International Journal of
Strategic Research in Education, Technology and Humanities
p-ISSN: 2465-731X | e-ISSN: 2467-818X
IJSRETH
April, 2025
Vol. 13, No. 1

The Potential of the Digital Economy: A Comparative Assessment of Key Countries' Cybersecurity

[1]**Xiuli Chen,** [2]**Tao Wang,**
[3]**Xiaoxi Lin,**
[4]**Dylan Elliott Hinde,**
[5]**Qianhao Yan, &**
[6]**Zmire Zeljana**
Graduate School of International Studies,
Hanyang University, South Korea

Article DOI:
10.48028/iiprds/ijsreth.v13.i1.05

Abstract

This study investigates the digital economy capacities and cyber challenges in key nations, including China, India, Japan, Australia, South Korea, Canada, Singapore, and the United States. Using a SWOT analysis and comparative approach with data from the National Cyber Security Index (NCSI), the research focuses on digital infrastructure, cybersecurity, innovation promotion, digital divide, and regulatory challenges. The findings underline the importance of a comprehensive approach to cybersecurity, addressing national and international concerns. The study also highlights the significance of strong digital infrastructure, innovation ecosystem, and robust cybersecurity framework for success in the digital era. Although some countries have emerged as leaders in the digital economy, others like China and India are making progress in building their digital capacities. The analysis emphasizes the need for continued investment in digital infrastructure, fostering innovation, and enhancing cybersecurity to maintain competitiveness in the global digital landscape.

Keywords:
Digital capabilities, Digital divide, Cyber-attacks, Innovative ecosystem, Regulatory challenges.

Corresponding Author:
Xiuli Chen

First Published:
https://drpress.org/ojs/index.php/ijeh/article/view/12740/12399

Background to the Study

The global debate on competition policy in the digital economy revolves around the market power of large high-tech companies due to economies of scale and scope, network externalities, and the rising economic significance of data, which creates high entry barriers; regulating the sharing of data may correct these shortcomings, but privacy protection and prevention of collusive aspects must be addressed (Szczepanski, 2020). It is highlighted that the impressive growth rates of the digital economy in Southeast Asia, accelerated by the COVID-19 pandemic, and projects the digital economy to hit over $300 billion by 2025, while cautioning that the future prospect of the digital economy in the region is highly dependent on the policies enacted by the government, and benchmarks six selected ASEAN countries against critical aspects in digital economy policymaking (Erh, 2021).

Policymakers need to address issues such as digital infrastructure, access to digital technologies, digital skills development, and regulatory frameworks that facilitate innovation and protect users' rights. Building cyber- security capability can help to create an open digital trade system mediated by e-government maturity, and developing a governance framework for a secure and open digital trade system (Huang & Madnick, 2019). By examining the experiences of countries such as China, the United States, South Korea, Japan, Australia, India, Canada, Singapore and considering the insights offered by academic research, policymakers can gain valuable knowledge and guidance for developing effective strategies to harness the potential of the digital economy and address its associated cyber challenges.

Literature Review

The digital economy is influenced by a multitude of factors that affect its expansion, development, and long-term viability. Five pivotal issues that significantly contribute to the digital economy include digital infrastructure (Schade & Schuhmacher, 2022), cybersecurity (Fysarakis et al., 2022), innovation promotion (Zhang et al., 2022), digital divide (Marimuthu, et al., 2022), and regulatory challenges (Tang et al., 2022).

A resilient digital infrastructure is indispensable for delivering efficient digital services and fostering economic growth (Koutsikouri et al., 2018). Maintaining robust cybersecurity measures instills trust in digital services and safeguards essential infrastructure (Weiss & Biermann, 2021). Encouraging innovation can accelerate economic growth, generate employment, and enhance overall quality of life (Broughel & Thierer, 2019). Tackling the digital divide is crucial for guaranteeing that all citizens can reap the benefits of digital progress and actively engage in the information society (Chetty et al., 2018). Finally, effective regulation is required to strike a balance between innovation and stability, protect users, and address potential market failures (Bu, et al., 2022). These interrelated issues hold significant consequences for the evolution and growth of the digital economy and are vital considerations when analyzing the strengths, weaknesses, opportunities, and threats that key nations face.

Research Methods

In this research, two primary methods are employed to analyze the digital capacities of selected countries: 1) SWOT (Strengths, Weaknesses, Opportunities, and Threats) analysis and 2) comparison of five key issues which are highlighted from the literature review, including digital infrastructure, cybersecurity, fostering innovation, digital divide, and regulatory challenges. To conduct a comprehensive and accurate analysis, data is utilized from the National Cyber Security Index (NCSI) website, a database developed by the e-Governance Academy in Estonia. The NCSI measures countries' preparedness to prevent and respond to cyber threats and incidents. By integrating the data from the NCSI, the strengths and weaknesses of each country are identified in terms of digital capacity and cybersecurity, as well as examine their performance in addressing the challenges associated with fostering innovation, bridging the digital divide, and overcoming regulatory obstacles. This combined approach allows for a holistic understanding of the digital capacities and potential areas for improvement among the selected countries.

Economic significance is a crucial factor in choosing these key nations. As some of the world's largest and most influential economies, their impact on international trade, investment, and digital technology development is considerable. Regional representation is another vital consideration in choosing key nations for this research. With strategic locations across different regions, these nations offer diverse perspectives and regional insights, facilitating the development of comprehensive and globally relevant policies, norms, and best practices (Kleinberg et al., 2015). Technological leadership also plays an essential role in selecting these nations. Known for their technological innovations, advanced digital infrastructure, and cutting-edge research in cybersecurity, their combined efforts in addressing cyber threats can lead to significant advancements in cyber defense technologies (Boes & Leukfeldt, 2017). These advancements will benefit not only the participating nations but also contribute to the global community's collective security (Müller & Beeson, 2022).

Research Analysis and Results

The current Cyber Security Rank, National Cyber Security Index, Digital Development for the eight key nations are illustrated as figure 1. The data presented showcases the rankings and National Cyber Security Index scores of eight countries, along with their digital development scores and the differences between these two indicators. Singapore, ranked 31st, demonstrates a solid cyber security posture with an index score of 71.43, despite having a lower digital development score of 79.93. Similarly, Canada, ranked 33rd, has a cyber security index score of 70.13 and a digital development score of 75.96. South Korea, Australia, the United States, and Japan rank 34th, 40th, 44th, and 48th respectively, with varying cyber security index scores and digital development scores, all exhibiting a negative difference between the two indicators. In contrast, India, ranked 51st, shows a significant positive difference of 19.72 between its cyber security index score of 59.74 and digital development score of 40.02. Lastly, China, ranked 69th, exhibits a cyber security index score of 51.95 and a digital development score of 62.41, with a

negative difference of 10.46. This data highlights the disparities between these countries' cyber security readiness and their digital development progress, indicating the need for a more balanced approach to ensure a secure and resilient digital environment.

Rank	Country	National Cyber Security Index	Digital development	Difference
31.	Singapore	71.43	79.93	-8.50
33.	Canada	70.13	75.96	-5.83
34.	Korea (Republic of)	68.83	82.23	-13.40
40.	Australia	66.23	77.61	-11.38
44.	United States	64.94	81.05	-16.11
48.	Japan	63.64	78.69	-15.05
51.	India	59.74	40.02	19.72
69.	China	51.95	62.41	-10.46

Figure 1. Key Nations' National Cyber Security Index (2023)
Source: Data available at NCSI: https://ncsi.ega.ee

SWOT Analysis of The Digital Economy Capacities in Key Nation
The SWOT analysis (see Figure 2) above provides an overview of the cyber security situation in eight countries: China, India, Japan, Australia, South Korea, Canada, Singapore, and the United States. This discussion aims to further elaborate on the strengths, weaknesses, opportunities, and threats identified in the table.

Strengths: China, Japan, Australia, South Korea, Canada, and the United States exhibit strong policy development in cyber security, with India and Singapore closely following suit. High scores in this area suggest that these countries have a solid foundation in place to address cyber security challenges. Furthermore, Japan, Australia, South Korea, Canada, and the United States demonstrate a strong commitment to education and professional development, which helps cultivate a skilled workforce capable of addressing emerging cyber threats, In terms of incident and crisis management, Singapore stands out with its high cyber crisis management score, indicating a robust response plan to address cyber incidents. Additionally, Japan, Australia, Canada, and the United States have a strong track record in fighting against cybercrime, which contributes to the overall security of their digital environments.

Weaknesses: A common weakness among several countries is the insufficient protection of digital services and essential services. India, Australia, Singapore, and the United States exhibit low scores in these areas, indicating potential vulnerabilities that could be exploited by cybercriminals or nation-state actors. Moreover, China, India, Japan, and the United States have room for improvement in their cyber threat analysis and information capabilities. Another notable weakness is the low e-identification and trust services scores across many countries, which could hinder the adoption of secure digital services and impede the development of a reliable digital infrastructure.

Opportunities: As the digital landscape continues to evolve, countries must adapt their cyber security strategies to address emerging threats and vulnerabilities. There are significant opportunities for countries to improve their cyber threat analysis and information capabilities, as demonstrated by the United States, China, and India. By enhancing these capabilities, countries can better anticipate and mitigate potential threats. Furthermore, countries can invest in strengthening the protection of digital and essential services, as well as improving e-identification and trust services. As more services transition to digital platforms, ensuring the security and trustworthiness of these services becomes increasingly vital. Additionally, countries like Japan and Singapore, with relatively weaker military cyber operations, can focus on bolstering their capabilities in this area to deter potential adversaries and contribute to global cyber security.

Threats: The low rankings of several countries in the National Cyber Security Index present a concerning picture of their overall cyber security posture. This could make them more susceptible to cyber-attacks and increase the likelihood of successful breaches. As cyber threats become more sophisticated and prevalent, countries must continue to invest in their cyber security infrastructure, workforce, and international collaboration to mitigate these risks effectively.

The SWOT analysis highlights the varying strengths and weaknesses of different countries in the realm of cyber security. By capitalizing on the opportunities for improvement and addressing the identified threats, these nations can work towards establishing a more secure and resilient digital environment.

Table 1: SWOT Analysis of Key Nations' Cyber-Security Development

Country	Strengths	Weaknesses	Opportunities	Threats
China	-High protection of essential services and personal data - Strong cyber-security policy development	- Low e-identification and trust services - Weak cyber crisis management	- Improve cyber threat analysis and information - Enhance military cyber operations	- Low ranking in National Cyber Security Index
India	- Strong education and professional development - High protection of essential services	- Poor protection of digital services and personal data - Low global cybersecurity contribution	- Strengthen digital services protection - Enhance cyber incidents response	- Low ranking in ICT Development Index
Japan	- High scores in policy development, threat analysis, and professional development - Strong fight against cybercrime	- Low protection of essential services - Weak military cyber operations	- Improve digital and essential services protection - Strengthen military cyber operations	- Low ranking in National Cyber Security Index
Australia	- Strong policy development, threat analysis, and professional development - High fight against cybercrime	- Low protection of digital and essential services - Weak e-identification and trust services	- Enhance protection of services - Improve e-identification and trust services	- Low ranking in National Cyber Security Index
South Korea	- High scores in policy development, threat analysis, and professional development - Strong contribution to global cyber security	- Low protection of essential services - Moderate military cyber operations	- Strengthen protection of essential services - Enhance military cyber operations	- Moderate ranking in National Cyber Security Index
Canada	- Strong threat analysis and professional development - High fight against cybercrime and military cyber operations	- Low protection of digital services and e-identification and trust services - Moderate policy development	- Improve digital services protection - Enhance cyber crisis management	- Moderate ranking in National Cyber Security Index
Singapore	- Strong policy development, threat analysis, and professional development - High cyber crisis management	- No protection of digital services - Moderate e-identification and trust services	- Enhance protection of digital services - Strengthen military cyber operations	- Low ranking in National Cyber Security Index
United States	- High scores in policy development and global cybersecurity contribution - Strong fight against cybercrime and military cyber operations	- Low cyber threat analysis and information - Weak e-identification and trust services	- Improve cyber threat analysis and information - Enhance protection of essential services	- Low ranking in National Cyber Security Index

Note: This table provides a general analysis based on the data provided and may not cover every aspect of each country's cyber security situation. Data see Appendix 1

Five Key Issues Comparison

The table in Figure 3 compares the digital economy capacities of China, India, Japan, Australia, South Korea, Canada, Singapore, and the United States by examining their performance in the ICT Development Index, National Cyber Security Index, and Networked Readiness Index. These capacities are essential for driving economic growth, innovation, and competitiveness in the evolving digital landscape. South Korea, Japan, and Singapore demonstrate strong digital economy capacities, with high rankings in both the ICT Development Index and Networked Readiness Index. These countries have invested significantly in digital infrastructure, innovation, and skills. Conversely, India and China face challenges in building digital capacities, despite commitments to enhancing their digital economies. China's digital economy, for example, has grown rapidly, driven by e-commerce, internet finance, and digital manufacturing, with global technology giants like Alibaba, Tencent, and Huawei exemplifying its prowess.

Cybersecurity is a crucial aspect of digital economy capacity, with the United States leading in the Global Cybersecurity Index. However, its lower National Cyber Security Index ranking highlights the need for a holistic cybersecurity approach addressing both national and international concerns. China, despite its lower ranking, shows strengths in some cybersecurity indicators, such as protecting essential services and personal data, reflecting its efforts to secure critical infrastructure and safeguard data privacy. Yet, China's low scores in areas like cybersecurity policy development and cyber threat analysis underline the need for more comprehensive policies and initiatives.

This comparative analysis emphasizes the importance of robust digital infrastructure, innovation ecosystems, and cybersecurity frameworks for success in the digital era. While South Korea, Japan, and Singapore lead in the digital economy, China and India are progressing in building their digital capacities. Lower ICT Development Index rankings for China and India are mainly due to disparities in digital infrastructure, uneven distribution of digital resources, and challenges in providing consistent, affordable, and high-quality internet services to their populations (Wang et al., 2023). Addressing these challenges is essential for these countries to remain competitive in the global digital landscape.

Table 2: Comparison of Digital Economy Capacities (based on Appendix 1)

Country	Digital Infrastructure	Cybersecurity	Fostering Innovation	Digital Divide	Regulatory Challenges
China	80th ICT Development	69th National CSI	23rd Networked RDI	56%	14% policy development
India	134th ICT Development	51st National CSI	67th Networked RDI	30%	86% policy development
Japan	10th ICT Development	48th National CSI	13th Networked RDI	84%	100% policy development
Australia	14th ICT Development	40th National CSI	14th Networked RDI	82%	100% policy development
South Korea	2nd ICT Development	34th National CSI	9th Networked RDI	89%	100% policy development
Canada	29th ICT Development	32nd National CSI	11th Networked RDI	78%	71% policy development
Singapore	18th ICT Development	30th National CSI	2nd Networked RDI	81%	86% policy development
United States	16th ICT Development	44th National CSI	1st Networked RDI	82%	100% policy development

Conclusion and Discussion

In conclusion, the study offers valuable insights into the digital capabilities of key countries, emphasizing the importance of addressing digital infrastructure, cybersecurity, innovation promotion, digital divide, and regulatory challenges. The research's SWOT analysis highlights each nation's cybersecurity strengths and weaknesses, revealing growth opportunities and risks in creating a secure digital landscape. By capitalizing on these opportunities and addressing threats, countries can enhance their digital capabilities significantly. The comparative analysis of digital economy capacities, using metrics like the ICT Development Index, National Cyber Security Index, and Networked Readiness Index, exposes disparities between cybersecurity preparedness and digital development progress. South Korea, Japan, and Singapore lead the digital economy, while China and India advance their digital capabilities despite considerable challenges.

Key research findings stress the need to tackle the digital divide, characterized by digital infrastructure discrepancies and uneven digital resource distribution, for countries like China and India to remain competitive globally. Additionally, the study underscores the necessity of adopting a holistic cybersecurity approach, addressing both national and international concerns, for countries like the United States to maintain their leading position in the Global Cybersecurity Index. Overall, the research findings highlight the

significance of strong digital infrastructure, an innovative ecosystem, and a robust cybersecurity framework for success in the digital age. By addressing identified challenges and building on the discovered strengths, nations can work towards a more secure and resilient digital environment, ultimately contributing to global advancements and collective security.

Despite China's lower ranking in the ICT Development Index, the global success of companies like Alibaba, Tencent, and Huawei highlights China's digital economy prowess. This success can be attributed to factors such as focused investments in e-commerce, internet finance, and digital manufacturing (Noesselt, 2020), a vast domestic market (Negro, 2017), and active government support through favorable policies, financial incentives, and infrastructure. Although gaps in digital infrastructure persist, innovation hubs in cities like Beijing, Shanghai, and Shenzhen foster technological innovation and entrepreneurship (Liu & Yan, 2022). Digital infrastructure and investment significantly affect China's digital economy development (Xie, 2021), allowing Chinese tech giants to thrive globally despite lower ICT Development Index rankings (Cave et al., 2019).

Considering recent and diverse perspectives on emerging trends like artificial intelligence, blockchain, and the Internet of Things (IoT) is crucial (Yang et al., 2022). Acknowledging and exploring potential contradictions or gaps, such as the complex relationship between innovation and regulation, can enrich the literature (Noesselt, 2020). Additionally, a comparative analysis of different nations' approaches to digital economy capacities would provide valuable insights, enabling a more comprehensive understanding of the global digital landscape. Examining country-specific strategies and policies and identifying best practices and areas for improvement can better inform the ongoing discourse on developing and sustaining digital economies worldwide.

References

Boes, S., & Leukfeldt, E. R. (2017). Fighting cybercrime: A joint effort. In R. Clark & S. Hakim (Eds.), cyber-physical security: *Protecting Critical Infrastructure* (Vol. 3, pp. 137-155). Springer. https://doi.org/10.1007/978-3-319-32824-9_9.

Broughel, J., & Thierer, A. D. (2019). Technological innovation and economic growth: A brief report on the evidence. Mercatus Research Paper. https://www.mercatus.org/publications/entrepreneurship/techn ological-innovation-and-economic-growth assessed on April 18, 2023.

Bu, Y., Li, H., & Wu, X. (2022). Effective regulations of FinTech innovations: The case of China. *Economics of Innovation and New Technology,* 31(8), 751-769. https://doi.org/10.1080/10438599.2020.1868069

Cave, D., Hoffman, S., Joske, A., Ryan, F., & Thomas, E. (2019). Mapping China's technology giants. https://www.asianstudies.org/wp-content/uploads/chinas-national-champions-alibaba-tencent-and-huawei.pdf. assessed on April 19, 2023.

Chetty, K., Qigui, L., Gcora, N., Josie, J., Wenwei, L. & Fang, C. (2018). Bridging the digital divide: measuring digital literacy. *Economics*, *12*(1), 20180023. https://doi.org/10.5018/economics-ejournal.ja.2018-23

Erh, Joey. (2021). *Assessing digital economy policies in Six Southeast Asian countries*. © ISEAS Yusof Ishak Institute. http://hdl.handle.net/11540/13645.

Fysarakis, K., Mavroeidis, V., Athanatos, M., Spanoudakis, G., & Ioannidis, S. (2022). A Blueprint for Collaborative Cybersecurity Operations Centres with Capacity for Shared Situational Awareness, Coordinated Response, and Joint Preparedness. In 2022 IEEE International Conference on Big Data (Big Data) (pp. 2601-2609). IEEE. https://doi.org/10.1109/BigData55660.2022.10020736

Huang, K., & Madnick, S. E. (2019). *Does high cybersecurity capability lead to openness in digital trade? the mediation effect of e-government maturity within Cross-border Digital Innovation*, Available SSRN: https://ssrn.com/abstract=3542552 or http://dx.doi.org/10.2139/ssrn.3542552.

Jiang, H., & Murmann, J. P. (2022). The rise of China's digital economy: An overview, *Management and Organization Review, 18*(4), 790-802. DOI: https://doi.org/10.1017/mor.2022.32

Kleinberg, H., Reinicke, B., & Cummings, J. (2015). Cyber security best practices: What to do?. *Journal of Information Systems Applied Research, 8*(2), 52-59. http://jisar.org/2015-8/ ISSN: 1946-1836. (A preliminary version appears in The Proceedings of CONISAR 2014).

Koutsikouri, D., Lindgren, R., Hen fridsson, O., & Rudmark, D. (2018). Extending digital infrastructures: A Typology of Growth Tactics. *Journal of the Association for Information Systems, 19*(10). Retrieved from https://aisel.aisnet.org/jais/vol19/iss10/2

Liu, C., & Yan, S. (2022). Transnational technology transfer network in China: Spatial dynamics and its determinants, *Journal of Geographical Sciences, 32*, 2383-2414. https://doi.org/10.1007/s11442-022-2053-y

Marimuthu, R., Gupta, S., Stapleton, L., Duncan, D., & Pasik-Duncan, B. (2022). Challenging the Digital Divide: Factors Affecting the Availability, Adoption, and Acceptance of Future Technology in Elderly User Communities. *Computer, 55*(7), 56-66. doi:10.1109/MC.2022.3172026.

Müller, L. M., & Beeson, M. (2022). From collective security to the construction of regional security communities: regional security governance in a global context. In Handbook on Global Governance and Regionalism (pp. 307-322). Edward Elgar Publishing. https://doi.org/10.4337/9781800377561.00033

Negro, G. (2017). *Internet in China (pp. 193-208).* London, UK: Palgrave Macmillan. https://link.springer.com/book/10.1007/978-3-319-60405-3. accessed on April 18, 2023.

Noesselt, N. (2020). City brains and smart urbanization: regulating 'sharing economy' innovation in China, *Journal of Chinese Governance, 5*(4), 546-567. https://doi.org/10.1080/23812346.2020.1762466

Schade, P., & Schuhmacher, M. C. (2022). Digital infrastructure and entrepreneurial action-formation: A multilevel study, *Journal of Business Venturing, 37*(5), 106232. https://doi.org/10.1016/j.jbusvent.2022.106232.

Szczepanski, M. (2020*). Is data the new oil? Competition issues in the digital economy,* EPRS: European Parliamentary

Research Service. Belgium. Retrieved from https://policycommons.net/artifacts/1337441/is-data-the-new-oil-competition-issues-in-the-digital-economy/1945293/ on 17 Apr 2023. CID: 20.500.12592/5qwqk4.

Tang, J., Wu, Z., Zhang, Y., Guo, H., Du, X., & Wang, D. (2022*). Financial application scenarios and regulatory challenges of blockchain technology*, ITM Web of Conferences, 45, 01069. https://doi.org/10.1051/itmconf/20224501069

Wang, Y., Peng, Q., Jin, C., Ren, J., Fu, Y., & Yue, X. (2023). Whether the digital economy will successfully encourage the integration of urban and rural development: A case study in China, *Chinese Journal of Population, Resources and Environment, 21*(1), 13-25. https://doi.org/10.1016/j.cjpre.2023.03.002

Weiss, M., & Biermann, F. (2021). Cyberspace and the protection of critical national infrastructure, *Journal of Economic Policy Reform, 1*-18. https://doi.org/10.1080/17487870.2021.1905530

Xie, Z. (2021). *Research on comprehensive evaluation of digital economy development level in typical areas of China.* In 2021 International Conference on Public Management and Intelligent Society (PMIS) (pp. 181-184). IEEE. https://doi.org/10.1109/PMIS52742.2021.00046

Yang, Q., Zhao, Y., Huang, H., Xiong, Z., Kang, J., & Zheng, Z. (2022). Fusing blockchain and AI with Metaverse: A survey. *IEEE Open Journal of the Computer Society, 3*, 122-136. https://doi.org/10.1109/OJCS.2022.3188249

Zhang, J., Lyu, Y., Li, Y., & Geng, Y. (2022). Digital economy: An innovation driving factor for low-carbon development. *Environmental Impact Assessment Review, 96*, 106821. https://doi.org/10.1016/j.eiar.2022.106821.