Economic security in the digital economy in Vietnam

Assoc. Prof. Dr. Do Thi Kim Tien
Academy of Public Administration and Governance

Abstract: ***Ensuring socio-economic stability and development has always been a critical concern for nations throughout history, directly influenced by economic security. In the current context, the rapid advancement of the technological revolution, accompanied by digital transformation and the growth of the digital economy, has presented numerous opportunities while also posing significant challenges to Vietnam's economic security. This study aims to clarify the nature of economic security and identify the risks and challenges posed by the digital economy. Based on these insights, it proposes strategic directions and policy solutions to overcome such challenges, effectively adapt to the new context, and fully leverage development opportunities in the country's digital era.***

Keywords: *Economic security; digital transformation; digital economy; risk identification.*

1. Introduction

The remarkable development of modern technologies - such as the Internet, artificial intelligence (AI), big data, cloud computing, and the digital economy - profoundly transforms the entire chain of production, distribution, and consumption. These advancements are occurring rapidly and diversely, no longer conforming to traditional models. In Vietnam, the digital economy has been identified as a key driver of growth and innovation. However, alongside tremendous development opportunities, the digital economy also presents increasingly complex challenges, particularly in the field of economic security.

Currently, economic risks no longer manifest in traditional forms but predominantly emerge in cyberspace, with greater sophistication and difficulty in control. Although the Government is actively implementing the National Digital Transformation Program and striving to build a sustainable digital economy, issues such as data security, financial information safety, e-commerce fraud, and high-tech crime pose serious and latent threats to national economic security.

This situation becomes even more concerning as digital infrastructure systems, technology enterprises, and the financial banking system increasingly rely on digital platforms. At the same time, cybersecurity capabilities remain

Received:
April 02, 2025
Revised:
May 08, 2025
Accepted:
June 20, 2025
https://doi.org
10.59394/JSM.65

limited, fragmented, and lagging behind the pace of technological advancement. In light of these growing non-traditional threats, identifying and analyzing the risks to economic security in the digital economy context is crucial for proposing effective strategic solutions to safeguard national interests.

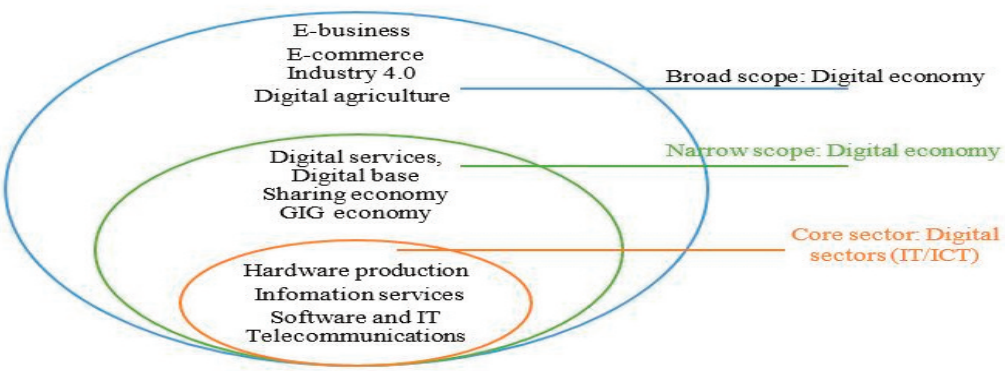
2. Overview of economic security in the digital economy

The term "digital economy" was first introduced in 1995 by Don Tapscott, a Canadian technology expert. According to Tapscott, the digital economy is not merely a system of technological machinery but a network that connects people through technology. This concept laid the foundation for an extensive wave of research on the nature and scope of the digital economy in the following decades. Lane (1999) approached the digital economy from an e-commerce perspective, viewing it as the development of business activities through the Internet. Margherio et al. (1999) identified four main drivers of the digital economy: (1) the emergence and development of the Internet, (2) the expansion of e-commerce, (3) the digitization of the distribution of goods and services, and (4) the shift toward a digital retail environment.

Brynjolfsson and Kahin (2000) argued that the digital economy entails the transformation of economic sectors through the digitization of information. Similarly, Kling and Lamb (2000) defined the digital economy as the entire process of producing, delivering, and consuming goods and services based on digital technology. More recently, Besada (2018) expanded the definition by considering the digital economy as a business model and a new economic structure that integrates intellectual capital, intangible assets, and technological innovation. According to Ganichev and Koshovets (2019), the digital economy encompasses creating, distributing, and utilizing digital technologies and related products and services. Mambetomorov and Almasbekova (2021) emphasized that the digital economy drives a comprehensive transformation of socioeconomic systems, in which goods and services are digitized and operated primarily in virtual spaces enabled by advances in information technology.

Notably, Verhoef et al. (2021) highlighted that value is generated within enterprises across entire digital ecosystems and collaborative networks in the digital economy context. This underscores a critical requirement for businesses: shifting their strategic mindset from traditional value chain models to collaborative value creation, where all stakeholders actively participate in value co-creation.

Figure 1. Scope of the digital economy



Source: Rumana Bukht & Richard Heeks (2017).

Based on the synthesis of the perspectives mentioned above, the digital economy is a collection of economic activities that originate from or operate based on digital goods and services, encompassing both core digital sectors and extended economic activities supported by digital technologies. Under the prevailing classification, the digital economy is commonly divided into three scopes: (1) The core sector, which includes digital technology industries such as software, telecommunications, and artificial intelligence (AI); (2) The narrow scope, which encompasses economic activities that primarily rely on digital technologies for operation, such as e-commerce and digital finance; and (3) The broad scope, referring to traditional economic sectors that have been partially digitized, including smart agriculture and smart tourism (*see Figure 1*).

The concept of economic security has received increasing attention in recent years, particularly as nations are compelled to adapt and adjust policies amid deepening international economic integration and globalization. This context has led to a rapid expansion of cross-border economic relations, diversification of economic actors, and qualitative and quantitative transformations in economic elements, resulting in the emergence of regional and global crises, as well as multifaceted and complex economic threats. Accordingly, economic security is generally understood as the condition in which an economy is either free from or capable of managing threats and risks, thereby ensuring stability and the capacity to absorb unpredictable environmental shocks. In other words, economic security involves sustaining the stable development of economic sectors despite internal and external instabilities (Tohirov, 2013).

Moreover, economic security threats directly impact both businesses and individuals. For businesses, the risks include industrial espionage, cyberattacks, data theft, and manipulation. For individuals, over dependence on technology may result in the gradual loss of control over personal information, negatively affecting identity, competitiveness, and - more broadly - national economic security. To safeguard economic security, countries often implement measures such as promoting innovation, directing strategic investments, developing national programs, expanding public-private partnerships, and optimizing the use of existing resources. The integration of digital technology into economic activities and governance also has a direct effect on the effectiveness of economic security assurance.

3. Economic risks in the context of digital economy development in Vietnam

Digital transformation is currently identified as one of Vietnam's top strategic priorities in the national development process. Resolution No. 57-NQ/TW, dated December 22, 2024, issued by the Politburo, clearly outlines the country's vision for 2045, emphasizing that breakthroughs in science, technology, innovation, and digital transformation are essential conditions for enhancing national competitiveness. The Government has concretized this policy through the National Digital Transformation Program to 2025, with an orientation toward 2030, which includes key targets such as developing electronic payment accounts for over 80% of the population, universalizing digital infrastructure (broadband Internet and 5G), building a digital government, developing

digital platforms for businesses, and positioning Vietnam among the top 30 countries in the world for cybersecurity, as measured by the Global Cybersecurity Index (GCI).

Based on this strategy, Vietnam has identified four main pillars for digital economy development: the information technology industry, digitalization of industrial sectors, digital governance, and digital data management. Cyberspace is now regarded as a new domain of national survival, with digital transformation playing a central role. This transformation aims to develop the digital economy, build e-government and smart cities, and ultimately transition to a fully digital government model. The digital economy is becoming an increasingly critical component of Vietnam's overall economic structure. Specifically, the digital economy's contribution to GDP increased from 12.66% in 2020 to 13.17% in 2024. The service sector experienced significant growth, rising from 6.53% to 7.15% of GDP, while the industrial and construction sectors saw a slight decline (*see Table 1*). In 2024, the scale of the digital economy reached approximately USD 36 billion and is projected to grow to USD 45 billion by 2025, with the potential to reach between USD 90 and 200 billion by 2030 (Temasek & Brain, 2024).

Table 1. Contribution of the digital economy to Vietnam's GDP by economic sector (2020 - 2024)

Sectors / Years	2020	2021	2022	2023	2024
Agriculture, Forestry and Fisheriesfl	0,05	0,05	0,05	0,06	0,06
Industry and Construction	6,08	6,20	5,90	5,81	5,96
Services	6,53	6,62	6,88	7,00	7,15
Total	**12,66**	**12,87**	**12,83**	**12,87**	**13,17**

Source: General Statistics Office (2024).

However, the process of digital transformation and the development of the digital economy also pose numerous challenges to national security - particularly in terms of economic security and cybersecurity. Resolution No. 52-NQ/TW, dated September 27, 2019, issued by the Politburo, explicitly emphasizes the core task of proactively preventing and responding to the negative impacts of the Fourth Industrial Revolution while ensuring national defense, security, social equity, and sustainable development. To achieve these goals, Vietnam has established a legal framework comprising key laws, including the 2015 Law on Cyberinformation Security, the 2018 Law on Protection of State Secrets, the 2018 Cybersecurity Law, and the National Cybersecurity and Safety Strategy to 2025 with a vision to 2030. This strategy identifies cybersecurity and safety as the foundational pillars for building digital trust, thereby laying the groundwork for prosperity and national autonomy in the digital era.

In the digital economy, risks to economic security can be classified into three main groups. The first is systemic risks, which affect the entire economy or key sectors. These

include dependence on imported technologies and hardware components, such as semiconductors, which are essential for implementing digital transformation. A related issue is the undervaluation of the real economy within the digital ecosystem. To mitigate such risks, priority must be given to transitioning from a resource-based economy to a production-based economy and, ultimately, to a digital economy. The second group comprises structural risks, which arise from reorganizing and shifting market structures throughout the digital transformation process. The third group includes sector-specific risks, which arise in the process of digitizing particular sectors within the socio-economic system.

Despite having a relatively comprehensive legal and policy framework, the rapid and profound changes brought about by digital transformation continue to generate new and complex risks to Vietnam's economic security.

The first is systemic risks, including:

(1) Institutional risk. Although Vietnam has made significant efforts to develop its legal infrastructure to support digital transformation, the pace of legal reform has not kept up with real-world developments - particularly in emerging areas such as digital currencies, financial centers, the sharing economy, national data governance, enterprise data, personal data protection, and artificial intelligence (AI). The absence of an appropriate legal framework can create systemic vulnerabilities that endanger the digital economy and the traditional economy.

(2) Financial insecurity. The financial sector is a leader in Vietnam's digital transformation, yet with the rise of digital currencies and digital assets, integration into global digital platforms exposes the country to risks such as transaction fraud, cybercrime, money laundering, and financial scams. Vietnam's financial monitoring and regulatory systems remain largely conventional and are unable to respond effectively to emerging financial risks. Many financial institutions have not yet established robust cybersecurity protocols. Technologies such as data encryption, intrusion detection, and access control are not widely or consistently applied, increasing the risk of exploitation in digital environments.

(3) Job displacement. Vietnam's economy still depends heavily on low-skilled labor. As industries move toward automation and innovative technologies, the replacement of manual labor becomes increasingly likely. This transition could result in significant job losses among traditional workers, heightening social pressure and disrupting macroeconomic stability.

(4) An increase in inequality. Digital transformation tends to amplify existing income and development gaps among regions and demographic groups. Workers with higher education and digital skills adapt more easily to technological changes and benefit from higher productivity and incomes. In contrast, low-skilled workers are at greater risk of exclusion from the labor market. This dynamic exacerbates income inequality. While improving workforce quality is a crucial long-term solution to this issue, the rapid pace of digital transformation leaves little time for gradual adaptation (*see Table 2*).

The following table summarizes the key information regarding the Da Nang Hi-Tech Park, including planning details and investment capital (in VND billion).

This table outlines key systemic risks associated with Vietnam's digital transformation process.

Table 2. Systemic risks in Vietnam's digital transformation

Risk Category	Description
Institutional Risk	Outdated laws for digital areas like AI and data.
Financial Insecurity	Weak cybersecurity and outdated financial oversight.
Job Displacement	Automation threatens low-skilled jobs.
Rising Inequality	Tech benefits skilled workers, leaving others behind.

Sources: Compiled by author (2025).

Table 3. Key cybersecurity statistics (2024)

Indicator	Value	Notes
Organizations experiencing at least one cyberattack	46.15%	Reported within the past year
Organizations frequently targeted by cyberattacks	6.77%	Identified themselves as frequent targets
Total number of cyberattacks (nationwide)	Over 659,000	Estimated in the year 2024
Cyber threat alerts in critical institutions	Over 74,000	Alerts recorded in essential or high-priority sectors
Number of targeted attack campaigns	83 campaigns	Part of the 74,000+ alerts; focused and coordinated threats

Sources: National Cybersecurity Association (2024).

The second is the risks businesses face.

During the digital transformation process, enterprises and organizations face significant challenges related to information security and cybersecurity. Cyberattacks can cause substantial damage to computer systems, databases, and digital infrastructure while leaking sensitive information that severely undermines customer and partner trust. According to statistics, up to 46.15% of organizations and businesses reported having experienced at least one cyberattack in the past year, and 6.77% indicated that they are frequent targets. In 2024 alone, the total number of cyberattacks was estimated to exceed 659,000. Among critical institutions, over 74,000 cyber threat alerts were recorded, including 83 targeted attack campaigns (*See table 3*) (National Cybersecurity Association, 2024).

Cyberattacks or system failures can disrupt production, transactions, and service delivery, resulting in significant economic and data losses. Notably, in 2025, with the rapid

advancement of AI, cyberattacks are becoming more sophisticated. AI is being exploited to carry out social engineering attacks, create deepfakes, and spread malware capable of identity theft and bypassing traditional security layers. In this context, businesses are compelled to make substantial investments in security systems to prevent and mitigate risks. Additionally, the costs of adapting operational processes, training personnel on new technologies, and deploying comprehensive IT infrastructure pose a significant financial burden. These expenses increase investment and operational costs, affecting competitiveness - especially for small and medium-sized enterprises (SMEs).

The third is the risks individuals face.

For individuals, using the Internet and digital services brings many conveniences but also exposes them to privacy and personal data security risks. Hackers increasingly utilize sophisticated attack methods, including malware, phishing websites, and malware-as-a-service tools, to infiltrate users' devices and steal sensitive data. Particularly concerning is the growing danger of malware designed to steal personal information. These programs can bypass standard security protocols and gain access to login credentials and banking accounts. Individuals who do not enable multi-factor authentication are especially vulnerable. According to the National Cybersecurity Association (2024), online fraud continues to rise, with estimated losses reaching 18.9 trillion VND in 2024 alone. The most common forms of fraud include financial investment scams and the theft of personal data through online platforms, resulting in significant harm to users.

4. Recommendations for safeguarding economic security in the digital economy

In the context of rapid global digital transformation, Vietnam not only faces opportunities to accelerate development but also confronts emerging risks related to economic security. To ensure a stable, safe, and reliable digital economic environment, the following comprehensive groups of solutions should be implemented:

First, there must be a unified and comprehensive understanding of economic security as a strategic interdisciplinary domain encompassing key sectors such as energy, finance and banking, telecommunications, food security, water resources, and digital technology. In the digital economy, vulnerabilities in any one area can lead to widespread disruptions throughout the entire system. Therefore, building a secure digital economic ecosystem must be grounded in safeguarding economic security. The Government should issue clear guidelines on risk assessment criteria and the strategic sensitivity of each sector in the digital environment to establish appropriate protective mechanisms.

Second, it is crucial to develop and implement flexible economic policies tailored to the digital economy's characteristics. Development policies should not only promote economic growth but also integrate requirements for macroeconomic stability and economic security. Policies on digital taxation, electronic identification, digital financial transactions, and cross-border investment controls - particularly in sensitive sectors - must be promptly updated to prevent

external manipulation and influence.

Third, strengthening international cooperation on economic and cyber security is imperative, especially as national borders become increasingly blurred in cyberspace. Vietnam should proactively participate in trade agreements that include provisions on data protection and cross-border data transfers while also establishing bilateral and multilateral cooperation frameworks for intelligence sharing, cyberattack alerts, and coordinated responses to large-scale cyber crises.

Fourth, developing high-quality human resources is a prerequisite for enhancing the resilience of the digital economy against security threats. The State should prioritize investment in education and training in cybersecurity, big data analytics, digital forensics, encryption, and system security engineering. Additionally, mechanisms that link training institutions with businesses should be promoted to ensure a practical and relevant workforce. At the same time, enterprises should be encouraged to implement regular internal training programs on information security for employees at all levels.

Fifth, a comprehensive legal framework on data protection and privacy must be established and enforced, covering both personal and business data. The law should clearly define the responsibilities of organizations involved in storing, processing, and exploiting data and include provisions for routine inspections and supervision. An independent monitoring system should also be developed to assess compliance and impose strict penalties for violations, thereby enhancing deterrence and ensuring accountability.

Sixth, the proactive role of enterprises and the enhancement of social responsibility among citizens must be emphasized. The business community should not only be protected but also serve as an active participant in safeguarding economic security through legal compliance, investments in security technologies, and transparent cooperation with regulatory authorities. Simultaneously, public awareness must be raised through mass media campaigns and community education programs on digital literacy, online fraud prevention, and the safe use of financial services, thereby contributing to creating a secure and sustainable digital society.

5. Conclusion

In the context of the rapid development of the digital economy, economic security has become an essential factor in ensuring every nation's stability and sustainable development. Protecting economic security in the digital environment requires close coordination among state agencies, the business community, and society as a whole. Policies and legal frameworks must be refined promptly to adapt to the evolving digital landscape while also facilitating the advancement of modern security technologies.

In parallel, raising awareness about cybersecurity and building a robust defense system - from the national level to individual organizations and enterprises - is an urgent priority. Only when economic security is comprehensively safeguarded can countries fully harness the potential of the digital

revolution, strengthen their internal capacities, enhance competitiveness, and move toward long-term sustainable development.

References:

1. Besada. (2018). *The digital economy: Global trends and policy implications*. International Journal of Economic Policy, 55(3), 119 - 134.

2. Brynjolfsson, E., & Kahin, B. (2000). *Understanding the digital economy*. MIT Press.

3. Ganichev, V., & Koshovets, O. (2019). *Digital transformation of economic systems*. Economic Journal, 64(2), 45 - 67.

4. National Cybersecurity Association. (2024a). *Annual cybersecurity report 2024 (governmental and corporate sector).* Retrieved from https://nca.org.vn/news/detail/bao-cao-tong-ket-an-ninh-mang-nam-2024-khu-vuc-co-quan-doanh-nghiep?l=vi

5. National Cybersecurity Association. (2024). *Annual cybersecurity report 2024 (individual users sector).* Retrieved from https://nca.org.vn/news/detail/bao-cao-tong-ket-an-ninh-mang-nam-2024-khu-vuc-nguoi-dung-ca-nhan?l=vi

6. Kling, R., & Lamb, R. (2000). *IT and organizational change in digital economies. In E.* Brynjolfsson & B. Kahin (Eds.), Understanding the digital economy (pp. 295-324). MIT Press.

7. Lane, N. (1999). *Advancing the digital economy into the 21st century.* Information Systems Frontiers, 1(3), 317 - 320.

8. Mambetomorov, K., & Almasbekova, A. (2021). *The shift towards a virtual economic space: Implications for national markets.* Economic Studies, 89(3), 201 - 220.

9. Margherio, L., Henry, D., Cooke, S., & Montgomery, A. (1999). *The emerging digital economy.* Discover U.S. Government Information.

10. Tapscott, D. (1995). *The digital economy: Promise and peril in the age of networked intelligence.* McGraw-Hill.

11. Tohirov, M. (2013). *Management of economic security of the region. State and Municipal Management, 4, 189 - 194. Cited in M.A. Nikolaev, M.Yu. Makhotaeva, Risks and threats to the economic security of a region in the digital economy.* Proceedings of the International Scientific and Practical Conference "Russia 2020 - a new reality: economy and society" (ISPCR 2020).

12. Verhoef, P. C., Broekhuizen, T., Bart, Y., Bhattacharya, A., Dong, J. Q., Fabian, N., & Haenlein, M. (2021). *Digital transformation: A multidisciplinary reflection and research agenda.* Journal of Business Research, 122, 889 - 901.

Further reading:

1. A, D. (2024). *Digital transformation and new requirements for network safety and security.* Retrieved from https://nhandan.vn/chuyen-doi-so-va-yeu-cau-moi-ve-an-toan-an-ninh-mang-post829697.html

2. General Statistics Office. (2024). *Press release on the results of compiling the index of the proportion of added value of the digital economy in GDP and GRDP for the period 2020 - 2024.* Retrieved from https://www.nso.gov.vn/du-lieu-va-so-lieu-thong-ke/2025/01/thong-cao-bao-chi-ket-qua-bien-soan-chi-tieu-ty-trong-gia-tri-tang-them-cua-kinh-te-so-trong-gdp-grdp-giai-doan-2020-2024/

3. Ha, N. T. T. (2023). *Identifying economic security in digital transformation in Vietnam.* Retrieved from https://www.quanlynhanuoc.vn/2023/10/26/nhan-dien-an-ninh-kinh-te-trong-chuyen-doi-so-tai-viet-nam/

4. Ha, P. T. T. (2024). *Digital transformation in the financial sector in Vietnam: current situation and some solutions.* Retrieved from https://kinhtevadubao.vn/chuyen-doi-so-trong-nganh-tai-chinh-o-viet-nam-thuc-trang-va-mot-so-giai-phap-30448.html

5. Huyen, N. (2024). *Losses due to online fraud in Vietnam in 2024 reach nearly 19,000 billion VND.* Retrieved from https://en.vneconomy.vn/thiet-hai-do-lua-dao-truc-tuyen-nam-2024-tai-viet-nam-len-toi-gan-19-000-ty-dong.htm

6. Linh, P. T. M. (2025). *Current situation of digital economic development in Vietnam.* Retrieved from https://kinhtevadubao.vn/thuc-trang-phat-trien-kinh-te-so-tai-viet-nam-31341.html

7. Thang, L. T. (2023). *The impact of digital transformation on economic security in Vietnam.* Retrieved from https://www.quanlynhanuoc.vn/2023/10/26/tac-dong-cua-chuyen-doi-so-den-an-ninh-kinh-te-o-viet-nam/