studies', 20 April 2023, available at home.treasury.gov/news/press-releases/jy1425; A.B. Schwarzenberg, Industrial Policy and International Trade, CRS In Focus IF12119 (9 August 2024), available at crsreports.congress.gov/product/pdf/IF/IF12119.

https://doi.org/10.1017/S0922156526100909 Published online by Cambridge University Press

targeted sectors.[21] The Biden administration already constrained outbound data transfers to certain countries of concern which may use the data to develop strategic advantages over the US, threatening US national security and foreign policy.[22] While this restriction on data flows to selected countries is apparently driven by security concerns, the US government recognizes that data protection can serve multiple goals such as protecting US leadership and competitiveness.[23]

Similar regulatory developments where industrial policy and national security become increasingly integrated are also underway in other major economies. For example, faced with geopolitical shocks and uncertainties, the EU's 'New Industrial Strategy' has inevitably become multi-purpose with an emphasis on strengthening its 'strategic autonomy'.[24] When it comes to the digital domain, the Digital Agenda for Europe is currently focused on fulfilling the EU's technological and geopolitical goals by prioritizing critical and emerging technologies such as semiconductors and quantum computing, as well as security-related interests such as cybersecurity and digital sovereignty.[25] As such, the EU's digital industrial policy treats digital capabilities and competitiveness as essential security interests.[26] The EU's data strategy in particular, while maintaining a focus on the protection of individuals, sets forth a comprehensive blueprint for enhancing EU's data-related technologies, infrastructure, and capabilities as a crucial way to safeguard its fundamental values, rights, and digital sovereignty.[27]

Digital industrial policy has also gained popularity in developing economies. While these policies are aimed at advancing domestic digital sectors, including the data industry, they are also driven by non-economic goals, particularly national security and (data) sovereignty.[28] Consequently, policy tools, such as data blocking and localization, are put in place to serve multiple objectives, demonstrating the growing intersection of industrial policy and national security.[29] India has presented a more proactive case given the comprehensiveness of India's digital industrial policy and its accomplishments in enabling the regulatory environment and mobilizing diverse resources to foster the development of its digital firms and data-related

[21]See, generally, National Science and Technology Council, National Strategy for Advanced Manufacturing, Report by the Subcommittee on Advanced Manufacturing and Committee on Technology (October 2022), available at www.energy.gov/sites/default/files/2024-03/National-Strategy-for-Advanced-Manufacturing-10072022.pdf.

[22]The White House, 'Executive Order on Preventing Access to Americans' Bulk Sensitive Personal Data and United States Government-Related Data by Countries of Concern', 28 February 2024, available at www.federalregister.gov/documents/2024/03/01/2024-04573/preventing-access-to-americans-bulk-sensitive-personal-data-and-united-states-government-related.

[23]See National Science and Technology Council, *supra* note 21, at 8.

[24]See, generally, S. Tagliapietra and R. Veugelers, 'Industrial Policy in Europe: Past and Future', in S. Tagliapietra and R. Veugelers (eds.), *Sparking Europe's New Industrial Revolution: A Policy for Net Zero, Growth and Resilience* (2023), 13; European Parliament, 'General Principles of EU Industrial Policy', *Fact Sheets on the European Union*, available at www.europarl.europa.eu/factsheets/en/sheet/61/general-principles-of-eu-industrial-policy.

[25]European Parliament, 'Digital Agenda for Europe', *Fact Sheets on the European Union*, available at www.europarl.europa.eu/factsheets/en/sheet/64/digital-agenda-for-europe.

[26]European Commission, 'European Industrial Strategy', available at commission.europa.eu/strategy-and-policy/priorities-2019-2024/europe-fit-digital-age/european-industrial-strategy_en; European Commission, Communication from the Commission to the European Parliament, the European Council, the Council, the European Economic and Social Committee and the Committee of the Regions: A New Industrial Strategy for Europe, COM(2020) 102 final (10 March 2020), available at eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:52020DC0102.

[27]European Commission, Communication from the Commission to the European Parliament, the European Council, the Council, the European Economic and Social Committee and the Committee of the Regions: A European Strategy for Data, COM(2020) 66 fina (19 February 2020), available at https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:52020DC0066; M. Keck et al., 'The Role of Cross-Border Data Flows in the Digital Economy', UNCDF Policy Accelerator Brief, July 2022, 11–12, available at policyaccelerator.uncdf.org/all/brief-cross-border-data-flows#:~:text=In%20a%20digital%20economy%2C%20cross,transfer%20of%20goods%20or%20services.

[28]C. Foster and S. Azmeh, 'Latecomer Economies and National Digital Policy: An Industrial Policy Perspective', (2020) 56(7) *Journal of Development Studies* 1247, at 1257; S. Han, 'Data and Statecraft: Why and How States Localize Data', (2024) 26(2) *Business and Politics* 263, at 273–80.

[29]Ibid.

https://doi.org/10.1017/S0922156526100909 Published online by Cambridge University Press

infrastructure and capabilities.[30] At the same time, India's digital industrialization has relied on a range of laws and regulations to protect digital security, currently focusing on data security and sovereignty.[31] Data control measures such as localization requirements are employed not only as protectionist instruments but also as security instruments under India's overarching digital industrial policy.[32]

In short, as the global race for digital transformation intensifies, digital industrial policy has developed on an unprecedented scale, underpinned by both economic and security considerations.[33] This emerging trend in the development of digital industrial policy requires more detailed studies to understand how such policies now interact with security interests.

3. The evolution of China's data regulation: National security as industrial policy?

China offers a good case study for at least two reasons: (i) China's economic growth has relied heavily on industrial policies for decades, and (ii) the ambitious and fast-developing digital industrial policy in China has prioritized economic and security goals. Through a careful review and analysis of China's data-related policies and regulation, we seek to expound the extent to which the development of these policies has been shaped by security concerns and how national security may be (ab)used as a disguised protectionist tool to advance China's global leadership in digital industrialization. For this purpose, we adopt a so-called process-tracing methodology by tracing the evolution of China's data regulatory regime based on primary sources.[34]

3.1 China's digital industrial policy in a nutshell

A brief review of the evolution of China's overarching digital industrial policy provides an important context for understanding its regulatory framework for data. This evolution dates to the 1990s and covers at least three main phases. In the first phase, up to 2005, China's primary goal was to foster the infant information industry, particularly the manufacturing capabilities of electronics and information products, to build the hardware foundation for the industry.[35] A well-known example was the growth of the semiconductor sector based on a wide array of subsidies and regulatory support, such as grants, tax preferences, export promotion, and government

[30]See Singh, *supra* note 12, at 35–56. For a more comprehensive discussion of India's digital strategy, see L. Zhang and D. Hu, 'National Digital Development Strategy and Its Practice in India', in G. Yang et al. (eds.), *Countries and Regions: Dynamic Interconnectivity* (2024), 137.

[31]International Trade Administration, 'India: Digital Economy', updated 18 September 2024, available at www.trade.gov/country-commercial-guides/india-digital-economy; see Zhang and Hu, *supra* note 30, at 165.

[32]K. Bagchi et al., 'Data Flows and Data Localisation: An Economic Analysis', *Indian Council for Research on International Economic Relations Working Paper No. 389*, June 2020, ii–iv, available at icrier.org/pdf/Data_Flows_and_Data_Localisation.pdf; R. Chaudhuri and A. Kang Joseph, 'Living in a Fragmented World: India's Data Way', (2024) 23(2) *India Review* 154, at 156–7.

[33]See Evenett and Fritz, *supra* note 11.

[34]'Process tracing is a fundamental tool of qualitative analysis' through a 'systematic examination' of select evidence – 'as part of a temporal sequence of events' – to describe and test existing knowledge or inferences, discover new phenomena, or gain fresh insights in response to a given research question or objective. See, generally, D. Collier, 'Understanding Process Tracing', (2011) 44(4) *PS: Political Science & Politics* 823. This methodology has proven effective and reliable in demystifying complex regulatory frameworks in the digital space. See, e.g., R. Creemers, 'China's Emerging Data Protection Framework', (2022) 8(1) *Journal of Cybersecurity* 1; see Han, *supra* note 28.

[35]《中华人民共和国国民经济和社会发展十年规划和第八个五年计划纲要》[Ten-Year Plan and the Eighth Five-Year Plan for Economic and Social Development of the People's Republic of China (1991–1995)], issued in April 1991, available at www.ndrc.gov.cn/fggz/fzzlgh/gjfzgh/200709/P020191029595681819982.pdf; 《中华人民共和国国民经济和社会发展"九五"计划和 2010年远景目标纲要》[Ninth Five-Year Plan for Economic and Social Development of the People's Republic of China and the Outlines of Objectives in Perspective of the Year 2010 (1996–2000)], issued on 17 March 1996, available at www.ndrc.gov.cn/fggz/fzzlgh/gjfzgh/200709/P020191029595686994247.pdf; F. Jiang et al., 'China's Industrial Policy in the Digital Economy Era' [数字经济时代的中国产业政策], (2024) 6 *Study & Exploration* 168, at 169–74.

https://doi.org/10.1017/S0922156526100909 Published online by Cambridge University Press

procurement.[36] More broadly, through similar supportive schemes at both central and local levels, the information industry developed rapidly to become a key pillar of the national economy by 2005.[37]

Building upon the development and consolidation of basic digital capabilities and infrastructure, China's policy priorities shifted in the second phase (2006–2015) to advance indigenous innovation and competitiveness in critical technologies.[38] In light of its technology-and-innovation-oriented development model, China allocated massive resources to advance R&D and innovation in frontier information technologies[39] and expand supportive digital infrastructure.[40] A landmark achievement was the innovation in key technologies for network communications. China's proprietary TD-LTE Advanced technology became one of the mainstream international standards for 4G,[41] developing a critical home-market advantage for domestic tech champions like Huawei and ZTE.[42] By leveraging the massive commercial deployment of this indigenous standard, these firms were able to achieve economies of scale and technological maturity, which facilitated their global expansion. Moreover, China's policy shift enabled it to possess the world's largest broadband network infrastructure as well as the world's largest internet user base, which produces a tremendous amount of data.[43]

In 2015, the Chinese government recognized data as a 'basic strategic resource' and since then has placed growing emphasis on the development and application of data in traditional and emerging industries to advance digital transformation.[44] Meanwhile, however, the rapid and widespread adoption of digital technologies, such as the internet, generated significant security-related challenges. Since the early 2010s, the Chinese government has taken steps to

[36]《国务院关于印发鼓励软件产业和集成电路产业发展若干政策的通知》[Several Policies to Encourage the Development of the Software Industry and Integrated Circuit Industry], issued by the State Council on 24 June 2000, available at www.gov.cn/gongbao/content/2000/content_60310.htm; A. He, 'China's Techno-Industrial Development: A Case Study of the Semiconductor Industry', *CIGI Papers No. 252*, May 2021, 15, available at www.cigionline.org/static/documents/documents/no.252%20web.pdf.

[37]《中华人民共和国国民经济和社会发展第十个五年计划纲要》[Tenth Five-Year Plan for Economic and Social Development of the People's Republic of China (2001–2005)], issued on 5 March 2001, available at www.gov.cn/gongbao/content/2001/content_60699.htm; '"十五"期间我国信息化发展概况' [An Overview of China's Informatization Development during the Tenth Five-Year Period] (23 June 2006), available at tech.sina.com.cn/it/2006-06-23/18251005965.shtml.

[38]《2006–2020年国家信息化发展战略》[The National Informatization Development Strategy for 2006–2020], issued by the General Office of the Central Committee of Communist Party of China and the General Office of the State Council on 19 March 2006, available at www.gov.cn/gongbao/content/2006/content_315999.htm.

[39]《信息产业"十一五"规划》[Eleventh Five-Year Plan for Information Industry], issued by the Ministry of Industry and Information Technology and Information on 1 March 2007, available at www.ndrc.gov.cn/fggz/fzzlgh/gjjzxgh/200709/P020191104623156010398.pdf;《关于印发国家十二五科学和技术发展规划的通知》[Development Plan of Science and Technology for the Twelfth Five-Year Plan], issued by the Ministry of Science and Technology on 4 July 2011, available at www.most.gov.cn/xxgk/xinxifenlei/fdzdgknr/qtwj/qtwj2011/201107/t20110713_88228.html.

[40]《中华人民共和国国民经济和社会发展第十一个五年规划纲要》[Eleventh Five-Year Plan for Economic and Social Development of the People's Republic of China (2006–2010)], issued on 14 March 2006, available at www.gov.cn/gongbao/content/2006/content_268766.htm;《中华人民共和国国民经济和社会发展第十二个五年规划纲要》[Twelfth Five-Year Plan for Economic and Social Development of the People's Republic of China (2010–2015)], issued on 14 March 2011, available at www.ndrc.gov.cn/fggz/fzzlgh/gjfzgh/201109/P020191029595702423333.

[41]'"十二五"期间宽带运营业发展回顾' [Review of the Development of Broadband Operation Industry during the Twelfth Five-Year Period] (2 August 2017), available at www.ndrc.gov.cn/xwdt/gdzt/xyqqd/201708/t20170802_1197809_ext.html.

[42]See, e.g., S. Johnson and L. Abboud, 'China's 4G Bonanza to Shake Up Mobile Gear Vendor Market', *Reuters*, 29 April 2013, available at www.reuters.com/article/business/chinas-4g-bonanza-to-shake-up-mobile-gear-vendor-market-idUSDEE93R033/.

[43]See Review of the Development of Broadband Operation Industry during the Twelfth Five-Year Period, *supra* note 41.

[44]《国务院关于积极推进"互联网+"行动的指导意见》[Guiding Opinions on Promoting the 'Internet Plus' Action Plan], issued by the State Council on 1 July 2015, available at www.gov.cn/zhengce/content/2015-07/04/content_10002.htm;《国务院关于印发促进大数据发展行动纲要的通知》[Action Outline for Promoting the Development of Big Data], issued by the State Council on 31 August 2015, available at www.gov.cn/zhengce/content/2015-09/05/content_10137.htm.

https://doi.org/10.1017/S0922156526100909 Published online by Cambridge University Press

strengthen security safeguard capabilities by enhancing digital security infrastructure[45] and tightening data protection,[46] amongst other means. As China's overarching economic policies continued to prioritize development and growth, data regulation in this phase remained piecemeal largely confined to consumer protection.[47] Nevertheless, these efforts laid the groundwork for the development of a comprehensive regulatory framework to address security concerns in the following decade.

Balancing development and security interests has been at the centre of China's digital industrial policy in the third phase (2016 to present). When it comes to data, the Thirteenth Five–Year Plan (2016–2020) reaffirmed the vital role of data in digital transformation and stressed the need for the openness and sharing of government data, the development of infrastructure such as data platforms and centres, the advancement of data-related technologies, etc.[48] The Plan also mandated the integration of data security into digital development by establishing a comprehensive regulatory framework for strengthening data protection across the entire data lifecycle.[49] The first major milestone in this balancing act was the enactment of the Cybersecurity Law (CSL)[50] in 2016, which became the cornerstone of China's digital security legislation.[51] Under the Fourteenth Five-Year Plan period (2021–2025), the balancing act has continued to evolve through new policy priorities and regulatory interventions.

The 'development' side has focused on broadening and deepening digital industrialization in both hardware and technology sectors (e.g., communication equipment, core electronic components, and critical software vs. AI, big data, blockchain, and cloud computing).[52] Data is regarded as a 'core engine' to drive digital industrialization, so a national data market is needed to establish a comprehensive data-related supply chain involving R&D, creation, collection, transfer, application, and storage of data.[53] For instance, new approaches have been introduced to facilitate the opening up of business data by leading digital and internet platforms and to promote cross-industry data interconnectivity and sharing through trusted data spaces collaboratively built by

[45]《国务院关于大力推进信息化发展和切实保障信息安全的若干意见》 [Several Opinions on Promoting the Development of Informatization and Effectively Ensuring Information Security], issued by the State Council on 28 June 2012, effective on 17 July 2012, available at www.gov.cn/zhengce/content/2012-07/17/content_5906.htm. In 2015, the Chinese government implemented 96 special projects for national information security. See《国家信息安全专项及下一代互联网技术研发、产业化和规模商用专项项目清单》[List of Projects for National Information Security, Next-Generation Internet Technology R&D, Industrialization, and Large-Scale Commercial Application], issued by the National Development and Reform Commission on 16 February 2015, available at zfxxgk.ndrc.gov.cn/web/iteminfo.jsp?id＝3331.

[46]See 'Several Opinions on Promoting the Development of Informatization and Effectively Ensuring Information Security', *supra* note 45. For specific regulations, see K. Cai, 'Jurisdictional Report: The People's Republic of China', in C. Girot (ed.), *Regulation of Cross-Border Transfers of Personal Data in Asia* (ABLI Legal Convergence Series, May 2018), 62 at 67–72, available at https://abli.asia/abli-publications/regulation-of-cross-border-transfers-of-personal-data-in-asia-softcover/.

[47]See Creemers, *supra* note 34, at 4.

[48]《中华人民共和国国民经济和社会发展第十三个五年规划纲要》[Thirteenth Five-Year Plan for National Economic and Social Development of the People's Republic of China (2016–2020)], issued on 17 March 2016, available at www.gov.cn/xinwen/2016-03/17/content_5054992.htm;《国务院关于印发"十三五"国家信息化规划的通知》[National Informatization Plan for the Thirteenth Five-Year Period], issued by the State Council on 15 December 2016, available at www.gov.cn/zhengce/content/2016-12/27/content_5153411.htm.

[49]Ibid.

[50]《中华人民共和国网络安全法》[Cybersecurity Law of the People's Republic of China 2016] [hereinafter 'CSL'], promulgated by the Standing Committee of the National People's Congress on 7 November 2016, effective on 1 June 2017, available at www.npc.gov.cn/zgrdw/npc/xinwen/2016-11/07/content_2001605.htm.

[51]See Creemers, *supra* note 34, at 4.

[52]《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 Fourteenth Five-Year Plan for the National Economic and Social Development of the People's Republic of China and 2035 Long Term Goals (2021–2025)], issued on 12 March 2021, available at www.gov.cn/xinwen/2021-03/13/content_5592681.htm.

[53]《国务院关于印发"十四五"数字经济发展规划的通知》[Digital Economy Development Plan for the Fourteenth Five-year Period], issued by the State Council on 12 December 2021, available at www.gov.cn/zhengce/content/2022-01/12/content_5667817.htm.

https://doi.org/10.1017/S0922156526100909 Published online by Cambridge University Press

enterprises, research institutions, and industry organizations.[54] One of the latest developments was the establishment of China's first state entity specializing in data integration and technology, which builds a platform for data sharing among highways, railways, waterways, aviation, and ports, thereby creating a more competitive and innovative service ecosystem.[55] These ongoing efforts to systematically integrate and exploit data resources have enabled and accelerated the development of China's digital industry. This is most evident in the rapid rise of domestic AI entities like DeepSeek. By prioritizing data interconnectivity and establishing unified platforms, the state has granted AI innovators access to structured, large-scale datasets that were previously fragmented.[56]

On the 'security' side, the Data Security Law[57] (DSL) and the Personal Information Protection Law[58] (PIPL) were enacted at the outset of the five-year period to provide detailed rules in specific areas of digital security, and, cumulatively, to create a comprehensive regulatory framework for safeguarding the digital ecosystem. These were followed by the promulgation of a series of implementing regulations detailing the standards and procedures of existing and new security-related measures, such as security review, standard data security contract, and personal information protection certification,[59] which are further discussed below. Overall, as data becomes a core strategic asset, security measures have not only tackled issues of data leakage and misuse for private, commercial, and defence-related interests, but have pivoted to protecting, developing, and leveraging data resources for developmental and strategic goals.

A raft of criticisms has been levelled at China's digital industrial policy, especially the security-related measures. For example, the CSL provoked an intense debate at the WTO with major players such as the US, the EU, and Japan criticizing the law for creating protectionist and trade-restrictive instruments in the guise of cybersecurity.[60] Commentators have similarly criticized

[54]《关于促进数据产业高质量发展的指导意见》[Guiding Opinions on Promoting the High-Quality Development of the Data Industry], issued jointly by six State ministries and departments on 28 December 2024, available at www.gov.cn/zhengce/zhengceku/202412/content_6995430.htm. For detailed policies on the opening and sharing of public and enterprise data, see 《关于加快公共数据资源开发利用的意见》[Opinions on Accelerating the Development and Utilization of Public Data Resources], issued by the General Office of the Central Committee of Communist Party of China and the General Office of the State Council on 21 September 2024, available at www.gov.cn/zhengce/202410/content_6978911.htm;《关于促进企业数据资源开发利用的意见》[Opinions on Promoting the Development and Utilization of Enterprise Data Resources], issued by five State ministries and departments on 20 December 2024, available at www.gov.cn/zhengce/zhengceku/202412/content_6994570.htm.

[55]K. Wong, 'How China Manages Big Data Is Changing, as New State-Owned Firm Takes the Helm', *South China Morning Post*, 20 December 2024, available at www.scmp.com/economy/china-economy/article/3291731/how-china-manages-big-data-changing-new-state-owned-firm-takes-helm.

[56]M. Zou, 'DeepSeek Is Now a Global Force. But It's Just One Player in China's Booming AI Industry', *UNSW Newsroom*, 26 February 2025, available at www.unsw.edu.au/newsroom/news/2025/02/deepseek-global-force-Chinas-AI-industry.

[57]《中华人民共和国数据安全法》[Data Security Law of the People's Republic of China] [hereinafter 'DSL'], promulgated by the Standing Committee of the National People's Congress on 10 June 2021, effective on 1 September 2021, available at www.npc.gov.cn/c2/c30834/202106/t20210610_311888.html.

[58]《中华人民共和国个人信息保护法》 [Personal Information Protection Law of the People's Republic of China] [hereinafter 'PIPL'], promulgated by the Standing Committee of the National People's Congress on 20 August 2021, effective on 1 November 2021, available at www.gov.cn/xinwen/2021-08/20/content_5632486.htm.

[59]《数据出境安全评估办法》 [Measures for Security Assessment of Outbound Data Transfer 2022] [hereinafter 'Security Assessment Measures'], issued by the Cyberspace Administration of China on 7 July 2022, effective on 1 September 2022, available at www.gov.cn/zhengce/zhengceku/2022-07/08/content_5699851.htm;《个人信息出境标准合同办法》[Measures on Standard Contract for Outbound Transfers of Personal Information] [hereinafter 'Standard Contract Measures'], issued by the Cyberspace Administration of China on 22 February 2023, effective on 1 June 2023, available at www.gov.cn/zhengce/202311/content_6917770.htm;《关于实施个人信息保护认证的公告》[Announcement on the Implementation of Personal Information Protection Certification], issued by the State Administration for Market Regulation and the Cyberspace Administration of China on 4 November 2022, available at www.samr.gov.cn/rzjgs/zcfg/art/2022/art_e7cf688ac2944d84b641008252e31db8.html.

[60]See, e.g., WTO, Committee on Technical Barriers to Trade, Minutes of the Meeting of 29–30 March 2017, G/TBT/M/71 (2 June 2017), 3–6.

https://doi.org/10.1017/S0922156526100909 Published online by Cambridge University Press

China's security-related data localization requirements and cross-border data flow restrictions as digital protectionism which boosts Chinese tech firms at the cost of foreign competitors.[61] Has China used security-related measures to foster its digital industrialization? To answer this question, a more detailed assessment of China's balancing act in data regulation is warranted.

3.2 Balancing development and security in data regulation

As mentioned, the CSL, DSL, and PIPL have consolidated and strengthened China's data protection mechanisms.[62] To expound China's balanced approach, we focus on analysing the security measures related to data localization and cross-border data flows below. This focus is aligned with the shared observation that data localization and cross-border transfer restrictions constitute major forms of digital protectionism in many jurisdictions, including China.[63] In general, the above-mentioned Chinese legislation has established a tiered risk management system for protecting data security based on the importance of data, operators, and security interests.[64] This system does not impose a blanket restriction on the cross-border flow or localization of data. Rather, it adopts different levels of regulatory checks and requirements commensurate with the severity of security risks and impacts.

3.2.1 Data localization

Data localization is required in three major situations. The first concerns personal information and 'important data' collected and generated by critical information infrastructure operators (CIIOs).[65] As further clarified in the implementing regulations, 'critical information infrastructure' refers to 'important network infrastructure and information systems in important industries and sectors, including telecommunications, information services, energy, transportation, hydraulic engineering and water utilities, finance, public services, e-government services, national defense, science and technology, and others that once damaged or suffer a data leakage, could severely harm national security, the economy, livelihoods, or the public interest'.[66] 'Important data' covers 'data that can endanger national security, economic operations, social stability, or public health and safety if manipulated, destroyed, leaked or illegally obtained or used'.[67] To provide better clarity and certainty, the DSL mandates competent authorities to formulate

[61]Council on Foreign Relations, 'The Rise of Digital Protectionism', 18 October 2017, available at www.cfr.org/report/rise-digital-protectionism. For detailed discussions of digital protectionism, see, e.g., S. A. Aaronson, 'What Are We Talking about When We Talk about Digital Protectionism?', (2019) 18(4) *World Trade Review* 541.

[62]The CSL did not only unify the fragmented rules on data localization and cross-border transfer scattered in different prior regulations. It also reduced the relevant restrictions by requiring data localization only in certain circumstances and permitting cross-border data transfers when prescribed conditions are met, a more balanced approach subsequently reaffirmed in the DSL and PIPL. See CSL, *supra* note 50, Art. 37; see DSL, *supra* note 57, Art. 31; see PIPL, *supra* note 58, Art. 40. To compare with the previous restrictions, see Cai, *supra* note 46, at 67–72.

[63]C. Del Giovane et al., 'The Nature, Evolution and Potential Implications of Data Localisation Measures', *OECD Trade Policy Paper No. 278*, 10 November 2023, available at www.oecd.org/en/publications/the-nature-evolution-and-potential-implications-of-data-localisation-measures_179f718a-en.html. For an assessment of the economic costs associated with restrictions on cross-border data flow and data localization requirements, see OECD and WTO, *Economic Implications of Data Regulation: Balancing Openness and Trust* (2025), available at www.wto.org/english/res_e/booksp_e/data_regulation_e.pdf.

[64]Our discussions below are dedicated to data security measures contemplated in the DSL and implementing regulations and do not consider measures designed to protect privacy more broadly under the PIPL.

[65]See CSL, *supra* note 50, Art. 37.

[66]《关键信息基础设施安全保护条例》 [Regulation on Security Protection of Critical Information Infrastructure], issued by the State Council on 30 July 2021, effective on 1 September 2021, available at www.gov.cn/gongbao/content/2021/content_5636138.htm, Art. 2.

[67]See Security Assessment Measures, *supra* note 59, Art. 19.

https://doi.org/10.1017/S0922156526100909 Published online by Cambridge University Press

'important data' catalogues which specify the scope of important data in specific sectors.[68] As stated by President Xi, the localization requirement targets data generated by industries of the highest economic and social importance and likely to attract the most advanced attacks.[69] Since CIIOs have greater control over data, data localization enables easier monitoring of local servers and faster responses to data leaks and cyberattacks.[70]

The second situation requires non-CIIOs to localize 'important data'.[71] Thus, this localization requirement targets the importance of data and the interests that such data may affect, rather than who controls the data. For instance, personal and business data held by private firms can be subject to this requirement if the data falls within the 'important' category.[72] As noted above, the development of 'important data' catalogues is delegated to competent authorities overseeing specific industries. One example is the automotive industry, which possesses increasingly advanced data processing capabilities and generates huge volumes of data.[73] A joint measure issued by five central authorities classifies six types of data as being 'important', including geographic data, pedestrian and vehicle flows in sensitive areas (e.g., defence, and military administrative zones), data related to certain segments of economic operations (e.g., vehicle flow and logistics), operational data of automobile charging networks, external video and image data (e.g., facial and licence information), and other data that may impact national security, public interests, and individual rights as decided by the authorities.[74] Therefore, while 'important data' may vary among industries, the localization of such data is driven by concerns about security risks associated with the exposure of sensitive information, leakage of key personnel movements, disclosure of critical national targets (e.g., locations of military and defence industrial bases, and government facilities), theft of R&D data, and damage to critical infrastructure, etc.[75]

The third situation concerns personal information collected and generated by non-CIIOs that process such information where the volume is above prescribed thresholds.[76] The current thresholds involve a non-CIIO 'cumulatively providing personal information of over 1 million individuals (excluding sensitive personal information) or sensitive personal information of over 10,000 individuals to overseas entities since January 1 of the current year'.[77] While the thresholds

[68]See DSL, *supra* note 57, Art. 21.

[69]'习近平在网络安全和信息化工作座谈会上的讲话' [Xi Jinping's Speech at the Symposium on Cybersecurity and Informatization Work], Xinhua News (26 April 2016), available at www.xinhuanet.com//zgjx/2016-04/26/c_135312437_4.htm.

[70]N. Mishra, 'Privacy, Cybersecurity, and GATS Article XIV: A New Frontier for Trade and Internet Regulation?', (2020) 19(3) *World Trade Review* 341, at 355; J. Liu, 'China's Data Localization', (2020) 13(1) *Chinese Journal of Communication* 84, at 91.

[71]See Security Assessment Measures, *supra* note 59, Art. 4.1; 《促进和规范数据跨境流动规定》[Provisions on Facilitating and Standardizing Cross-Border Data Flow 2024] [hereinafter 'Facilitating and Standardizing Provisions'], issued by the Cyberspace Administration of China on 22 March 2024, available at www.cac.gov.cn/2024-03/22/c_1712776611775634.htm, Art. 7.2.

[72]See '数据出境安全评估：保护基础性战略资源的重要一环' [Security Assessment of Outbound Data Transfer: An Important Part of Protecting Basic Strategic Resources], Cyberspace Administration of China (7 August 2017), available at www.cac.gov.cn/2017-08/07/c_1121443948.htm.

[73]For example, the daily data generation of an autonomous vehicle is estimated at 4,000 gigabytes, which train the car how to behave in real-life road conditions. See C. Foster and S. Azmeh, 'Aligning Digital and Industrial Policy to Foster Future Industrialization', *Industrial Analytics Platform Insights*, May 2023, available at iap.unido.org/articles/aligning-digital-and-industrial-policy-foster-future-industrialization.

[74]《汽车数据安全管理若干规定（试行）》[Provisions on the Management of Automobile Data Security (Trial)], issued by five ministries on 16 August 2021, effective on 1 October 2021, available at www.gov.cn/zhengce/zhengceku/2021-09/12/content_5640023.htm, Art. 3.

[75]'智能网联汽车信息安全是国家安全的重要防线' [Information Security of Intelligent Connected Vehicles is a Crucial Defense for National Security], 22 October 2021, available at www.rmzxw.com.cn/c/2021-10-22/2971170.shtml.

[76]See PIPL, *supra* note 58, Art. 40.

[77]See Facilitating and Standardizing Provisions, *supra* note 71, Art. 7.2.

https://doi.org/10.1017/S0922156526100909 Published online by Cambridge University Press

specifically target the cross-border transfer of data (see below), they would also trigger the localization requirement.[78] Major technology firms such as Google, Apple, and Alibaba hold vast amounts of user information. As explained by a leading Chinese expert and government advisor, if foreign entities obtain such information, they could combine the data with other datasets, using various algorithms for data mining, to extract information that could potentially threaten China's national security.[79] Thus, this localization requirement is designed to minimize security risks associated with the transmission of personal data at a scale that may pose security risks due to the rapid development of digital firms and technologies.[80]

3.2.2 Cross-border data flows

Similar to its regulatory approach to data localization, China does not prohibit data holders from transferring data abroad. The tiered risk management mechanism consists of two main layers of requirements: (i) security review and (ii) a standard contract or personal data protection certification. The circumstances that would trigger the security review are essentially those in which the localization requirement applies, namely, (i) the transfer of personal information and 'important data' by CIIOs, and (ii) the transfer of 'important data' or the transfer of personal data beyond the above-mentioned thresholds by non-CIIOs.[81] According to the Cyberspace Administration of China (CAC), the security review is based on objective criteria to address genuine security risks and balance security concerns with commercial interests by allowing data operators to transfer important data and personal information abroad when necessary for business purposes.[82] The assessment criteria involve, for example, the necessity and legitimacy of a proposed transfer, the importance of data and the scale of the transfer, the situation of cybersecurity protection, and the availability of protective measures for business and personal data in the recipient jurisdiction, etc.[83] In other circumstances, a security review is not needed before data can be transferred abroad. Where the transfer of data by non-CIIOs is below the prescribed thresholds but involves non-sensitive personal information of over 100,000 individuals, the transferring entity is asked to conclude a standard contract formulated by the CAC with the overseas recipient or obtain a personal information protection certification from a third-party accredited institution according to standards and requirements set forth by the CAC.[84] Like the security review criteria, the mandatory contractual clauses and the certification requirements seem to be focused on addressing potential security risks associated with the transfer of data overseas in accordance with China's cyber/data security laws and standards.[85]

[78]J. Chen et al., '《数据出境安全评估办法》十四个焦点问题的理解' [Understanding the Fourteen Key Issues in the Measures for Security Assessment of Outbound Data Transfer], *Zhong Lun Law Firm*, 8 July 2022, available at www.zhonglun.com/research/articles/9175.html.

[79]Y. Hong, 'The Cross-Border Data Flows Security Assessment: An Important Part of Protecting China's Basic Strategic Resources', (20 June 2017) *Yale Law School Paul Tsai China Center Working Paper*, 9, available at law.yale.edu/sites/default/files/area/center/china/document/dataflowssecurity_final.pdf.

[80]L. Zhang, '个人信息跨境流动制度的三重维度' [Three Dimensions of the Cross-Border Flow of Personal Information System], (2021) 5 *China Law Review* 37, at 41.

[81]See Facilitating and Standardizing Provisions, *supra* note 71, Art. 7.

[82]'《数据出境安全评估办法》答记者问' [Press Conference: Measures for Security Assessment of Outbound Data Transfer], *Cyberspace Administration of China,* 7 July 2022, available at www.cac.gov.cn/2022-07/07/c_1658811536800962.htm.

[83]See Security Assessment Measures, *supra* note 59, Art. 8.

[84]See Facilitating and Standardizing Provisions, *supra* note 71, Art. 8.

[85]See Standard Contract Measures, *supra* note 59, Art. 5; 《网络安全标准实践指南—个人信息跨境处理活动安全认证规范V2.0》 [Cybersecurity Standards Practice Guidelines: Security Certification Specifications for Cross-Border Personal Information Processing Activities], issued by the Secretariat of the National Information Security Standardization Technical Committee on 16 December 2022, Art. 5.4, available at www.tc260.org.cn/front/postDetail.html?id＝20221216161852.

https://doi.org/10.1017/S0922156526100909 Published online by Cambridge University Press

3.2.3 Security as industrial policy? – An appraisal

Our review of China's regulation of data localization and cross-border transfer provides little evidence to suggest an abuse of national security for digital industrialization. Rather, it depicts a balanced approach in China's pursuit of development and security interests in data regulation. At face value, this approach appears to be aimed at establishing a delicate level of specificity and proportionality so that security measures target genuine risks and do not unnecessarily impede trade, investment or, other business activities.

There are some facts to support this observation. For instance, a survey conducted by the European Chamber in 2023 showed that a vast majority of European companies (70 per cent) were able to transfer data out of China via the standard contract path without having to undertake a security review.[86] Likewise, a recent survey conducted by the American Chamber of Commerce in China found that in 2024 only 6 per cent of responding companies experienced difficulties in gaining approval for cross-border data transfer vital to business operations, despite the escalation of US-China trade tensions.[87] In addition, China's National Data Administration reported that by the end of 2024, the CAC completed security reviews of 285 cross-border data transfer cases, of which only 27 cases (i.e., less than 10 per cent) failed to pass the review, mostly due to procedural issues and only a few concerning important data.[88] The CAC further clarified that, as of March 2025, it had rejected only 7 out of 44 notified cases involving outbound transfer of important data.[89] These facts also provide some comfort about Chinese authorities' application of security reviews in practice, suggesting a cautious approach to confine the scope of security-based restrictions to reasonable parameters.

To reinforce its balancing act, China has streamlined its data regulatory mechanisms. In March 2024, the CAC introduced a 'negative list' approach for free trade zones (FTZs), allowing those areas to develop their own catalogue of data that needs to be subject to the regulatory checks.[90] By the end of the year, Beijing, Shanghai, Tianjin, Hainan, and Zhejiang[91] released a negative list for their own FTZs to delineate the boundaries of important data within specific sectors. By confining national security oversight to a finite set of risk scenarios, the 'negative list' approach prevents regulatory overreach into non-sensitive commercial activities. It establishes a legal baseline for unhindered transfers of most commercial data, substantially reducing compliance burdens and uncertainty for enterprises. Moreover, to ease ongoing anxieties of foreign investors, the State Council reiterated that China is committed to facilitating 'secure, orderly, and free flows of data across borders'.[92] On 27 June 2025, the CAC issued the third edition of Security Review Guidelines

[86]European Chamber, *Flash Survey: The Impact of China's Data Regulations on European Business*, 15 November 2023, 3, available at www.europeanchamber.com.cn/en/flash-survey-on-impact-of-china-rsquo-s-data-regulations.

[87]American Chamber of Commerce in the People's Republic of China, *AmCham China's 2025 China Business Climate Survey Report* (2025), 93, available at www.amchamchina.org/wp-content/uploads/2025/01/AmCham-China-BCS-2025.pdf.

[88]'国家数据局举行专题新闻发布会,介绍"关于推动数据产业高质量发展和促进企业数据资源开发利用"相关情况' [Press Conference: Promoting High-Quality Development of the Data Industry and Facilitating the Development and Utilization of Enterprises Data"], National Data Administration (31 December 2024), available at www.nda.gov.cn/sjj/swdt/xwfb/1231/20241231172831486110195_pc.html.

[89]'数据出境安全管理政策问答(2025年4月)' [Q&A on Security Management Policies of Data Outbound Flow (April 2025)], Cyberspace Administration of China (9 April 2025), available at www.cac.gov.cn/2025-04/09/c_1745906286623776.htm.

[90]See Facilitating and Standardizing Provisions, *supra* note 71, Art. 6. For a discussion of the negative list approach, see G. Ma and H. Wu, 'Cross-Border Data Flow Supervision in China's Free Trade Zones: Security and Compliance Rules', (2025) 33(3) *Asia Pacific Law Review* 231.

[91]'《促进和规范数据跨境流动规定》实施一周年 数据出境安全管理工作取得积极成效' [One Year after the Implementation of the Regulations on Facilitating and Standardizing Cross-Border Data Flow, Positive Results have been Achieved in the Security Management of Data Outbound Flow], Cyberspace Administration of China (21 March 2025), available at www.cac.gov.cn/2025-03/21/c_1744174598705025.htm.

[92]《关于进一步优化外商投资环境加大吸引外商投资力度的意见》 [Opinions on Further Optimizing the Foreign Investment Environment and Attracting Foreign Investment 2023], issued by the State Council on 25 July 2023, effective on 13 August 2023, available at www.gov.cn/zhengce/content/202308/content_6898048.htm;《扎实推进高水平对外开放更大力度吸引和利用外资行动方案》[Action Plan on Promoting High-Level Opening Up and Attracting and Utilizing Foreign

https://doi.org/10.1017/S0922156526100909 Published online by Cambridge University Press

setting out detailed document lists and procedures for cross-border data transfer applications.[93] These improvements, with enhanced procedural predictability against administrative delays and regulatory opacity, are welcomed by foreign commentators.[94] While some aspects of China's regulatory framework remain problematic (as further discussed below), China has continued to experiment with new ways of softening security checks and requirements and liberalizing data-related restrictions incrementally. China also seems willing to address concerns of foreign firms and governments about its data security regulation. For instance, Chinese authorities have consulted foreign firms in the policymaking process and have adopted some of their recommendations.[95] The China–EU Cross-Border Data Flow Communication Mechanism, established in August 2024, is further evidence of China's willingness to collaborate with foreign governments to continuously improve the balance between security interests and the need to facilitate cross-border flows of data for trade and investment.[96]

China's balanced approach towards data security can be explained in at least four ways. The first relates to China's ambition to advance digital transformation, which requires a market-oriented data sector to stimulate competition, innovation, and growth while maintaining government interventions, including security measures, only to the extent necessary.[97] Secondly, a market-based regulatory framework is also aligned with China's long-term opening-up strategy, which includes attracting foreign investment by consecutively reducing regulatory restrictions and enhancing the protection of foreign investors.[98] Avoiding excessive and discriminatory requirements on data localization and cross-border data flows is key to ensuring the efficacy and attractiveness of China's foreign investment policy in the digital age.[99] Thirdly, a balanced approach is necessary for advancing China's global strategies and engagement, particularly its continued efforts to join more advanced trade or digital economy agreements such as the CPTPP and the DEPA.[100] These agreements, and many other free trade agreements (FTAs) concluded in recent times, require the parties to facilitate free flows of data across borders and minimize data localization requirements.[101] Using security measures for digital industrial policy would

Investment 2024], issued by the General Office of State Council on 28 February 2024, effective on 19 March 2024, available at www.gov.cn/zhengce/content/202403/content_6940154.htm; 《2025年稳外资行动方案》[Plans to Stabilize Foreign Investment 2025], issued by the State Council on 17 February 2025, available at www.gov.cn/zhengce/content/202502/content_7004409.htm.

[93]《数据出境安全评估申报指南（第三版）》[Guidelines for Security Assessment Application for Outbound Data Transfer (Third Edition)], issued by the Cyberspace Administration of China on 27 June 2025, available at www.cac.gov.cn/2025-06/27/c_1752652339765002.htm.

[94]See, e.g., 'China Relaxes Security Review Rules for Some Data Exports', *Reuters*, 22 March 2024, available at www.reuters.com/technology/cybersecurity/chinas-cyberspace-regulator-issues-rules-facilitate-cross-border-data-flow-2024-03-22/.

[95]See, e.g., European Chamber, Business Confidence Survey 2024 (May 2024), 22, fn. 27, available at www.europeanchamber.com.cn/en/publications-archive/1177/Business_Confidence_Survey_2024.

[96]European Commission, 'EU and China Launch Cross-Border Data Flow Communication Mechanism', 28 August 2024, available at policy.trade.ec.europa.eu/news/eu-and-china-launch-cross-border-data-flow-communication-mechanism-2024-08-28_en.

[97]See National Data Administration, *supra* note 88.

[98]For a review of China's foreign investment regime, see W. Zhou, H. Jiang, and Q. Kong, 'Technology Transfer under China's Foreign Investment Regime: Does the WTO Provide a Solution?', (2020) 54(3) *Journal of World Trade* 455, at 460–9. For China's current foreign investment negative list, see 《外商投资准入特别管理措施（负面清单）（2024年版）》[Special Management Measures for the Market Entry of Foreign Investment (Negative List) (2024 Version)], issued by the National Development and Reform Commission and the Ministry of Commerce on 8 April 2024, effective on 1 November 2024, available at www.gov.cn/zhengce/202409/content_6973047.htm.

[99]See note 92, *supra*.

[100]State Council, 'China to Speed Up Accession to CPTPP', 22 March 2024, available at www.gov.cn/news/202403/22/content_WS65fcddf2c6d0868f4e8e555c.html; State Council, 'China to Advance Efforts to Join DEPA: Ministry of Commerce', 21 November 2024, available at english.www.gov.cn/news/202411/21/content_WS673f328bc6d0868f4e8ed4a9.html.

[101]The full text of the CPTPP is available at www.dfat.gov.au/trade/agreements/not-yet-in-force/tpp/Pages/tpp-text-and-associated-documents, Arts. 14.11 and 14.13. The full text of the DEPA is available at www.mfat.govt.nz/en/trade/free-trade-agreements/free-trade-agreements-in-force/digital-economy-partnership-agreement-depa/depa-text-and-resources, Arts. 4.3

https://doi.org/10.1017/S0922156526100909 Published online by Cambridge University Press

undermine not only China's efforts to join these agreements but also its global reputation more generally, as China has long positioned itself as a proponent of the rules-based trading system and an opponent to the abuse of national security.[102] Finally, and coupled with the reasons above, the availability of and interplay between diverse policy instruments also diminishes the incentive to overstretch security reviews. Particularly, the combination of traditional policy instruments (e.g., subsidies) to boost data-driven economic growth, emerging mechanisms to promote the sharing and commercial use of data, etc. seems to have worked well for China's digital industrialization.[103] In other words, China's advancement of digital competitiveness and leadership seems to have primarily relied on policy instruments other than security measures.

Thus, at least at the normative level, there is no compelling evidence to suggest that China has used security-based measures to bolster its data sector. Yet, these measures have continued to attract criticisms about their (potential) asymmetric impact on foreign business. For example, a recent OECD policy paper observed that China's data localization requirements fall within the 'most restrictive' category among all types of such requirements adopted by a host of economies.[104] In this connection, some have argued that the data localization requirements have increased the costs for foreign investors in China and have supported the development of local digital infrastructure and particularly data centres.[105] It has also been reported that global automakers such as BMW, Daimler, Ford, and Tesla had to set up facilities in China to store data generated by their cars locally, in order to comply with China's data localization rules.[106] Similarly, China's security review mechanism for cross-border data transfers, despite the positive developments discussed above, has also been subject to sustained criticisms due to certain major deficiencies in the mechanism. These deficiencies – mainly concerning ambiguities in the definitions of key terms, particularly 'important data' and 'CIIOs', the lack of progress in developing industry-specific catalogues of important data, the need to adapt to different regulatory requirements in different regions, and non-transparency of security reviews – continue to generate administrative burdens for foreign companies and potentially benefit Chinese firms.[107] These ongoing concerns are valid. While the scope of important data has been increasingly refined, especially through negative lists in the FTZs,[108] these lists vary significantly leading to continued regulatory fragmentation. The nationwide application of the negative list approach will take time, so companies in non-FTZ areas continue to face ambiguities about the boundaries of 'important

and 4.4. For a detailed review of digital trade commitments in recent FTAs, see M. Burri and K. Kugler, 'Regulatory Autonomy in Digital Trade Agreements', (2024) 27(3) *Journal of International Economic Law* 397, at 400–3.

[102]For a discussion of China's approaches to national security under the global trading system, see Zhou et al., *supra* note 8.

[103]For a discussion of China's subsidization of its high-tech industries and the applicability of WTO rules, see W. Zhou and M. Fang, 'Subsidizing Technology Competition: China's Evolving Practices and International Trade Regulation', (2021) 30(3) *Washington International Law Journal* 470. For policy documents, see, e.g., '中共中央 国务院印发《数字中国建设整体布局规划》' [A Blueprint for Developing a Digital China], issued by the Central Committee of Communist Party of China and the State Council on 27 February 2023, available at www.gov.cn/zhengce/2023-02/27/content_5743484.htm; See Guiding Opinions on Promoting the High-Quality Development of the Data Industry, *supra* note 54, Art. 9.2.

[104]See Del Giovane et al., *supra* note 63, at 8–11.

[105]E. de la Bruyère and N. Picarsic, 'China's Quest for Asymmetric Dominance in Data Centers', (25 June 2024) *Hinrich Foundation White Paper*, 8, available at www.hinrichfoundation.com/research/wp/tech/china-quest-for-asymmetric-dominance-in-data-centers/.

[106]Y. Sun and T. Munroe, 'As China Plans New Rules, Global Automakers Move to Store Car Data Locally', *Reuters*, 27 May 2021, available at www.reuters.com/business/exclusive-china-plans-new-rules-global-automakers-move-store-car-data-locally-2021-05-27/.

[107]See, e.g., European Chamber, 'European Business in China Position Paper 2024/2025', 30–31, available at, europeanchamber.oss-cn-beijing.aliyuncs.com/upload/documents/documents/European_Business_in_China_Position_Paper_2024_2025.%5B1269%5D.pdf; European Chamber, 'Siloing and Diversification: One World, Two Systems', 9 January 2025, 26, available at www.europeanchamber.com.cn/en/publications-archive/1272/Siloing_and_Diversification_One_World_Two_Systems; see American Chamber of Commerce in the People's Republic of China, *supra* note 87, at 79, 94.

[108]The Negative Lists for FTZs in Beijing, Shanghai, Zhejiang, Tianjin and Hainan are available at wap.cac.gov.cn/wxzw/sjzl/sjcjfmqd/A09370806phoneindex_1.htm

https://doi.org/10.1017/S0922156526100909 Published online by Cambridge University Press

data'. Moreover, although the CAC has been optimizing the workflow for security reviews, details of completed reviews remain undisclosed to the public. The combination of these outstanding issues provides wide discretion in security reviews, which may be abused to benefit China's data sector when needed.[109] Towards this end, it is also worth noting that, like many other economies, China adopts a broad definition of 'national security' in its legislative system,[110] thereby leaving considerable flexibility in its implementation, including for industrial policy goals. The current geopolitical context has only incentivized China's application of trade restrictions for strategic purposes – often on security grounds – which effectively protect or support domestic industries while disrupting supplies for foreign stakeholders.[111] Given the global industrial policy race in the digital domain, a major way to minimize such abuse of national security as industrial policy is for all governments involved to tackle security-based data policies through concerted efforts.

4. Modernizing security exceptions in trade agreements

Global or regional efforts to establish certain legal constraints on (potential) abuses of data security measures require a proper balance between rules and exceptions. For any trade or digital economy agreements to include binding commitments on cross-border data transfer and/or data localization, they must also provide exceptions necessary to preserve policy space for governments to pursue domestic non-economic imperatives. The balancing act requires that such exceptions not be excessively restrictive or overly deferential. This balance, however, is far from being established in the context of data liberalization and security. While trade or digital economy agreements have added more discipline on data-restrictive measures, they have also maintained a range of exceptions and carve-outs for regulatory intervention on privacy, cybersecurity, and other public policy objectives.[112] To continue our core inquiry about the nexus between national security and industrial policy, this section argues that security exceptions in major trade and digital economy agreements have been overly expanded, thereby providing no effective constraints on the abuse of data security measures. Particularly, such expanded security exceptions are adopted in agreements to which China is a party (e.g., RCEP) or which China is keen to join (e.g., CPTPP & DEPA). These agreements, therefore, leave room for China to use the security measures discussed in Section 3 to protect or promote its data industry.

[109]See, e.g., R.Y. Gao, 'A Battle of the Big Three? Competing Conceptualizations of Personal Data Shaping Transnational Data Flows', (2023) 22(4) *Chinese Journal of International Law* 707, at 771; see Reuters, *supra* note 94.

[110]See, generally, Zhou et al., *supra* note 8. Notably, China's National Security Law treats all harms or threats to China's fundamental economic principles and system, the development of major industries and economic sectors etc. as matters of economic security. See 《中华人民共和国国家安全法》[State Security Law of the People's Republic of China] (Expired), Order No. 6 of the President, issued on 22 February 1993, effective on the same date. This law has been replaced by the Counter-espionage Law of the People's Republic of China on 1 November 2014, Art. 19.

[111]Thus, our concern about potential abuses of the data security law relates more to the application of the law in security reviews than the law on paper. Protectionist application is possible precisely because of the remaining ambiguities in the data security law, coupled with the broad scope of national security. For instance, security reviews provide room for restricting the transfer of data to foreign parties to allow the relevant Chinese firms or industries to build competitive advantages when needed. Such restrictions may even include any data (beyond 'important data') if and when strategic competition, especially in the tech space, intensifies. For instance, China's export controls of rare earths and other critical minerals, while adopted in retaliation of US trade measures, can act as input subsidies for domestic downstream users. See, e.g., 《对部分中重稀土相关物项实施出口管制的决定》[Decision to Implement Export Control on Some Medium and Heavy Rare Earth Related Items], Announcement No. 57, issued by the Ministry of Commerce and the General Administration of Customs of the People's Republic of China, on 9 October 2025, available at www.mofcom.gov.cn/zwgk/zcfb/art/2025/art_59ec4f6bec0b459aa4a30c4bbd0a41c1.html; A. Powers-Riggs et al., 'Beyond Rare Earths: China's Growing Threat to Gallium Supply Chains', *CSIS Brief*, 17 July 2025, available at www.csis.org/analysis/beyond-rare-earths-chinas-growing-threat-gallium-supply-chains.

[112]See, generally, Burri and Kugler, *supra* note 101; S.-Y. Peng, *International Economic Law in the Era of Datafication* (2024).

https://doi.org/10.1017/S0922156526100909 Published online by Cambridge University Press

4.1 Constraints (or a lack of constraints) of security exceptions under the WTO and FTAs

The security exceptions under the WTO have been widely discussed. The provisions that might be applicable to data security measures are Article XXI(a) and Article XXI(b)(iii) of the GATT, as reproduced below. To date, the case law has been developed by WTO panels in four disputes, all concerning Article XXI(b)(iii).[113] Article XXI reads:[114]

> Nothing in this Agreement shall be construed
>
> (a) to require any contracting party to furnish any information the disclosure of which it considers contrary to its essential security interests; or
>
> (b) to prevent any contracting party from taking any action which it considers necessary for the protection of its essential security interests
>
> (i) relating to fissionable materials or the materials from which they are derived;
>
> (ii) relating to the traffic in arms, ammunition and implements of war and to such traffic in other goods and materials as is carried on directly or indirectly for the purpose of supplying a military establishment;
>
> (iii) taken in time of war or other emergency in international relations; or
>
> (c) to prevent any contracting party from taking any action in pursuance of its obligations under the United Nations Charter for the maintenance of international peace and security.

The panels' rulings on three key legal issues for determining the scope of the security exception under Article XXI(b)(iii) were consistent. First, whether a security measure that violates WTO rules is justifiable under the exception is not self-judging. Rather, such measures must satisfy certain legal conditions, a matter that is justiciable.[115] These conditions 'circumscribe (and limit) the circumstances in which the invoking Member may take action which it considers necessary for the protection of its essential security interests'.[116] Second, the scope of 'emergency in international relations' is highly restrictive and involves situations 'of the utmost gravity' leading to 'a breakdown or near-breakdown' in international relations.[117] It is limited to an exceptional state of affairs and does not encompass mere 'tensions' or 'divergences'.[118] Thus, armed conflicts (e.g., *Russia – Traffic in Transit*) or comprehensive diplomatic crises (e.g., *Saudi Arabia – IPRs*) would constitute an 'emergency in international relations', whereas international concerns about an economic or strategic matter (e.g., global steel overcapacity in *US – Steel and Aluminium Products (China)*)[119] or limited economic or political tensions (e.g., *US – Origin Marking*

[113]The four panel decisions are: Panel Report *Russia – Measures Concerning Traffic in Transit*, adopted 26 April 2019, WT/DS512/R,; Panel Report *Saudi Arabia – Measures Concerning the Protection of Intellectual Property Rights*, circulated 16 June 2020, WT/DS567/R,; Panel Report *United States – Certain Measures on Steel and Aluminium Products*, circulated 9 December 2022, WT/DS544/R,; Panel Report *United States – Origin Marking Requirement*, circulated 21 December 2022, WT/DS597/R,.

[114]Where data regulation raises issues under the General Agreement on Trade in Services (GATS) or the Agreement on Trade-Related Aspects of Intellectual Property Rights (TRIPs), GATS Article XIV *bis* and TRIPs Article 73(b)(iii) provide for security exceptions identical to GATT Article XXI. Whether data should be treated as 'goods' or 'services', or even a mix of them, is beyond the scope of this paper. However, where GATS Article XIV *bis* becomes applicable, the case law developed under GATT Article XXI may well be applied to the interpretation of GATS security exceptions which are textually identical.

[115]See Panel Report, *Russia – Traffic in Transit*, *supra* note 113, Paras. 7.81, 7.98; see Panel Report, *US – Steel and Aluminium Products (China)*, *supra* note 113, Paras. 7.105–28; see Panel Report, *US – Origin Marking (Hong Kong, China)*, *supra* note 113, Paras. 7.48–88.

[116]See Panel Report, *US – Origin Marking (Hong Kong, China)*, *supra* note 113, Paras. 7.89, 7.263.

[117]See Panel Report, *Russia – Traffic in Transit*, *supra* note 113, Para. 7.136; see Panel Report, *Saudi Arabia – IPRs*, *supra* note 113, Paras. 7.257–60; see Panel Report, *US – Steel and Aluminium Products (China)*, *supra* note 113, Para. 7.139; see Panel Report, *US – Origin Marking (Hong Kong, China)*, *supra* note 113, Paras. 7.289, 7.297–8.

[118]See Panel Report, *US – Origin Marking (Hong Kong, China)*, *supra* note 113, Paras. 7.289, 7.311.

[119]See Panel Report, *US – Steel and Aluminium Products (China)*, *supra* note 113, Paras. 7.142–8.

https://doi.org/10.1017/S0922156526100909 Published online by Cambridge University Press

(Hong Kong, China))[120] do not satisfy the requisite degree of severity. Third, Article XXI(b)(iii) imposes an obligation of 'good faith', which in turn entails a minimum requirement of 'plausibility' between the means and the ends.[121] While this requirement is needed to avoid abuse of 'Article XXI as a means to circumvent' GATT obligations,[122] the relevant evidentiary standard is significantly lower than that of 'emergency', merely requiring that a contested measure is not 'so remote from, or unrelated to' the security interest concerned. Thus, the key constraint on policy space under Article XXI(b)(iii) pertains to the high standard imposed on what situations may amount to an 'emergency' in international relations. This constraint stems from the narrowness of the treaty language itself, as intended by the drafters.[123] As such, Article XXI(b)(iii) provides little room for data security measures (including those used for industrial policies) precisely because of the requirement that an 'emergency in international relations' must be present.

In sharp contrast, Article XXI(a) provides considerable flexibility for governments to refrain from 'furnish[ing] any information the disclosure of which it considers contrary to its essential security interests'. The term 'information' is not defined or otherwise restricted and therefore has the potential to capture data. It is true that Article XXI was crafted seven decades ago when 'digital economy/trade' was completely unknown. However, WTO tribunals have long endorsed an evolutionary interpretation of existing trade rules to enable the application of the rules to address 'contemporary concerns of the community of nations'.[124] The fact that all of the trade or digital economy agreements discussed below refer to 'information' in their cross-border data transfer provisions is strong evidence of global concerns about data trade in the digital age. Once this threshold issue is resolved, Article XXI(a), which operates independently from Article XXI(b), is not subject to any additional legal requirements such as those implicated by the subparagraphs of Article XXI(b). While it would still not permit self-judgement, the only applicable condition would be the minimum requirement of plausibility.[125] Thus, restrictions on transferring or supplying data can be justified so long as they are not implausible as measures protective of a chosen security interest. Such a minimum degree of connection between the means and the ends is not hard to establish. In addition, Article XXI(a) does not limit the entities that provide information but instead allows *any* measures to be taken to address security risks associated with the supply of *any* information by *any* entity. Therefore, when compared with Article XXI(b)(iii), Article XXI(a) almost goes to the other extreme for a lack of any substantive constraint on data security measures, thereby leaving room for the use of such measures for a mix of security and industrial policy goals. Nevertheless, Article XXI(a) may be refined by clarifying whether the provision or supply of data also captures data localization requirements or measures limiting access to data.[126]

The WTO's security exception has been further developed in recent trade or digital economy agreements in two major aspects. One is softening the legal conditions to allow more flexibility in invoking security exceptions in general. The other is expanding the scope of the exceptions for data regulation more specifically. For example, Article 32.2 of the USMCA[127] clarified that the

[120]See Panel Report, *US – Origin Marking (Hong Kong, China)*, *supra* note 113, Paras. 7.323–54. In reaching this conclusion, the panel also relied on the fact that the US actions targeted HK only (i.e., not China) and only certain areas of their relations while bilateral trade and cooperation had continued in many other aspects.

[121]See Panel Report, *Russia – Traffic in Transit*, *supra* note 113, Paras. 7.132, 7.138; see Panel Report, *Saudi Arabia – IPRs*, *supra* note 113, Paras. 7.283–8.

[122]See Panel Report, *Russia – Traffic in Transit*, *supra* note 113, Para. 7.133.

[123]See M. Pinchis-Paulsen, 'Trade Multilateralism and U.S. National Security: the Making of the GATT Security Exceptions', (2020) 41(1) *Michigan Journal of International Law* 109 (noting that the narrow interpretation of 'emergency' is consistent with the drafting record of the security exception).

[124]Appellate Report *United States – Import Prohibition of Certain Shrimp and Shrimp Products*, adopted 6 November 1998, WT/DS58/AB/R, Paras. 129–31.

[125]See Panel Report, *Russia – Traffic in Transit*, *supra* note 113, Paras. 7.132–3, 7.138.

[126]See Burri and Kugler, *supra* note 101, at 420–1.

[127]The full text of the USMCA is available at ustr.gov/trade-agreements/free-trade-agreements/united-states-mexico-canada-agreement/agreement-between.

https://doi.org/10.1017/S0922156526100909 Published online by Cambridge University Press

disclosure of information includes not only actively transferring or supplying information but also allowing access to information (Paragraph 1(a)). This is arguably added to close the potential loophole under GATT Article XXI(a) noted above.[128] Paragraph 1(b) then removes the sub-paragraphs of GATT Article XXI(b), while maintaining the chapeau so that the phrase 'it considers necessary' is no longer subject to additional legal conditions. As discussed above, while an obligation of 'good faith' would continue to apply, the minimum requirement of plausibility is not hard to satisfy. Thus, the combination of the two developments significantly reduced the rigidity of security exceptions and expanded the scope of justifiable circumstances for data security measures. These developments have also been adopted in digital economy agreements such as the DEPA.[129] The enhanced policy space for data security is clearly a response to the more liberal approaches to data flows and localization adopted in these agreements, acting as a classic 'safety valve' to enable progressive liberalization or more advanced rules on data.[130]

Among China's trade agreements, RCEP is the first to provide a set of data-specific rules and exceptions. While incorporating standard obligations on cross-border data transfer and data localization, RCEP maintains and refines security exceptions based on the WTO model.[131] Particularly, Article 17.13(a) replicates GATT Article XXI(a), thereby allowing RCEP governments to retain broad policy space for addressing data security concerns. Article 17.13(b) adds another exempted circumstance (compared to GATT Article XXI(b)) covering security measures 'taken so as to protect critical public infrastructures including communications, power, and water infrastructures'. Together, these exceptions provide abundant room for China to maintain and develop its data security measures in addressing key policy concerns around 'important data' and 'CIIOs'.[132] Arguably, such policy space constitutes a necessary condition for China to agree to data liberalization obligations. This is evident from China's application to join DEPA, which leaves considerable room for data security measures as noted above. Overall, China's existing international commitments (e.g., WTO, RCEP) do not constrain its use of data security measures. China is also unlikely to pursue any future agreements which may reduce its policy flexibility. As discussed in Section 3, although China has not used data security measures for industrial policy goals, the possibility of such use remains, especially in response to geopolitical tensions and its own strategic needs. The lack of international disciplines over data security measures, however, is not only a challenge in dealing with China but a global issue, given how security exceptions have evolved in recent times to expand policy space for all governments involved.

4.2 Developing security exceptions

Proposals for constraining the abuse of national security to protect trade liberalization and a rules-based trading system have flourished since *Russia – Traffic in Transit*.[133] Yet, detailed discussions

[128]Ibid.

[129]See DEPA, *supra* note 101, Art. 15.2.

[130]See WTO, World Trade Report 2009: Trade Policy Commitments and Contingency Measures (2009), 47

[131]See RCEP, Arts. 12.14.2, 12.15.2, 17.13. The full legal text is available at www.dfat.gov.au/trade/agreements/in-force/rcep/rcep-text.

[132]Notably, Art. 12.17 of the RCEP also excludes digital trade obligations from dispute settlement, as an additional or alternative approach to safeguarding policy space. See H. Gao, 'Data Sovereignty and Trade Agreements: Three Digital Kingdoms', in A. Chander and H. Sun (eds.), *Data Sovereignty: From the Digital Silk Road to the Return of the State* (2023), 213 at 228–31.

[133]See, e.g., S. Lester and H. Zhu, 'A Proposal for "Rebalancing" To Deal With "National Security" Trade Restrictions', (2019) 42(5) *Fordham International Law Journal* 1451; N. Lamp, 'At the Vanishing Point of Law: Rebalancing, Non-Violation Claims, and the Role of the Multilateral Trade Regime in the Trade Wars', (2019) 22(4) *Journal of International Economic Law* 721; J. J. Bacchus, 'The Black Hole of National Security: Striking the Right Balance for the National Security Exception in International Trade', *Cato Policy Analysis No. 936*, 9 November 2022, available at www.cato.org/sites/cato.org/files/2022-11/policy-analysis-936.pdf; M. Pinchis-Paulsen, 'Let's Agree to Disagree: A Strategy for Trade Security', (2022) 25(4) *Journal of International Economic Law* 527; W. Maruyama and A.W. Wolff, 'Saving the WTO from the National Security Exception',

https://doi.org/10.1017/S0922156526100909 Published online by Cambridge University Press

on how best to design security exceptions for data regulation are developing slowly.[134] Below, we offer some preliminary thoughts on how to move negotiations on security exceptions for legitimate data regulation forward.

Negotiation is the only way to address the expansion of security exceptions in trade or digital economy agreements to rebalance data liberalization and security. However, the well-known difficulties in progressing and concluding negotiations on a multilateral basis mean that alternative approaches must be taken. The WTO itself has resorted to plurilateral initiatives for negotiations on emerging issues, including digital trade, to ensure the multilateral trading system stays up to date. Via the JSI, 91 WTO members concluded 'a stabilised text' in July 2024,[135] with a plan to seek its adoption as a plurilateral agreement under Annex 4 of the WTO Agreement.[136] Unfortunately, the JSI text does not include the more advanced rules on cross-border data transfers and data localization adopted in the CPTPP (Articles 14.11 and 14.13), the USMCA (Articles 19.11 and 19.12), and the DEPA (Articles 4.3 and 4.4). This outcome reflects the ongoing challenges in achieving more liberalized data-related rules among a significantly larger group of governments.[137] Thus, even plurilateral negotiations will take time and need to progress incrementally.

Nevertheless, negotiations on data security can help facilitate data liberalization and constrain the abuse of security measures for industrial policy. To do so, the negotiations need to involve detailed discussions of major security-related issues to confine security exceptions to reasonably clear parameters. One threshold question is whether a categorization of data is required. Academic work has proposed ways for data classification.[138] New-generation (digital) trade agreements, including those noted above, have also drawn a distinction between different types of data (e.g., government data, personal data, etc.). What is lacking in the current practice, however, is a dedicated discussion of how such data classifications would help develop exceptions to specifically address data security issues. Another threshold question is whether a classification of data holders or providers is needed,[139] as suggested by China's regulatory approaches relating to CIIOs. Article 17.13(b)(iii) of the RCEP, as considered above, is currently too broad and hence requires further negotiations to clarify the coverage of critical infrastructure, perhaps with a combination of a general list and country-specific lists to establish a commonly accepted baseline while allowing certain flexibility for individual economies.

These threshold issues implicate a risk-based approach concerning the likelihood or gravity of security risks *vis-à-vis* different types of data or data holders. Apart from China's tiered risk management mechanism discussed in Section 3, Professor Peng has observed a general trend of

(May 2023) *Peterson Institute for International Economics Working Paper No. 23-2*, available atwww.piie.com/publications/working-papers/2023/saving-wto-national-security-exception; S. Kho et al., 'The Conundrum of the Essential Security Exception: Can the WTO Resolve the GATT Article XXI Crisis and Save the Dispute Settlement Mechanism?', (2024) 40(1) *American University International Law Review* 127.

[134]See, e.g., Cohen, *supra* note 7, at 814–15.

[135]WTO, Joint Statement Initiative on Electronic Commerce, INF/ECOM/87 (26 July 2024).

[136]WTO, 'Information on the Agreement on Electronic Commerce', 12, available at www.wto.org/english/tratop_e/ecom_e/information_on_agreement_ecom.pdf.

[137]Submissions by JSI participants are available at www.wto.org/english/tratop_e/ecom_e/joint_statement_e.htm. See also N. Sen, 'Understanding the Role of the WTO in International Data Flows: Taking the Liberalization or the Regulatory Autonomy Path?', (2018) 21(2) *Journal of International Economic Law* 323, at 339–41. In contrast, some recent digital trade agreements concluded at the bilateral level have advanced the relevant commitments. One example is the EU–Singapore Digital Trade Agreement which sets out more detailed obligations to prohibit restrictions of cross-border data flows and data localization requirements (Art. 5). Nevertheless, this agreement incorporates the same security exception from Art. XXI(a) (Art. 30 by reference to Art. 16.11 of the EU–Singapore Free Trade Agreement), thereby allowing wide policy space as discussed above. The full texts of the two agreements are available at www.bilaterals.org/IMG/pdf/eu-singapore_text_of_the_digital_trade_agreement.pdf and policy.trade.ec.europa.eu/eu-trade-relationships-country-and-region/countries-and-regions/singapore/eu-singapore-agreements/texts-agreements_en.

[138]See Sen, *supra* note 137, at 343–6.

[139]For a detailed discussion of data security challenges associated with critical infrastructure and how to refine security exceptions through a distinction between critical and noncritical infrastructure, see Peng, *supra* note 112, Ch. 2.

https://doi.org/10.1017/S0922156526100909 Published online by Cambridge University Press

governments 'moving toward risk-based approaches to protect national security and cybersecurity'.[140] Such approaches have also been incorporated into the USMCA (Article 19.15.2) and the JSI (Article 17.3) to facilitate cooperation on cybersecurity issues. A risk-based approach should also be used to advance negotiations on data security more broadly. At a systemic level, recent studies have suggested that the so-called 'targeting rule' derived from the theory of distortions remains applicable to balance trade and security interests by inquiring about whether a chosen policy instrument addresses a claimed security objective at its source.[141] Accordingly, this inquiry entails two key steps: (i) identifying the policy objective(s), and (ii) assessing the appropriateness of the policy instrument(s). The identification of policy objectives necessarily involves an assessment of the security risks and the level of protection that a regulating government seeks to address or achieve. Understanding such risks and objectives provides the basis for evaluating the reasonableness of the chosen means. Where the CPTPP, USMCA, RCEP, and DEPA further liberalized cross-border data transfer and data localization requirements, they also adopted a broad exception to allow measures 'necessary to achieve a legitimate public policy objective' as long as they do not cause 'arbitrary or unjustifiable discrimination' or impose restrictions on data transfers or localization 'greater than are necessary to achieve the objective'.[142] Since security exceptions are separate from this exception, one may argue that data security does not fall within the ambit of the undefined 'legitimate public policy objective'.[143] Nevertheless, the legal conditions contemplated in this exception, particularly the 'necessity' and 'arbitrary or unjustifiable discrimination' tests, provide a good starting point for strengthening the connection between data restrictive measures and security goals beyond a minimum requirement of plausibility. In doing so, the intention is not to restrain the freedom of governments to address any perceived security risks or pursue any chosen security goals. Rather, negotiators should focus on developing a mutual understanding of such risks and goals raised by their counterparts as well as reasons for adopting certain data-restrictive measures. Despite the controversies over the 'necessity' and 'arbitrary or unjustifiable discrimination' tests,[144] they have been well developed through a large volume of cases and could be further refined and elaborated to ensure that data-restrictive measures target security risks and objectives as directly as feasible to minimize abuses for protectionist or other strategic goals.[145] To alleviate concerns about the potential rigidity of the 'necessity' test, governments may consider adopting a country-specific negative list of non-conforming measures to accommodate different regulatory preferences, capacity constraints, and other legitimate considerations.[146]

As negotiations take place, governments should continue to use existing committees and other venues under the WTO to discuss data security and regulatory practices to build transparency and trust and manage unilateral actions and potential trade tensions via concerted efforts.[147] Enhanced understanding of (data-related) security goals and regulatory tools and increased trust among

[140]Ibid., 73.

[141]See generally M. Pinchis-Paulsen et al., 'The National Security Exception at the WTO: Should It Just Be a Matter of When Members Can Avail of It? What About How?', (2024) 23(3) *World Trade Review* 271.

[142]See CPTPP, *supra* note 101, Arts. 14.11.3 and 14.13.3; see DEPA, *supra* note 101, Arts. 4.3.3 and 4.4.3; see USMCA, *supra* note 127, Art. 19.11.2.

[143]This observation finds support in RCEP where the security exception is separate from the 'legitimate public policy objective' exception under the clauses on data localization (Art. 12.14.3) and cross-border data flows (Art. 12.15.3).

[144]See, e.g., M. Słok-Wódkowska and J. Mazur, 'Between Commodification and Data Protection: Regulatory Models Governing Cross-border Information Transfers in Regional Trade Agreements', (2024) 37(1) *Leiden Journal of International Law* 111, at 129–30.

[145]See W. Zhou, 'In Defence of the WTO: Why Do We Need A Multilateral Trading System', (2020) 47(1) *Legal Issues of Economic Integration* 9; N. Mishra, *International Trade Law and Global Data Governance: Aligning Perspectives and Practices* (2024), 188–9.

[146]For an example of non-conforming measures, see CPTPP, *supra* note 101, Chapter 17, Annex IV.

[147]For detailed discussions of how WTO committees can be used for governments to deliberate on trade-security issues, see Pinchis-Paulsen, *supra* note 133.

https://doi.org/10.1017/S0922156526100909 Published online by Cambridge University Press

governments are crucial for modernizing (data) security exceptions. The development of such exceptions would provide legal clarity on the availability of policy space. To the extent that such development adds constraints on governments' discretion in their recourse to national security, it would also provide more certainty on the enforceability of data liberalization commitments. It is from such positive spillovers of progressing negotiations on data security that progressive data liberalization may be attained and the abuse of security measures for industrial policy can be reduced.

5. Conclusion

Industrial policy is no longer confined to economic efficiency or competitiveness but has been increasingly motivated by a mix of economic and non-economic goals, particularly national security. This is especially so in the digital domain as governments compete for digital industrialization. While China's digital transformation has embraced ambitious industrial policies and rigorous security protection, our analysis of China's regulatory framework for data has revealed little evidence to suggest that China has (ab)used security measures to foster its data sector at the cost of foreign competitors. Rather, China's approaches to data security have arguably sought to target security risks and incrementally streamline regulatory checks and requirements. Yet, major loopholes remain in China's regulatory framework, which provide room for discretion and abuse in data security reviews. Faced with escalating geopolitical tensions and burgeoning security-based trade or investment restrictions, China's recourse to data restrictions on security grounds is not a remote possibility. A looming data trade war in the name of national security would harm all economies as well as the rules-based global trading system they jointly built. The security exceptions under existing trade or digital economy agreements can hardly strike a proper balance between data liberalization and security. Governments should join forces to modernize these exceptions, ideally via the multilateral forum provided by the WTO for coordinated and inclusive discussions. Such discussions and negotiations would in turn promote progressive data liberalization by bringing about enhanced clarity and certainty on rebalanced rules and exceptions on data security measures. Policy space is essential in this balancing act, but the right balance cannot be achieved with security exceptions that are either overly deferential or excessively restrictive.

Cite this article: Qu X and Zhou W (2026). Digital industrial policy through data security? – China's approach and security exceptions under trade agreements. *Leiden Journal of International Law* **39**, 655–676. https://doi.org/10.1017/S0922156526100909

https://doi.org/10.1017/S0922156526100909 Published online by Cambridge University Press