MEST Journal
DOI 10.12709/mest.12.12.02.10

DIGITAL ECONOMY AND CYBERSECURITY ANALYSIS WITH A FOCUS ON CHINA AND SLOVENIA

Bogdan Vukosavljevic
China-CEEC Innovation Cooperation Research Center, Ningbo University of Technology, Ningbo, PR China, and
The European Center for Peace and Development, Belgrade, Serbia
https://orcid.org/0009-0008-1228-5070

Martin Kralj
University of Ljubljana, Ljubljana, Slovenia
https://orcid.org/0009-0002-6799-2035

Marko Vidnjevic
China-CEEC Innovation Cooperation Research Center, Ningbo University of Technology, Ningbo, PR China, and
Alma Mater Europaea - ECM, Slovenia
https://orcid.org/0009-0004-1107-1186

JEL Category: **F15, F36, O18**

Abstract

This paper explores the evolving landscape of digital economy cooperation between China and the Central and Eastern European Countries (CEECs), set against the backdrop of the China-CEEC Cooperation Initiative and the Belt and Road Initiative (BRI). It highlights the untapped potential for digital economy projects, despite the absence of major projects under the BRI framework, and underscores China's strategic shift towards exploring new areas of collaboration, including the digital economy, artificial intelligence, financial technology, life sciences, and environmental protection. The paper delves into the rapid development of the digital economy, accelerated by the COVID-19 pandemic, focusing on how both China and the CEECs are strengthening their digital economies to overcome current challenges and foster future growth. It examines China's commitment to digital economy expansion, digital governance, and international cooperation, including initiatives such as the "Global Initiative on Data Security" and the application to join the Digital Economy Partnership Agreement (DEPA). Additionally, the paper considers the digital economy in Slovenia, highlighting its strategic

Address of the corresponding author:
Martin Kralj
martin.kralj007@gmail.com

commitment to digitalization, cybersecurity efforts, and its role within the broader digital transformation landscape in Europe. Through this analysis, the paper aims to provide insights into the opportunities and challenges of China-CEEC digital economy cooperation, offering recommendations for fostering effective collaboration and advancing mutual benefits in the digital era.

Keywords: *China-CEEC Cooperation Initiative. Belt and Road Initiative (BRI). Digital economy cooperation. Digital governance. Cybersecurity efforts.*

1 INTRODUCTION

The China-Central and Eastern European Countries (CEEC) Cooperation, initiated on April 26, 2012, serves as a cross-regional platform fostering mutual benefit and development through pragmatic collaboration across diverse sectors such as economy, culture, education, and technology. Facilitated by regular Leaders' Summits, this cooperation has expanded substantially, contributing positively to bilateral relations between China and the CEECs and enhancing broader China-Europe relations. (China-CEEC Cooperation, 2021).

The integration of digital economy sectors into the Belt and Road Initiative started in 2015 to enhance international communications connectivity and establish an "Information Silk Road" with the cross-border optical cable networks and other communication trunk lines construction. Despite the Central and Eastern European countries' participation in Belt and Road Forums, no major digital economy projects were organized or implemented under the BRI framework. Nevertheless, there is significant untapped potential for further development (China-CEE Institute, 2021).

Moreover, during the summit in 2019 held in Ljubljana, Chinese State Councilor and Foreign Minister Wang Yi emphasized the cooperation's transition towards exploring new areas of collaboration. He highlighted the opportunity to deepen traditional collaboration while also expanding into new fields such as the digital economy, artificial intelligence, financial technology, life science, and environmental protection. This strategic shift underscores a proactive approach aimed at fostering even stronger win-win cooperation and exploring new avenues of mutual benefit, ultimately pushing for the advancement of China-Europe relations (China CEEC, 2019).

The rapid development of the digital economy, driven by technologies like the Internet, big data, and artificial intelligence, is reshaping global economic structures and competitive dynamics. The COVID-19 pandemic has further accelerated this trend, with countries increasingly relying on digital means for pandemic control and economic recovery. China and Central and Eastern European countries (CEECs) are both actively strengthening their digital economies amidst the pandemic challenges. Despite facing new cooperation hurdles, digital economic collaboration has emerged as a key focus for advancing China-CEEC cooperation (CIIS & HIIA, 2022).

2 DIGITAL ECONOMY IN CHINA

China views the digital economy as pivotal amidst global transformations. The government is committed to promoting digital applications and services for the benefit of its citizens, while also enhancing domestic laws and regulations and integrating into global digital governance frameworks. China actively seeks to join high-level digital trade agreements, fosters global digital economic cooperation, and advocates for an open, inclusive, and balanced approach to digital governance. On the other hand, Economic growth in Central and Eastern European countries (CEECs) has traditionally relied on key industries, exports, foreign direct investments, and EU cohesion funds. However, these growth drivers are becoming exhausted, with labor shortages and overreliance on specific export markets and industries such as automotive. To overcome these challenges and move up in the global value chain, CEECs are increasingly focusing on digitization. Furthermore, China actively engages in global cooperation within the digital economy, collaborating with other nations to foster its healthy development and create new opportunities for global economic growth. President Xi Jinping called for a shared cyberspace community at the 3rd World Internet Conference in November 2016. In September 2020, China introduced the "Global Initiative on

Data Security," aimed at contributing insights to data security maintenance, digital development, cooperation, and global digital governance enhancement. Additionally, China's formal application to join the Digital Economy Partnership Agreement (DEPA) in November 2021 showcases China's commitment to participating in international digital economy exchanges and cooperation efforts (CIIS & HIIA, 2022).

Since then, China has engaged in several rounds of dialogues with DEPA members, providing insights into its laws, regulations, and regulatory practices concerning the digital economy. Additionally, China has actively demonstrated its willingness to cooperate under the DEPA framework (Xinhua, 2023a).

The recent developments in China's digital economy underscore a remarkable journey of digitalization and growth over the past decade. By 2022, the digital economy had surged to approximately 6.99 trillion U.S. dollars, a significant leap from its valuation in 2012. This expansion is mirrored in the country's internet user base, which nearly doubled, reaching 1.08 billion by June 2023, alongside a substantial increase in internet penetration from 42.1% to 76.4%. The thriving digital community has paved the way for the success of internet enterprises, with the number of Chinese internet companies listed on stock markets expanding from just over 50 in 2012 to nearly 160 in 2023, marking the rise of giants such as ByteDance and Pinduoduo. The advancement of AI technologies, particularly foundation models, is reshaping the digital landscape, enhancing productivity, and fostering industry innovation. The China Internet Development Report 2023 highlights China's commitment to amplifying the application of new technologies across critical sectors, including agriculture and education, while addressing the digital transformation hurdles faced by small and medium-sized enterprises due to financial and technological constraints. China's vision for international cooperation in digital applications and the promotion of global digital governance rules reflects its proactive stance on shaping a more inclusive digital future. The Digital Silk Road initiative exemplifies this approach, aiming to extend the benefits of internet development globally. The emphasis on fostering regional collaboration and creating an equitable digital ecosystem was echoed at the Wuzhen Summit, signaling China's intent to integrate digital and real economies more deeply and support the digital transformation of small and medium-sized businesses. Despite these advancements, challenges such as data privacy and security remain, particularly in the application of AI foundation models. These concerns highlight the need for balanced development that not only boosts productivity but also safeguards user privacy and data integrity, underscoring the complexities of navigating the digital economy's future trajectory (Xinhua, 2023b).

Xu and Li (2022) analyzed the digital economy across 31 provinces in mainland China from 2010 to 2020, they revealed several critical findings that contribute to the understanding of digital economic growth and its disparities. Firstly, the digital economy in China has exhibited a steady expansion, yet this growth is accompanied by increasing regional disparities, with a pronounced development gradient from east to west. This disparity is partly due to the varying effectiveness in adopting advanced digital technologies, with a notable decline in 2020 likely caused by the disruptions of the COVID-19 pandemic, which affected demand and supply chains, especially in economically developed regions. Secondly, the study underscores the steady progress in the performance of digital platforms, despite fluctuations influenced by domain name issues and regulatory changes aimed at fraud reduction and network security enhancement. It highlights a regional imbalance in digital platform development, with higher scores predominantly in the eastern and central regions, though the disparity gap has shown a slight narrowing over time. The research also points out a consistent upward trend in the performance of digital users, driven by improvements in mobile phone penetration and telecommunication service volumes. This trend reflects an enhanced network environment, reduced internet transaction costs, and expanded internet access, with a decreasing distribution trend from east to west. Furthermore, digital innovation has demonstrated growth from 2010 to 2019, with more developed regions typically generating more innovations. The geographical distribution of digital innovation aligns with the socioeconomic landscape, but there are efforts underway to balance the digital

resource distribution to foster innovation in less developed areas. Lastly, the digital industries have shown steady development over the decade, with a pronounced provincial and east-to-west imbalance. Despite this, certain less developed regions have made significant progress in digital industrialization, supported by favorable policies, exemplifying Liaoning's advancements in digital industries.

China's latest digital development plan outlines a comprehensive strategy to foster a digital China. Aimed at supporting the country's modernization efforts in the digital era, the plan envisions significant advancements in digital infrastructure, the economy, and technology innovation by 2025. By 2035, the goal is for China to become a global leader in digital development, achieving harmonious progress across economic, political, cultural, social, and ecological domains. The strategy emphasizes the integration of digital technology with the real economy, applying digital innovations across diverse sectors such as agriculture, manufacturing, finance, education, medical services, transportation, and energy. Additionally, the plan seeks to establish a thriving digital government, a vibrant cyberspace culture, accessible digital public services, and digital technology-driven ecological governance. Central to this vision is fostering an ecosystem that encourages independent digital technology innovation, with businesses playing a pivotal role and a strong emphasis on improving intellectual property protection. (Xinhua, 2023c)

3 CYBERSECURITY IN CHINA

As highlighted in China's commitment to international digital economy exchanges and cooperation efforts, the importance of cybersecurity in the digital transformation underscores the critical necessity of safeguarding digital infrastructure. In today's interconnected world, where data is increasingly digitized and exchanged across borders, cybersecurity plays a crucial role in protecting sensitive information, maintaining trust, and ensuring the integrity of digital transactions. With cyber threats evolving in sophistication and frequency, businesses, governments, and individuals face unprecedented risks of data breaches, cyberattacks, and digital fraud. Therefore, investing in robust cybersecurity measures is not only necessary to mitigate these risks but also essential for fostering confidence in digital technologies and enabling the continued growth and innovation of the digital economy. By prioritizing cybersecurity, organizations can proactively defend against cyber threats, safeguard critical assets, and uphold the privacy and security of digital infrastructure, thereby facilitating a safe and secure environment for digital commerce, communication, and collaboration.

The Data Security Law of the People's Republic of China, effective from September 1, 2021, aims to regulate data processing and ensure data security while promoting data utilization and protecting rights (The National People's Congress of the People's Republic of China, 2021). It encompasses:

- General Provisions: Establishes the law's purpose, scope, and fundamental principles, including the importance of safeguarding national security and individual rights in data activities.
- Data Security and Development: Outlines the state's role in promoting secure data development and utilization, emphasizing the balance between security and economic growth.
- Data Security Systems: Introduces systems for classifying, protecting, and managing data based on its importance and the potential impact of its compromise.
- Data Security Protection Obligations: Details obligations for data processors, including adherence to laws, implementing security measures, and conducting regular risk assessments.
- Security and Openness of Government Data: Focuses on enhancing e-government, protecting government data, and promoting transparency and accessibility.
- Legal Liability: Specifies penalties for violations of the law, including fines and other sanctions to enforce compliance.
- Supplementary Provisions: Addresses additional aspects like the application of the law to state secrets and military data security.

4 DIGITAL ECONOMY IN SLOVENIA

The digital economy in Slovenia is characterized by widespread internet and broadband access,

significant investments in ICT, and a growing ICT sector. Key elements include e-business, e-commerce, social media use, cloud computing, and the Internet of Things, underpinned by a skilled workforce with various levels of e-skills. The digital economy's growth is reflected in the increasing importance of online activities and ICT in economic, social, and cultural spheres, driving changes in business processes, work, production, and overall economic development (Zupan, 2016).

In the 2022 Digital Economy and Society Index (DESI), Slovenia showcases a strategic commitment to digitalization, ranking 11th among the EU countries. That reflects its consistent efforts towards enhancing digital skills, infrastructure, and public sector digitalization. Despite nearing the EU average in human capital, Slovenia identifies gaps in digital skills, emphasizing the need for ongoing reskilling and upskilling to adapt to technological advancements. Its enterprises outperform the EU average in providing ICT training, indicating a strong focus on workforce development. Slovenia's digital connectivity exhibits strengths in high-capacity network coverage but faces challenges in 5G deployment, highlighting areas for technological improvement. The country also demonstrates robust performance in integrating digital technologies among SMEs, particularly in cloud services and artificial intelligence, yet it sees potential for growth in big data utilization. The Digital Slovenia 2030 strategy outlines a comprehensive roadmap for digital transformation, focusing on digital skills, secure infrastructure, business digitization, and public service innovation. This initiative aims to foster an inclusive digital society, leveraging digital technologies for economic growth and social welfare. Moreover, Slovenia's proactive approach to cybersecurity and data governance, especially in response to global incidents, underscores the importance of resilience and trust in the digital era. Through strategic investments and policy initiatives, Slovenia aspires to a digitally enabled future, emphasizing inclusivity, innovation, and security as foundational pillars. The DESI 2022 report highlights Slovenia's journey towards realizing its digital ambitions, positioning it as a proactive participant in Europe's digital transformation landscape (European Commission, 2023).

5 CYBERSECURITY IN SLOVENIA

Cybersecurity in Slovenia has evolved significantly, marked by the adoption of the Cybersecurity Strategy in 2016 and the establishment of the Government Office for the Protection of Classified Information (UVTP) as the national cybersecurity authority in 2017. Slovenia's proactive approach to cybersecurity is further exemplified by the longstanding operation of SI-CERT, the national response center for cybersecurity incidents since 1995. Despite the comprehensive framework and efforts to safeguard digital assets, Slovenia has experienced minor cybersecurity incidents, with the most significant being the WannaCry ransomware attack in 2017, which underscored the persistent threat landscape and the need for continuous vigilance and enhancement of cybersecurity measures (Ministrstvo za javno upravo, 2018).

Slovenia's proactive approach to cybersecurity is underscored by the establishment of SI-CERT, the Slovenian Computer Emergency Response Team. This vital entity operates within the broader framework of ARNES (Academic and Research Network of Slovenia) and stands as a testament to the country's commitment to maintaining a secure and resilient digital environment. As the designated national authority for monitoring and responding to cybersecurity incidents, SI-CERT plays a critical role in Slovenia's cybersecurity strategy. It offers a comprehensive suite of services, including early warning systems, risk and incident analysis, methodological support in case of incidents, and the dissemination of crucial information on cybersecurity risks to relevant stakeholders. Furthermore, SI-CERT's involvement in international cooperation networks and its efforts to raise public awareness through initiatives like the Safe on the Internet program reflect Slovenia's integrated approach to addressing cybersecurity challenges. Funded by the Government Information Security Office, SI-CERT's operations are pivotal in safeguarding Slovenia's informational assets and enhancing the nation's cyber defense capabilities (SI-CERT, 2024).

In 2022, SI-CERT managed a total of 4,123 cybersecurity incidents. An estimated breakdown suggests that technical attacks and incidents

involving social engineering constituted roughly 30% of these occurrences each, with phishing attacks accounting for the remaining 40%. This figure indicates a marked escalation in incident numbers over the previous years, with 3,177 incidents recorded in 2021 and 2,775 incidents in 2020.

In the EU-27, the sectors that experienced the highest incidence of ICT security-related issues, leading to disruptions in ICT services, data destruction or corruption, or the disclosure of confidential information, were the ICT sector (29.6%), professional, scientific, and technical activities (30.8%), and the sectors of water supply, sewerage, waste management, and remediation activities (24.6%). The construction sector (17.6%) and the domain of wholesale and retail trade, including the repair of motor vehicles and motorcycles (23.7%), were comparatively less impacted. The higher vulnerability in the ICT sector can be linked to its extensive use of digital technologies, possession of vast amounts of sensitive information, and possibly more nascent security protocols relative to other sectors. In contrast, Slovenia's most impacted sectors were water supply, sewerage, waste management, and remediation activities (23.7%), along with professional, scientific, and technical activities (18.7%), reflecting a similar pattern of ICT security challenges (Gorišek, Pregarc, Dobnik, Ferjan, & Kralj, 2023)

Furthermore, Gorišek and others (2023) identified that organizations prioritize three primary components in their cybersecurity strategies: confidentiality, integrity, and availability, acknowledging the interconnectedness of these concepts. They observed that while some companies emphasize availability due to the operational necessity of continuous production, others, particularly in the financial sector prioritize confidentiality and integrity, highlighting industry-specific cybersecurity priorities. Their study identified five significant cybersecurity risks across various Slovenian sectors: environmental and human safety, production goals, product quality, and the protection of sensitive information, noting that the degree of cybersecurity threats often correlates with an organization's level of digitalization. Sensitive information was identified as the most pressing concern across all sectors. They reported that companies use standard risk assessment methodologies and invest in employee training and data security software for protection. Despite these measures, challenges such as remote workforce security and skills shortages underline the complexity of maintaining robust cybersecurity defenses.

The study highlighted the increasing risk of human exploits and the role of AI in enabling attackers to generate widespread attacks. The study advocates for a proactive approach to cybersecurity, emphasizing the importance of continuous employee training, regular updates to security software, and the development of comprehensive business continuity plans to navigate the evolving threat landscape effectively.

6 CONCLUSIONS

In conclusion, this paper analyzed the complex and dynamic nature of digital economy cooperation between China and the Central and Eastern European Countries (CEECs), framed within the context of the China-CEEC Cooperation Initiative and the Belt and Road Initiative (BRI). Despite the initial absence of major digital economy projects under the BRI framework, the analysis pointed out an evident potential for engaging in untapped areas such as artificial intelligence, financial technology, life sciences, and environmental protection. The rapid advancement of the digital economy, expedited by the COVID-19 pandemic, revealed both opportunities and challenges, emphasizing the importance of strengthening digital infrastructures, enhancing digital governance, and fostering international collaboration.

China's significant strides in digital economy expansion, including efforts to join international digital agreements like the DEPA and initiatives such as the "Global Initiative on Data Security," showcased a commitment to playing a leading role in global digital governance. The paper also analyzed the digital economy landscape in Slovenia, which exemplified a strategic commitment to digitalization, underscored by substantial progress in cybersecurity measures, thereby contributing to the broader European digital transformation efforts.

The insights derived from this analysis underscored the importance of continued collaboration, innovation, and mutual benefit. It

called for both China and the CEECs to leverage the opportunities presented by the digital economy to foster economic growth, enhance digital governance, and address cybersecurity challenges. As these regions navigated the complexities of the digital era, their collaborative efforts served as a blueprint for other cross-regional partnerships aiming to harness the benefits of the digital economy for sustainable and inclusive development.

WORKS CITED

China CEEC. (2019). Cooperation between China and Central and Eastern European Countries. Retrieved from China-CEEC cooperation entering new phase: Chinese FM: http://www.china-ceec.org/eng/zzwl/202001/t20200102_6581925.htm.

China-CEE Institute. (2021). Chinca-CEE Institute. Retrieved from Digital Economy in Central and Eastern Europe: https://china-cee.eu/wp-content/uploads/2021/08/2021Book01PDF.pdf.

China-CEEC Cooperation. (2021). Cooperation between China and Central and Eastern European Countries. Retrieved from About Us: http://www.china-ceec.org/eng/jj/zyjz/202112/t20211228_10476286.htm

CIIS & HIIA. (2022). China Institute of International Studies. Retrieved from The Status and Prospects of China-CEECs: https://www.ciis.org.cn/zdogjqqhbzx/yjcg/202204/P020220415311036312969.pdf

European Commission. (2023). European Commission. Retrieved from Slovenia in the Digital Economy and Society Index: https://digital-strategy.ec.europa.eu/en/policies/desi-slovenia.

Gorišek, A., Pregarc, M., Dobnik, T., Ferjan, M., & Kralj, M. (2023). Tackling Cybersecurity Challenges in the Age of AI. Beyond Bits and Algorithms: Redefining Businesses and the Future of Work, pp. 261-272.

Ministrstvo za javno upravo. (2018). Portal GOV.SI. Retrieved from Ocena kibernetskih tveganj: https://www.gov.si/assets/ministrstva/MDP/DID/Ocena-kibernetskih-tveganj-1_0.pdf

SI-CERT. (2023). SI-CERT. Retrieved from Poročilo o kibernetski varnosti za leto 2022: https://www.cert.si/wp-content/uploads/2023/06/Porocilo-o-kibernetski-varnosti_2022_web-1.pdf

SI-CERT. (2024). SI-CERT. Retrieved from About SI-CERT: https://www.cert.si/en/about-si-cert/.

Xinhua. (2023 a). State Council of the People's Republic of China. Retrieved from China keen to join Digital Economy Partnership Agreement: commerce minister: https://english.www.gov.cn/news/202305/27/content_WS6471c869c6d03ffcca6ed733.html.

Xinhua. (2023 b). China's economy ushers in digital transformation. State Council of the People's Republic of China. Retrieved from: http://english.scio.gov.cn/m/in-depth/2023-11/10/content_116806911.htm#:~:text=By%20June%202023%2C%20China%20had,China%20over%20the%20past%20decade.

Xinhua. (2023 c). State Council of the People's Republic of China. Retrieved from China unveils plan to promote digital development: https://english.www.gov.cn/policies/latestreleases/202302/28/content_WS63fd33a8c6d0a757729e752c.html.

Zupan, G. (2016). *E-skills and Digital Economy*. Republic of Slovenia Statistical Office. Retrieved from: https://www.stat.si/statweb/File/DocSysFile/8970/e-skills_and_digital_economy.pdf

The National People's Congress of the People's Republic of China. (2021). *The National People's Congress of the People's Republic of China*. Retrieved from Data Security Law of the People's Republic of China: http://www.npc.gov.cn/englishnpc/c2759/c23934/202112/t20211209_385109.html.

Xu, Y., & Li, T. (2022). Measuring digital economy in China. *National Accounting Review, 4*(3), pp. 251-272. Retrieved from https://www.aimspress.com/aimspress-data/nar/2022/3/PDF/NAR-04-03-015.pdf.

Received for publication: 19.03.2024
Revision received: 24.04.2024
Accepted for publication: 01.07.2024

How to cite this article?

Style – **APA** *Sixth Edition:*

Vukosavljevic, B., Kralj, M., & Vidnjevic, M. (2024, 07 15). Digital Economy and Cybersecurity Analysis with a Focus on China and Slovenia. (Z. Cekerevac, Ed.) *MEST Journal, 12*(2), 75-82. doi:10.12709/mest.12.12.02.10

Style – **Chicago** *Sixteenth Edition:*

Vukosavljevic, Bogdan, Martin Kralj, and Marko Vidnjevic. "Digital Economy and Cybersecurity Analysis with a Focus on China and Slovenia." Edited by Zoran Cekerevac. *MEST Journal* (MESTE) 12, no. 2 (07 2024): 75-82.

Style – **GOST** *Name Sort:*

Vukosavljevic Bogdan, Kralj Martin and Vidnjevic Marko Digital Economy and Cybersecurity Analysis with a Focus on China and Slovenia [Journal] // MEST Journal / ed. Cekerevac Zoran. - Belgrade – Toronto : MESTE, 07 15, 2024. - 2 : Vol. 12. - pp. 75-82.

Style – **Harvard** *Anglia:*

Vukosavljevic, B., Kralj, M. & Vidnjevic, M., 2024. Digital Economy and Cybersecurity Analysis with a Focus on China and Slovenia. *MEST Journal,* 15 07, 12(2), pp. 75-82.

Style – **ISO 690** *Numerical Reference:*

Digital Economy and Cybersecurity Analysis with a Focus on China and Slovenia. **Vukosavljevic, Bogdan, Kralj, Martin and Vidnjevic, Marko.** [ed.] Zoran Cekerevac. 2, Belgrade – Toronto : MESTE, 07 15, 2024, MEST Journal, Vol. 12, pp. 75-82.