Asian Review of Political Economy

EDITORIAL Open Access

Nexus between digital trade and security: geopolitical implications for global economy in the digital age

Chi Zhang[1*], Xuechen Chen[2], Jilong Yang[3] and Xinchuchu Gao[4]

*Correspondence:
cz38@st-andrews.ac.uk

[1] University of St Andrews, St Andrews KY16 9AJ, UK
[2] Northeastern University London, London E1W 1LP, UK
[3] Huaqiao University, Quanzhou 362021, Fujian, China
[4] University of Lincoln, Lincoln LN6 7TS, UK

Abstract

This special issue explores the relationship between digital trade and security, emphasizing the geopolitical implications for the global economy in the digital age. The rapid growth of digital trade has introduced significant challenges and opportunities, necessitating robust data governance to balance national security interests with the free flow of goods, services, and data across borders. The papers explore the different models of data governance championed by the US, China, and the EU, highlighting the complexities of cross-border data flows and their impact on international relations. Through detailed analyses of various international agreements and frameworks, this special issue provides a comprehensive overview of the current landscape of digital trade and its security implications, with a particular focus on China's evolving approach to data governance and its global influence.

Keywords: Digital Trade, Data Governance, Cybersecurity, Geopolitical Implications, Cross-border Data Flows

International politics today are profoundly influenced by digital trade, which carries significant implications for security considerations. As digital trade has emerged as a new arena for geostrategic and political rivalries, it is imperative to examine the nexus between digital trade and security.

The exponential growth of digital trade since the 2000s has reshaped global commerce. Emerging e-commerce platforms, payment systems, and mobile technology have introduced a host of complex challenges and opportunities. At the intersection of digital trade and security, governments are grappling with both old and new challenges as they navigate between national security interests and the need for an unhindered flow of goods, services, and data across borders.

Digital trade encompasses the exchange of goods and services through digital platforms, including e-commerce, digital services, and cross-border data transfers (Lund et al. 2019). The phrase "data is the new oil," attributed to Clive Humby, a British mathematician, succinctly captures the crucial role of data in contemporary geopolitical dynamics (Bhageshpur 2019). According to the Organisation for Economic Co-operation and Development (OECD), data governance is a top policy priority for

governments. Effective data governance is essential to maximizing the benefits of data access and sharing while addressing associated risks and challenges (Organisation for Economic Co-operation and Development, n.d.).

In the context of increased cross-border data flows, which amplify the risk of cyber threats, data governance involves policies and frameworks to manage these flows, protect privacy, and facilitate international cooperation (Goldsmith and Wu 2006). This is not easy. Countries adopt different approaches to data sovereignty in trade agreements (Gao 2022). As the world digitizes, the clash between international law and national sovereignty inevitably manifests in data governance, with the US, China, and the EU championing different models (Gao 2022). These models prioritize different actors – the firm, the state, or the individual – posing challenges for cross-jurisdiction compliance and cross-country operations.

To facilitate digital trade, various plurilateral agreements have been established. For example, the Comprehensive and Progressive Agreement for Trans-Pacific Partnership (CPTPP) includes a dedicated chapter on e-commerce, addressing issues such as the prohibition of data localization requirements. The United States-Mexico-Canada Agreement (USMCA) contains a chapter on data flows, data localization, and personal information protection. The Regional Comprehensive Economic Partnership (RCEP) outlines commitments to promote paperless trading and data protection. The European Union's standards are reflected in its agreements with Japan (EU-Japan Economic Partnership Agreement) and Singapore (EU-Singapore Free Trade Agreement).

Furthermore, comprehensive frameworks for cross-border data flows illustrate the normative landscape within global data governance. The Asia–Pacific Economic Cooperation (APEC) Cross-Border Privacy Rules (CBPR) System provides guidelines for APEC economies, while the OECD Guidelines on the Protection of Privacy and Transborder Flows of Personal Data apply to OECD member countries.

China launched the Global Initiative on Data Security (GIDS) in 2020 with the aim of promoting its model of data governance on an international scale. This initiative reflects China's strategic vision for global data management and security. In line with this global initiative, China has developed a comprehensive set of domestic legislations and regulations designed to give substance to its unique approach to data governance. These legal frameworks encompass various aspects of data protection, cybersecurity, and cross-border data flows, underscoring China's commitment to establishing robust data governance standards.

It is important to recognize that China's norms on data governance should not be viewed merely as a contrasting alternative to the models adopted by the EU and the US. Instead, the papers included in this special issue offer a more nuanced examination of China's data governance approach. They delve into the complexities and underlying principles that shape China's policies, providing a deeper understanding of how these norms interact with those in the EU and the US. Through these nuanced analyses, the papers contribute to a more comprehensive and balanced discourse on global data governance, highlighting the diverse strategies and considerations that influence the international landscape of data security and privacy.

Chi Zhang (2024, this issue) focuses on data localization, a key aspect of China's privacy protection strategy. Through comprehensive regulation, China is redefining the landscape of global governance by setting standards for multinational companies to comply with. The data localization strategy has been particularly stringent since its inception due to security concerns associated with a massive amount of data collected in China being accessible by foreign entities, including potentially hostile state actors. This concern is elucidated in Zhang's paper, which not only addresses the concept of data sovereignty but also delves into the cultural and political contexts surrounding privacy concerns.

During the institutionalization process of privacy protection, a hierarchy in understanding the level of security emerges. While the concept of human security is not entirely alien to Chinese society, the state has positioned itself as the guarantor of safety and privacy at the individual level. This implies that any efforts to protect individual privacy must be undertaken in conjunction with the exercise of state sovereignty (Zhang 2022).

In understanding China's approach to privacy protection, some argue that the concept of 'privacy' is a borrowed notion, suggesting that there is a lack of the cultural foundation for the diffusion of privacy protection norms in Chinese society. Zhang engages with this debate, delving into the origin of the Chinese term *yinsi* and its derogatory connotations in traditional Chinese culture. She argues that while the lack of a cultural foundation does make it more difficult to establish social norms of respecting data privacy, overemphasizing this aspect can lead to cultural essentialist assumptions. She also acknowledges socio-economic factors: the widespread use of the internet in general has led to reduced levels of privacy, regardless of whether a society is collectivist or individualist (Engström et al. 2023). Furthermore, social media also has a socializing effect and tends to cultivate more relaxed attitudes toward privacy (Tsay-Vogel et al. 2018).

While privacy protection as part of data governance is primarily a top-down, state-led project in China, there have been calls for greater privacy consciousness from within Chinese society. Citizens are increasingly concerned about the normalization of tracking technology and facial recognition driven by the prolonged 'crisis mode' that has persisted since the COVID-19 pandemic. Lao Dongyan, a professor at Tsinghua University, emphasized that the necessity for social control driven by infection prevention and control during the COVID-19 pandemic leads people to undervalue the risks associated with facial recognition technology (Liang 2021). She is one of those who have called for increasing awareness of the potential abuse of this technology.

Zhang also delves into the nuanced contrast between platform governance and governance over platforms. The case of Didi sheds light on the power dynamics at play between platforms and the state. Initially viewed as a partner in security governance, Didi found itself under scrutiny by various security departments as the state grew wary of the potential national security risks posed by the vast troves of data accessible to foreign entities. As regulations and laws were enacted to empower the state with greater control over cross-border data flows, companies now face stringent permission-seeking processes, which can often be prolonged significantly. It was not until recently that the Shanghai government initiated discussions on the fast-track approval initiative to expedite the permission-seeking process (Yu and Tham 2024).

This undoubtedly holds significant global implications. The acceleration of this process aids China in restoring the confidence of foreign investors as it grapples with recovering from the economic downturn following the pandemic. This positions China to advance its data governance model, which is already serving as a model for emulation. As more countries grapple with the delicate balance between data security and digital trade, many tend to enact stringent regulations on cross-border data transfers due to the intangible threats to national data security. Collectively, these trends are likely to exacerbate the fragmentation of global business operations in the digital era.

China's efforts continue to evolve. In response to calls to curb the overuse of facial recognition technology, on 28 July 2021, the Supreme People's Court (SPC) issued the Provisions of the SPC on Several Issues Concerning the Application of Law in the Trial of Civil Cases Involving the Processing of Personal Information Using Facial Recognition Technology. These provisions recognize the infringement of individuals' personal rights by property management companies using facial recognition as the sole verification method for homeowners or property users to enter or exit the property (Library of Congress 2021). While the restriction on property management companies may seem like a small step, it is groundbreaking and lays the groundwork for future deliberations regarding data security risks stemming from the over-collection of data in China. In the long run, these initiatives are likely to foster positive changes, promoting a more balanced approach to data governance.

Danni Zhang's (2024, this issue) paper provides a comprehensive analysis of the evolution of China's approach to digital trade over the past three decades (1993–2023), drawing on the 3I theoretical framework to unpack the ideas, interests, and institutions underpinning China's digital trade strategies and policies. Against the backdrop of increasing economic globalization and global digitalization, China has seized the opportunity to actively engage with the development of digital trade rules at bilateral, regional, and multilateral levels. As rightly pointed out by Zhang, whilst the existing literature focuses on examining how China has deployed specific strategies and tactics to influence the existing international digital trade order, there has been insufficient research that unpacks the factors that have driven China's approaches to digital trade and how Beijing's visions and strategies concerning digital trade have evolved over the past few decades. In response to this gap in the literature, Danni Zhang's paper probes into two research questions: How has China's approach to digital trade evolved over time? What domestic and international factors have impacted its adopted approaches? Through a longitudinal analysis, Zhang contends that the evolution of China's digital trade strategies can be divided into three distinct phases. Specifically, in the first phase (between the early 1990s and the mid-2000s), based on the perspective of 'carrying out reform and opening up,' Beijing started accepting the new concept of e-commerce and highlighted the role of the government in the establishment of infrastructure and the formation of relevant policies that provide the necessary preconditions to develop e-commerce domestically while increasing its engagement with multilateral cooperation in order to join the World Trade Organization and enter the global trade market.

In the second phase (from the mid-2000s to the mid-2010s), despite Beijing's efforts to promote regional and international cooperation to gain support from other developing countries in accordance with its political interests, the Chinese government

focused more on its economic interests and domestic national stability. At the domestic level, China took advantage of technological innovation and the new concept of digital trade, which relies heavily on Information and Communication Technologies, to build relevant institutions in order to stimulate the transformation to new economic growth models and emphasized government intervention in data and online regulation to maintain national stability.

Finally, in the third phase (from the late 2010s to the present), whilst confirming that the targeted economic growth model relies on emerging industries and high-tech to align with its economic interests, the Chinese government invested more effort in pursuing political benefits at the regional and international levels aiming at obtaining increased discourse power in order to shape the rules or standards of international digital trade.

By tracing the process of institutionalization related to China's digital trade policies, Zhang argues that the Chinese government has shifted away from an initial focus on pursuing economic growth towards a growing emphasis on striking a balance between economic development and national stability at the domestic level. It is further pointed out that the Chinese government has increasingly prioritized its political interests by pursuing international discourse power in order to influence and reshape the rules or standards of international digital trade at the international level. In light of developing countries' increasing demand to enhance digital capabilities, China's approach to digital trade, which aims to advance the domestic digital economy and relevant technologies while maintaining stability under government regulations, has become increasingly attractive to the Global South.

Jun Zhang (2024 this issue) offers a distinct perspective in examining the nexus between digital trade and security, focusing on submarine cables as a crucial component of the global network infrastructure. Digital technology within these infrastructures plays a pivotal role in bolstering Chinese influence in regions where major powers are competing for dominance (Mankoff 2022). The principle of 'those who arrive first occupy the market' is particularly applicable in this context (Mankof 2022).

Hong Kong holds strategic significance due to its position as a submarine cable hub in the Asia Pacific region. Situated at the crossroads of 13 international submarine cable systems, it serves as a vital data hub connecting China to the global network of submarine cable systems (Zhang 2024). Hong Kong boasts strong competitiveness not only due to its reliable energy supply but also its excellence in fostering an environment conducive to thriving digital trade. The government minimizes intervention in the operation of data centers and has made significant strides in regulating the collection, use, and transfer of personal data.

However, issues stemming from the South China Sea disputes are emerging as potential challenges – new submarine cables destined for Hong Kong must traverse the South China Sea, posing obstacles for non-Chinese vendors seeking permission to establish submarine cable landing points in Hong Kong. This case serves as a notable example of how geopolitical tensions surrounding territorial disputes can potentially complicate the construction of infrastructure essential for facilitating digital trade. This places Hong Kong at a disadvantage compared to Singapore, which harbors significant ambitions regarding its Digital Connectivity Blueprint.

The Hong Kong government acknowledges the challenges stemming from the stagnation in further developing the submarine cable network. The local business community and scholars have also warned about the potential negative impact this could have on attracting investment and talent to Hong Kong. While it is evident that national security concerns have greatly impeded the development of Hong Kong's submarine cable industry, finding a solution is not straightforward. As Zhang highlights, the fundamental issue lies in the lack of mutual trust between China and the US. Beijing's concerns regarding the potential espionage by foreign entities through submarine cables, targeting China's political leaders, government departments, universities, and businesses, outweighed its concerns regarding economic interests in expanding the submarine cable network.

Zhang highlights the potential for achieving a better balance between national security concerns and the growth of the digital economy. This requires a strategic compromise to involve non-Chinese suppliers in business operations, thereby ensuring that China and Chinese companies retain their competitiveness in the telecommunications industry. Another area of potential opportunities is markets where the US does not dominate. The substantial commercial demand in the submarine cable industry precludes a US monopoly, given the significant requirements for installation, replacement, and maintenance. Furthermore, the US does not always achieve its objectives, even with the support of its allies. This is exemplified by the 'Peace Cable' project, where the US was unsuccessful in pressuring France to exclude Chinese companies from participating in cable construction.

The ongoing geopolitical rivalry between China and the US is manifesting in the global network infrastructure as a tendency toward bifurcation. Submarine cables are particularly susceptible to this dynamic and are likely to be sensitive to security concerns. However, for Hong Kong to continue its trajectory of growth, Zhang argues that policy-makers must exercise strategic wisdom to navigate these geopolitical tensions while sustaining its digital economy expansion, especially in playing an active role in projects related to the Belt and Road Initiative and the Digital Silk Road.

Aifang Ma's (2024, this issue) paper provides a timely comparative study of the antitrust regulations of the digital economy in China, the EU, and the US – the three largest digital economies in the world. Ma contends that, over the past two decades, the antitrust regulations of the digital economy in China, the EU, and the US tend to converge in terms of three dimensions: growing separation of the antitrust regulation of the digital economy from that of the other economic sectors, convergence of regulatory objectives that grant particular importance to maximize consumers' welfare, and convergence of regulatory methods. In this research, Ma further identifies four driving factors that result in the increasing degree of convergence of antitrust regulation across the three economies.

Firstly, it is argued that, from a historical perspective, both the EU and the US had proactively sought to leverage influence over the rule-making of China's antitrust regulation since the 1990s, as evidenced in the adoption of Chinese Anti-Monopoly Law, which can be regarded as the result of learning from the US and the EU. The second factor, according to Ma, is mainly concerned with the fact that with the globalization of the digital economy, platforms established in the three economics have taken similar trajectories of development, causing similar challenges to the regulation bodies as

well as the adoption of similar regulatory approaches to respond to these challenges. Furthermore, Ma points out that increasing interstate institutional and policy imitation and competition among the major digital powers of the world, along with the breakup of the Citizen-Platform alliances, have also played an important role in contributing to the convergence. In the long term, as Ma argues, the convergence of the antitrust regulation between China, the EU, and the US will not necessarily persist due to the differences in their respective value systems. While the EU tends to collaborate only with countries that share similar values and political systems, the US does not accept cooperating with any country that does not recognize the US as the 'Big Brother' of the group. Unlike the EU and the US, China prefers to build equal relations between sovereign countries in regulating the digital economy.

The collection of papers in this special issue offers a multifaceted examination of the relationship between digital trade and security, with a particular emphasis on China's evolving approach to data governance. The insights provided by these papers pave the way for future research in several areas. Further studies could explore the challenges and best practices for multinational companies navigating the diverse data governance frameworks across different regions, including understanding the compliance costs and strategies for harmonizing regulations. Research on how emerging technologies like artificial intelligence, blockchain, and quantum computing affect data governance and security is crucial, as these technologies introduce new dimensions of risks and opportunities that need to be addressed within the framework of digital trade. Comparative studies examining the effectiveness of various international data governance frameworks, such as the WTO's e-commerce negotiations and the OECD's privacy guidelines, could provide valuable insights into developing more cohesive and cooperative global policies. Additionally, investigating the cultural and socio-economic factors influencing different countries' approaches to data governance could help in understanding the diversity of strategies and the potential for finding common ground in international negotiations.

Acknowledgements
We are particularly grateful to Dr. Su Ruolin for her exceptional patience and unwavering support in shepherding this special issue through to publication. Her guidance and dedication were instrumental in ensuring the success of this project.
We also extend our heartfelt thanks to all the editors involved in the process. Their meticulous reviews, constructive feedback, and commitment to maintaining high standards have greatly enriched the quality of this special issue. Additionally, we appreciate the efforts of the authors who contributed their valuable research and the reviewers whose insightful comments and suggestions helped to enhance the final manuscripts.
Finally, we acknowledge the support of Shanghai Jiao Tong University and The Institute for International Affairs, Qianhai, CUHK-Shenzhen, for providing the necessary resources and environment conducive to academic research and collaboration.

Authors' contributions
Chi Zhang was responsible for developing the overall analytical framework and linking it with the summaries of the papers. Chi Zhang, Xuechen Chen, and Jilong Yang contributed to summarizing the papers from this special issue. Xinchuchu Gao reviewed and approved the final manuscript.

Funding
Not applicable.

Availability of data and materials
Not applicable.

Declarations

Ethics approval and consent to participate
This project did not involve human subjects.

Competing interests
The authors declare that they have no competing interests.The four authors are the guest editors for the special issue titled "Nexus between digital trade and security: Geopolitical implications for the global economy in the digital age" to be published in this journal.

Received: 19 June 2024 Accepted: 10 July 2024
Published online: 29 July 2024

References

Bhageshpur, K. 2019. Council post: Data is the new oil -- and that's a good thing. https://www.forbes.com/sites/forbestechcouncil/2019/11/15/data-is-the-new-oil-and-thats-a-good-thing/. Accessed 18 June 2024.
Engström, E., K. Eriksson, M. Björnstjerna, et al. 2023. Global variations in online privacy concerns across 57 countries. *Computers in Human Behavior Reports* 9: 100268. https://doi.org/10.1016/j.chbr.2023.100268.
Gao, H. 2022. Data sovereignty and trade agreements: Three digital kingdoms. https://www.hinrichfoundation.com/research/article/digital/data-sovereignty-trade-agreements-digital-kingdoms/. Accessed 18 June 2024.
Goldsmith, J., and T. Wu. 2006. *Who controls the internet? Illusions of a borderless world*. Oxford University Press. https://doi.org/10.1093/oso/9780195152661.001.0001.
Liang, C. 2021. Tsinghua law professor Lao Dongyan warns of facial recognition abuse: Risks underestimated, caution urged [**清**华**法学**教授劳东燕谈**人**脸识**别滥用**: **大大低**估**了**风险, **应**谨慎**推**广]. https://www.sohu.com/a/www.sohu.com/a/491743158_115565. Accessed 13 May 2024.
Library of Congress. 2021. China: Supreme People's Court issues judicial interpretation against misuse of facial recognition technology. https://www.loc.gov/item/global-legal-monitor/2021-08-15/china-supreme-peoples-court-issues-judicial-interpretation-against-misuse-of-facial-recognition-technology/. Accessed 13 May 2024.
Lund, S., J. Manyika, L. Woetzel, et al. 2019. Globalization in transition: The future of trade and value chains. McKinsey Global Institute. http://ceros.mckinsey.com/globalization-ex1-v1-online. Accessed 18 June 2024.
Mankoff, J. 2022. The East Wind prevails? Russia's response to China's Eurasian ambitions. *Europe-Asia Studies* 74 (9): 1616–1639. https://doi.org/10.1080/09668136.2022.2102150. Routledge.
Organisation for Economic Co-operation and Development. n.d. *Data governance*. https://www.oecd.org/digital/data-governance/. Accessed 18 June 2024.
Tsay-Vogel, M., J. Shanahan, and N. Signorielli. 2018. Social media cultivating perceptions of privacy: A 5-year analysis of privacy attitudes and self-disclosure behaviors among Facebook users. *New Media & Society* 20 (1): 141–161. https://doi.org/10.1177/1461444816660731. SAGE Publications.
Yu, X., and E. Tham. 2024. Exclusive: Shanghai to allow faster data transfer from China for foreign firms-sources. Reuters. https://www.reuters.com/world/china/shanghai-allow-faster-data-transfer-china-foreign-firms-sources-2024-02-07/. Accessed 2 Apr 2024.
Zhang, C., ed. 2022. *Human security in China: A post-pandemic state*. Singapore: Springer. https://doi.org/10.1007/978-981-16-4675-1_8.
Zhang, J. 2024. Heading in the direction of bifurcated networks: Hong Kong's evolution amidst the global submarine cable system. *Asian Review of Political Economy 2*. Online first. Accessed 12 July 2024.

Publisher's Note