CSCanada
Canadian Social Science
Vol. 21, No. 2, 2025, pp. 17-23
DOI:10.3968/13766

ISSN 1712-8056[Print]
ISSN 1923-6697[Online]
www.cscanada.net
www.cscanada.org

The Data Security Risks and Responses in China-ASEAN Digital Cooperation

LI Zongwei[a],*; WEI Nan[b]

[a] Center for Southeast Asian Study, South China Normal University, Guangzhou, China.
[b] Beijing Foreign Studies University, Beijing, China.
*Corresponding author.

Received 3 February 2025; accepted 6 April 2025
Published online 26 April 2025

Abstract

As China-ASEAN digital cooperation deepens, both parties face multidimensional data security risks in digital infrastructure connectivity, trade rule reconstruction, collaborative technological research, and industry ecosystem building. This study systematically analyzes the complex security challenges and their causes in China-ASEAN digital cooperation from a South-South cooperation perspective, and proposes targeted response strategies. The study finds that data security risks manifest across physical, informational, and sovereignty layers: geopolitical competition in technological standards, conflicts between data sovereignty and cross-border flow regulations, and intervention by major power rules collectively form the deep-rooted contradictions in regional digital cooperation. Specifically, digital infrastructure is hindered by technical compatibility and cybersecurity disputes, digital trade rules are trapped in "institutional competition and cooperation" due to fragmented regulation, core technology supply chains are impacted by geopolitical tensions, and digital industry collaboration faces dual challenges of cultural identity and regulatory misalignment.

The study further reveals that the root causes of these risks lie in the delayed regional risk awareness, imbalanced governance resources within ASEAN, and the geopolitical rule competition by major powers. To address this, the paper proposes four cooperative pathways: first, building a tiered governance mechanism under the RCEP framework to balance sovereignty and circulation through data categorization, classification, and mutual recognition; second, deepening strategic collaboration by establishing a cross-border data flow joint regulatory committee and a joint cybersecurity defense and control system; third, accelerating the construction of the "Digital Silk Road" by using quantum communication and edge computing to bridge the digital divide; and fourth, strengthening legal mutual recognition, resisting external rule fragmentation, and maintaining regional governance autonomy. These pathways provide a new paradigm of "co-building rules, co-researching technology, and sharing risks" for digital security governance in developing countries.

The study also highlights current limitations, such as the uneven data openness among ASEAN member states and insufficient empirical data in sensitive areas. Future research may focus on the compliance risks and financial stability impacts of the cross-border application of digital RMB, as well as technological and institutional innovations to bridge the digital divide. By deepening differentiated analysis and practical validation, future studies can offer more actionable theoretical support for the high-quality development of China-ASEAN digital cooperation.

Key words: China-ASEAN Digital Cooperation; Data Security; RCEP; Technology Development; Digital Governance; South-South Cooperation

Li, Z. W., & Wei, N. (2025). The Data Security Risks and Responses in China-ASEAN Digital Cooperation. *Canadian Social Science, 21*(2), 17-23. Available from: http://www.cscanada.net/index.php/css/article/view/13766
DOI: http://dx.doi.org/10.3968/13766

1. THE CONTINUOUSLY DEEPENING DIGITAL COOPERATION BETWEEN CHINA AND ASEAN

In recent years, digital cooperation between China and ASEAN has been continuously deepened, gradually

constructing a comprehensive cooperation framework encompassing infrastructure, trade rules, technological research and development, and industrial ecosystems. This cooperation reflects the economic complementarity between the two sides, but also faces challenges such as geopolitical issues and differences in technological standards.

1.1 Digital Infrastructure: Building the Physical Foundation for Regional Connectivity

Through the "Digital Silk Road" initiative, China is advancing both "hard connectivity" and "soft standards" in ASEAN. For example, several Chinese technology companies are establishing data centers in multiple Southeast Asian countries, demonstrating China's active investment in the digital infrastructure sector in the region.

Table 1
Distribution of Data Centres Built by Chinese Tech Companies in Southeast Asia

Country	Alibaba Cloud	Chindata Group	China Mobile	DYXnet	GDS	Huawei Cloud	Tencent Cloud	ZTE	Total
Indonesia	3	0	0	1	0	3	2	2	11
Malaysia	2	1	0	0	1	3	0	0	7
Philippines	1	0	0	1	0	0	0	1	3
Singapore	3	0	1	1	0	5	4	0	14
Thailand	1	0	0	0	0	3	2	0	6
Vietnam	0	0	0	2	0	0	0	0	2
Total	10	1	1	5	1	14	8	3	43

Source: Singapore Yusof Ishak Institute, ISEAS (ISEAS-Yusof Ishak Institute, 2024)

At the same time, ZTE Corporation has deployed the "ASEAN Information Superhighway" backbone network in Laos, successfully reducing regional latency by 30%, providing more efficient and stable network support for cross-border data flows within ASEAN countries. (ZTE Corporation, 2022) Additionally, significant progress has been made in the field of cybersecurity. The China-ASEAN Cybersecurity Emergency Response Center (ASEAN CERT) has established a multilateral drill mechanism, effectively enhancing the region's ability to respond to cybersecurity threats. In 2022, the center successfully intercepted over 12,000 cross-border cyberattacks, significantly strengthening the region's cybersecurity defense capabilities. Through these collaborative initiatives, the digital infrastructure development between China and ASEAN has not only facilitated regional connectivity but also laid a solid technological foundation for future economic development and cooperation.

1.2 Digital Trade: Reshaping the Cross-Border Transaction Rules System

In recent years, the volume of cross-border e-commerce transactions between China and ASEAN has grown at an annual rate exceeding 20%, becoming a key driver of trade between the two sides. (Zhu, 2024) In 2023, the total import and export value of China's cross-border e-commerce reached 2.38 trillion yuan, with ASEAN being China's largest trading partner. As a key hub, Guangxi's cross-border e-commerce transaction value amounted to 15.734 billion yuan, accounting for 70% of the region's total, (Guangxi Big Data Development Bureau, 2024) marking the second consecutive year that it exceeded 10 billion yuan. This highlights China's leading role in promoting regional digital trade. At the same time, China's "Global Data Security Initiative" and ASEAN's "Digital Data Governance Framework" are being aligned, with the aim of establishing a more secure and standardized data circulation mechanism, providing legal guarantees and policy support for the development of digital trade. These initiatives demonstrate that China and ASEAN are making significant progress in reshaping the cross-border transaction rules system, optimizing the regional digital trade environment, and laying the foundation for more efficient and convenient cross-border trade in the future.

1.3 Digital R&D and Innovation: Collaborative Ecosystem Building Under Technological Competition and Cooperation

Cooperation between China and ASEAN countries in the field of digital technology research and innovation has deepened, particularly in areas such as agriculture, healthcare, and navigation. Through technological competition and collaborative development, they have advanced the continuous progress of ecosystem building within the region. In terms of R&D and innovation cooperation, China and ASEAN have jointly established research and development centers, technology transfer centers, and international science and technology parks to promote the development and application of digital technologies. For example, the establishment of platforms such as the China-ASEAN Internet Application Technology Joint Innovation Center and the China-ASEAN Earth Big Data Regional Innovation Center has provided significant support for breakthroughs in key core technologies in areas such as the Internet, big data, and block chain. (China-ASEAN Technology Transfer Center,

2020) These innovative cooperation projects mark the deep integration and mutual promotion between China and ASEAN countries in the technology field, driving the vigorous development of the digital economy within the region.

1.4 Digital Industries: Differentiated Strategies Forming a Value Closed Loop

Cooperation between China and ASEAN in the digital industry has driven effective economic interaction and value closure in the industrial chain through precise market strategies and technological innovation. Chinese internet companies, through the "technology export + local operation" model, have achieved significant success. For example, last year, the total merchandise transaction volume of ByteDance's TikTok Shop across Southeast Asia accounted for more than 90% of the global total, with Indonesia alone contributing over 3.8 billion USD, representing 28%. (Henan International Digital Trade Research Institute, 2024) However, despite these remarkable economic results, TikTok's live-streaming e-commerce model has faced opposition from the Indonesian government, which believes it threatens domestic manufacturing. (Al Jazeera, 2023) Additionally, it has been labeled by the West as a means of cultural infiltration and data theft, highlighting the complex relationship between Southeast Asia's cultural diversity and the local adaptation of digital models.

In terms of industrial digital transformation, China's "Two-Country, Dual-Park" digital twin system with Malaysia has improved cross-border supply chain efficiency, while Vietnam continues to impose restrictions on the cross-border flow of industrial internet data. (Wang, 2021) These collaborations show that, although technological innovation drives the closure of industry value loops, cultural differences and policy barriers remain significant challenges in digital industry cooperation.

2. DATA SECURITY RISKS AND CHALLENGES

The concept of data security has expanded from traditional technical protection to a multidimensional governance system. Its core lies in ensuring the confidentiality, integrity, and availability of data throughout its entire lifecycle through the coordinated efforts of technology, law, and institutional frameworks, while also facilitating the lawful and compliant transformation of its value. With the rapid iteration of digital technologies and the acceleration of globalization, data security is no longer limited to basic objectives such as defending against cyberattacks or preventing data breaches. Instead, it has evolved into a complex security paradigm encompassing physical infrastructure protection, information content governance, and the safeguarding of digital sovereignty. In response to this, China first regulated data security legally in 2021, with the "Data Security Law of the People's Republic of China" stipulating in Article 3: "Data refers to any record of information in electronic or other forms... Data security refers to the necessary measures taken to ensure that data is effectively protected and legally utilized, and to maintain the capability to ensure its continued security. (Cyberspace Administration of China, 2021)"

Essentially, data security encompasses three levels: the physical layer ensures the security of network infrastructure, stabilizing data storage and transmission; the information layer protects data content through privacy computation and access control, preventing misuse and illegal circulation; the sovereignty layer involves the governance rights of nations in the digital space, addressing strategic issues such as cross-border data flow and technical standards. These three layers collectively form a dynamic governance system, reflecting the reconfiguration of national security boundaries in the digital economy era. They also reveal the structural contradictions in China-ASEAN digital cooperation: the physical layer faces geopolitical struggles over technical standards, and digital infrastructure interconnectivity is constrained by differentiated access rules; the information layer encounters institutional conflicts between data sovereignty and cross-border flow, with divergent national data governance concepts creating compliance barriers; the sovereignty layer is caught in the competition for rule leadership, and the regional digital rule system is showing signs of fragmentation under the intervention of multiple forces. The security challenges across these three dimensions are intertwined, forcing the cooperation process to seek a dynamic balance between infrastructure interconnection, data flow, and the relinquishment of digital sovereignty. This inherently points to the deep tension between the globalization of the digital economy and the localization of governance.

2.1 Risks and Challenges of Digital Infrastructure

China and ASEAN face multiple risks and challenges in their cooperation on digital infrastructure. First, the issue of technological standards and interoperability is significant. ASEAN countries have yet to establish unified standards in emerging technologies such as 5G and artificial intelligence. Some countries tend to adopt European Union or U.S.-based technological frameworks, leading to compatibility issues with China's technological system. For instance, while countries like the Philippines and Thailand prefer Chinese equipment, Singapore and Vietnam lean towards non-Chinese suppliers, creating a technological path divergence that complicates cross-border data flow and infrastructure connectivity. (Luo, 2024) Second, ongoing disputes over cybersecurity and data sovereignty persist. ASEAN member states have varying requirements for data localization, with

countries such as Indonesia and Malaysia demanding that critical data remain within national borders, while China advocates for the facilitation of cross-border data flows. These policy discrepancies could lead to data breaches and compliance conflicts. (Liu, 2025) Additionally, escalating geopolitical competition exacerbates external pressures. The U.S.-led "Clean Network" initiative, through device access restrictions and exclusivity clauses, creates institutional barriers, forcing ASEAN countries to adopt a "technological hedging" strategy in the construction of critical infrastructures such as 5G. (Fudan Development Institute, 2020)

2.2 Risks and Challenges of Digital Trade

The competition over digital trade rules reveals the structural contradictions between data sovereignty and free flow. ASEAN member states have inconsistent policies regarding data regulation. For instance, Indonesia's Personal Data Protection Law requires e-commerce and financial data to be stored domestically, while Vietnam mandates that cloud service providers keep local copies of user data. Singapore, on the other hand, was the first to join the ASEAN Digital Economy Framework Agreement (DEDA), allowing for cross-border data transfer. The differentiation in regulatory rules has resulted in Chinese companies needing to build data centers repeatedly across multiple ASEAN countries, leading to an increase in investment costs by 30% to 50%. (Zhang, 2025)

The deeper contradiction lies in the divergence of values between China's "Global Data Security Initiative" and ASEAN's "Digital Data Governance Framework" on key issues such as data classification, categorization, and cross-border transmission certification. This has led to a fragmented regional digital trade system, characterized by "excessive mechanisms but insufficient mutual recognition." Furthermore, the U.S. and EU, through the "Indo-Pacific Economic Framework" (IPEF), have embedded their digital rules and standards, further exacerbating the "institutional competition and cooperation" dilemma in regional data governance.

2.3 Risks and Challenges of Digital R&D and Innovation

In the realm of digital research and innovation, the "triangle dependence" on core technologies has created hidden risks for supply chain security. U.S. technology export control measures, such as chip export restrictions, investment limitations, and procurement bans, directly affect digital infrastructure cooperation between China and ASEAN countries. For example, Huawei's collaboration in 5G network construction has been rejected by certain ASEAN countries. According to Statista's charts, Vietnam is in a "possible ban on Huawei" status among ASEAN countries. (Statista, 2020) Furthermore, U.S. export controls on Southeast Asia's semiconductor industry have also exerted pressure on Malaysia's semiconductor sector, such as restrictions on the export of Nvidia chips. (Financial Times, 2025) These technological blockades and supply chain disruptions could cripple China's manufacturing capacity, which in turn would impact the digital economy's terminal applications in ASEAN.

2.4 Risks and Challenges of the Digital Industry

Collaboration in the digital industry faces dual challenges of cultural identity and regulatory misalignment. The "live-streaming e-commerce revolution" driven by TikTok, with over 38 million active users daily in Southeast Asia, has encountered opposition from government in the Philippines, accusing that TikTok may be influenced by Chinese laws, and has raised apprehensions about its plan to establish a content creator academy in the Philippines. (The Philippine Star, 2024) A deeper contradiction lies in the conflict between China's "technology export + data repatriation" industrial model and ASEAN countries' demands for digital sovereignty: Vietnam's restrictions on the cross-border flow of industrial internet data force Chinese companies to invest in local data centers. However, the technological conflict between local data storage and the need for optimized algorithm models results in a 17%-25% reduction in operational efficiency. Furthermore, the uneven digital regulatory capabilities within ASEAN (such as the Personal Data Protection Act (PDPA) in Singapore and the lack of basic data legislation in Myanmar) further exacerbate compliance risks for multinational digital enterprises.

In conclusion, China and ASEAN face multiple challenges in digital industry cooperation, including cultural identity, regulatory misalignment, technological conflicts, and compliance risks. A more balanced solution that aligns with the interests of all parties needs to be sought in their cooperation.

3. REASONS FOR DATA SECURITY RISKS IN CHINA-ASEAN COOPERATION

3.1 Lagging Risk Awareness: Structural Defects in Cybersecurity and Coordination Mechanisms

Southeast Asia's digital transformation has driven the prosperity of the digital economy, but it has simultaneously led to a sharp increase in the risk of cyberattacks. From 2021 to 2022, the rate of cybercrime in the ASEAN region rose by 82%, with economic losses exceeding $2.87 million. Advanced Persistent Threat (APT) attacks targeting critical infrastructure accounted for 79% of global APT attacks in 2023. (IBM， 2022) However, regional cybersecurity resilience remains weak, and the governance system is fragmented: due to differences in national sovereignty priorities and levels of digital development, cybersecurity standards are fragmented across countries.

China emphasizes self-reliant information technology

and national security, while ASEAN countries like Vietnam adopt ambiguous legislation to strengthen data sovereignty control, which raises concerns among foreign investors and poses risks to economic growth. The cognitive gap between the two sides on core issues such as data sovereignty boundaries and the compatibility of technological standards has led to a lack of institutional anchor points in the coordination mechanism. For example, China's proposed hardware security certification system conflicts with ASEAN's localized data regulations, creating policy tension, hindering sensitive data sharing, and reducing the effectiveness of cross-border threat prevention and control. This structural misalignment in awareness and rules fundamentally reflects the value conflict between state-driven security logic and market-driven development logic. If a consensus framework is not built, it will exacerbate institutional friction in regional digital cooperation.

3.2 Imbalance in ASEAN's Governance Resources: Digital Infrastructure and Talent Gaps

The significant digital capability gap between ASEAN member states severely restricts the effectiveness of regional data governance. Singapore, as a leader in digital infrastructure, operates 46 data centers and ranks among the top four data hubs in the Asia-Pacific region. In contrast, Cambodia's internet penetration rate is only 52.6% (2021), below the global average, while rural areas in Laos still lack mobile broadband, and Myanmar's ICT industry is underdeveloped. This disparity in infrastructure has led to a polarization of governance capabilities in areas such as data storage, transmission, and encryption.

A deeper contradiction lies in the imbalance of digital talent development systems. Singapore cultivates high-end technical talent through a government-business collaborative mechanism, while countries like Cambodia and Laos lack systematic investment in digital education. In summary, ASEAN member states face a significant "digital divide" in terms of "hard" factors such as digital infrastructure, technological innovation, and digital talent development. For ASEAN to strengthen its internal data governance, it must continually improve its digital capabilities. Therefore, the "digital divide" in ASEAN poses a substantial barrier to enhancing data governance within the region.

3.3 Geopolitical Hegemony and Rule Competition: Intensified Contest for Technological Standards and Leadership

The United States plays a pioneering role in global data governance, emphasizing the economic benefits of data free flow. It has promoted agreements with the European Union, such as the "Safe Harbor" and "EU-US Privacy Shield" frameworks, to facilitate transatlantic data flow and reduce operational costs. At the same time, the U.S. has strongly advocated for the prohibition of data localization through its leading regional trade agreements, such as the "Trans-Pacific Partnership Agreement (TPP)" and the "United States-Mexico-Canada Agreement," pushing for cross-border data flow as a core rule of U.S.-style digital trade. (Ren and Meng, 2022) However, with intensifying global geopolitical competition, ASEAN has become the focal point of the great power struggle in cyberspace. The U.S. has intervened in China-ASEAN data security cooperation through various means, including highlighting the security threats posed by Chinese digital products and encouraging its allies to resist Chinese technologies.

In addition, the European Union and Western countries such as Japan are actively positioning themselves in the ASEAN digital market to enhance their discourse power and influence. The EU has proposed the "EU-Indo-Pacific Strategy," deepening its digital cooperation with ASEAN, (Li, 2023) and signed the "EU-Singapore Digital Partnership (EUSDP)." In 2023, Japan promoted "O-Lan Alliance" technology cooperation and intervened in ASEAN's digital infrastructure development through international aid and other means. (Fang, Xing, and Tian, 2023) The strategic moves of these great powers have intensified the competition for technological standards and network leadership, placing pressure on China-ASEAN data security cooperation.

4. MAIN APPROACHES TO CHINA-ASEAN DATA SECURITY COOPERATION

4.1 Establishing a Unified Framework for Data Security Standards and Regulations

China and ASEAN should collaborate to develop a data security standard system that aligns with the interests of developing countries, using the "Regional Comprehensive Economic Partnership" (RCEP) as the institutional foundation. This should integrate international regulations with local practices, incorporating rules on cross-border data flow and personal data protection, as well as security cooperation in data governance. These principles are consistent with the data security philosophies of both China and ASEAN, laying a solid foundation for their data security cooperation within the RCEP framework. (Wu, 2022)

To balance data sovereignty and flow requirements, a tiered governance mechanism can be established: sensitive data such as financial and medical data should be managed through classification and grading systems, while blockchain traceability technology should be introduced to reinforce data sovereignty identification. For general commercial data, an "equivalence mutual recognition" approach can be adopted, allowing enterprises certified by CBPR to freely transfer data assets within the

region. Simultaneously, a joint technical working group should be established to focus on developing optical quantum encryption transmission devices suited to tropical climates, with technical validation conducted along the China-Laos railway's digital channel. It is recommended to establish a "data cross-border flow sandbox regulatory zone" in the China (Guangxi) Free Trade Pilot Zone, using a negative list approach to conduct stress testing and explore dynamic balance solutions between local data storage and cross-border transmission. Through the three-pronged approach of standard mutual recognition, joint technology research, and regulatory coordination, a new paradigm for developing countries' participation in global digital governance can be provided.

4.2 Deepening Strategic Coordination and Multilateral Mechanism Building

Leveraging the China-ASEAN Leaders' Meeting mechanism, the integration of the "ASEAN 2021-2025 Strategy" with the "Belt and Road" initiative should be promoted to establish an open, secure, and interoperable multilateral cyberspace order. (ASEAN Secretariat, 2021) A cybersecurity exchange platform and a joint cross-border data flow regulatory committee should be established to coordinate and address the fragmentation of internal ASEAN mechanisms, thereby enhancing the symmetry of information sharing. Through joint training and emergency drills (such as the China-ASEAN Cyber Dialogue Mechanism), the capabilities of joint prevention and control in key areas such as smart cities and 5G should be strengthened. These mechanisms can reduce data sharing barriers caused by the sovereignty-first principle of member states and provide institutionalized support for regional cybersecurity cooperation.

5. CONCLUSION

This study analyzes the data security risks and response strategies in China-ASEAN digital cooperation, revealing the complex security challenges faced by both parties in infrastructure connectivity, digital trade rule reconstruction, collaborative technological research and development, and industry ecosystem building. As a model of South-South cooperation, China and ASEAN have constructed a data security governance framework that balances the interests of developing countries and regional characteristics through technology sharing, standard mutual recognition, and multilateral mechanism innovation. Relying on platforms like RCEP, breakthroughs have been made in coordinating cross-border data flow rules, balancing sovereignty, and ensuring technological autonomy, providing a new paradigm of "joint rule-making, joint technology research, and shared risk" for developing countries' participation in global digital governance. However, challenges remain, such as technological standard competition, regulatory fragmentation, and the intervention of major power rules, which require further collaboration through a tiered governance mechanism, digital infrastructure connectivity, and joint technical endeavors.

Future research could combine field studies across multiple countries to deepen the analysis of regional differences. Subsequent studies are recommended to focus on two major areas: first, the compliance risks, privacy protection, and impact of digital RMB's cross-border application on ASEAN financial stability, exploring its adaptation path with local payment systems; second, the mechanism to bridge the digital divide within ASEAN, including the deployment of edge computing nodes, digital talent cultivation, and improving the effectiveness of cybersecurity joint defense and control. Further research on these topics will provide more actionable theoretical support and practical guidance for the high-quality development of China-ASEAN digital cooperation.

REFERENCES

Al Jazeera. (2023, October 23). *Indonesia's TikTok Shop ban reveals mixed feelings on e-commerce revolution.* https://www.aljazeera.com/news/2023/10/23/indonesias-tiktok-shop-ban-shows-mixed-feelings-on-e-commerce-revolution

ASEAN Secretariat. (2021). *ASEAN cybersecurity cooperation strategy (2021–2025).* https://asean.org/wp-content/uploads/2022/02/01-ASEAN-Cybersecurity-Cooperation-Paper-2021-2025_final-23-0122.pdf

China-ASEAN Technology Transfer Center. (2020, November 3). *Digital economy cooperation for win-win development and innovation*. https://portal.cattc.org.cn/v/article/1328243612392493056

Cyberspace Administration of China. (2021, June 11). *Data Security Law of the People's Republic of China.* http://www.cac.gov.cn/2021-06/11/c_1624994566919140.htm

Fang, Y., Xing, W. X., & Tian, Z. (2023). Opportunities, challenges, and strategies for China-ASEAN digital economy cooperation under RCEP. *International Trade, 10*, 76–85. https://doi.org/10.14114/j.cnki.itrade.2023.10.001

Financial Times. (2025, March 24). *Malaysia to crack down on Nvidia chip flows under US pressure.* https://www.ft.com/content/d0267fb8-36b2-41dc-9c0c-d493976812c7

Fortune China. (2025, March 10). *China-ASEAN digital ecosystem cooperation: Blue oceans and hidden reefs* [by Liu Lanxiang]. https://www.fortunechina.com/magazine/c/2025-03/10/content_462614.htm

Fudan Development Institute. (2020). *The Clean Network Program and U.S. digital hegemony* (Report No. 6). https://www.airuniversity.af.edu/Portals/10/CASI/documents/Translations/2020-09%20Fudan%20The%20Clean%20Network%20Report.pdf

Guangxi Big Data Development Bureau. (2024, June 21). Nanning establishes financing platforms for cross-border enterprises. *Guangxi Daily* http://dsjfzj.gxzf.gov.cn/zgdmxxg/zsyz/t18588461.shtml

Henan International Digital Trade Research Institute. (2024). *Cross-border e-commerce weekly report* (Issue 17). https://hnguoji.oss-cn-beijing.aliyuncs.com/20240527/7978b5b3aad758044fe21cc16267183d.pdf

IBM Security. (2022). *Cost of a data breach report 2021.* https://www.ibm.com/security/digital-assets/cost-data-breach-report/

IBM. (2022). *Security Cost of a Data Breach Report 2021.* https://www.ibm.com/security/digital-assets/cost-data-breach-report/.

ISEAS-Yusof Ishak Institute. (2024, January 5). *China's Digital Silk Road (DSR) in Southeast Asia: Progress and challenges.* https://www.iseas.edu.sg/wp-content/uploads/2024/01/ISEAS_Perspective_2024_1.pdf

Li, Q. Q. (2023). The U.S.-EU "Indo-Pacific Strategy": Divergent conceptions, drivers, and limits of cooperation. *Pacific Journal, 31*(4), 34–46.

Luo, J. (2024). An analysis of China-ASEAN digital economy cooperation. *E-Commerce Review, 13*(3), 5535–5540. https://doi.org/10.12677/ecl.2024.133680

Ren, J. L., & Meng, Y. M. (2022). Research on international digital trade and emerging rule trends. *Northeast Asia Economic Research, 6*(1), 109–120.

Statista. (2020, January 30). *Which countries have banned Huawei?* https://www.statista.com/chart/17528/countries-which-have-banned-huawei-products/

The Philippine Star. (2024, July 15). *Dangers of TikTok.* https://www.philstar.com/business/2024/06/15/2363074/dangers-tiktok

Wang, D. Z. (2021). China-Vietnam digital economy cooperation under the "Digital Silk Road" framework. *Journal of Hubei University of Economics, 19*(3), 32–38.

Wu, X. X. (2022). ASEAN data governance: Global context, regulatory frameworks, and cooperation with China. *Asia-Pacific Economic Review, 4*, 1–10.

Zhang, F. (2025, April 4). Building a sustainable and inclusive digital cooperation ecosystem. *Economic Daily.* http://paper.ce.cn/pad/content/202504/04/content_311750.html

Zhu, J. (2024, December 10). China and ASEAN collaborate to ignite a new engine for the digital economy. *Economic Daily.* https://www.jingjiribao.cn/static/detail.jsp?id=559757

ZTE Corporation. (2022, March 8). *ZTE Corporation 2022 annual report*. https://www.zte.com.cn/content/dam/zte-site/investorrelations/cn_annual_report/ceceefca2ea333e79768a225f02398b9.pdf