International Journal Of Humanities Education And Social Sciences ***(IJHESS)*** *E-ISSN:* **2808-1765**
Volume 2, Number 6, June 2023, *Page. 1917 - 1924*
Email : editorijhess@gmail.com

Challenges and Cybersecurity Threats in Digital Economic Transformation

Desta Lesmana[1)], Mochammmad Afifuddin [2)], Agus Adriyanto [3)]
[1,2,3)] Universitas Pertahanan Republik Indonesia

*Coresponding Author
Email: lesmanadesta@gmail.com

Abstract

The integration of digital technology in economic transformation can introduce new risks and threats caused by the emergence of new technologies and features in the digital economy. It is crucial for governments, as implementers and overseers of the economy, to identify potential risks and threats in order to ensure the security of the national economy during the digital economic transformation. The efficiency of the measures developed and implemented to minimize risks and eliminate threats to national economic security depends on the quality and precision of the policies implemented. A comprehensive approach to analyzing the risks and threats posed by cyber threats in the digital economy is necessary and should cover all economic processes, particularly the relationships among the actors involved in the economic process.

Keywords: Cyber Threats, Digital Transformation, Digital Economic.

INTRODUCTION

The development of technology has provided significant innovations in supporting human life activities, including in the economic aspect. Technology has facilitated and accelerated many business processes, as well as opened up new opportunities to create better and more efficient products and services. The rapid and innovative development of technology has brought significant changes in the way humans interact and conduct business. Digital transformation has become a solution to respond to global changes and the increasingly complex needs of customers (Piliang, 2012).

Digital transformation is a fundamental change in the way we use digital technology to conduct business, society, and government activities. This transformation involves the application of digital technology in all aspects of life and business, from data collection to decision-making based on the data generated. The development of digital technology has accelerated digital transformation in various fields such as transportation, commerce, health, and education. For example, the adoption of e-commerce platforms enables online buying and selling of goods and services, while artificial intelligence technology enables more effective decision-making based on data analysis (Kominfo, 2020).

Digital transformation also involves changes in the way we work and communicate. Many companies now adopt remote or hybrid work models to leverage digital technology and increase productivity. Meanwhile, messaging applications and social media allow people to communicate and interact more efficiently and effectively. Digital transformation has brought significant changes in various aspects of life, including the economic aspect. In the digital era, the economy is no longer limited to physical transactions or dependent on geographical locations, but can be done online and globally (World Economic Forum, 2019).

The economic sector is a sector that is greatly influenced by technological development. The need for technology in the economic sector will continue to follow the times because technology can help improve productivity, efficiency, and innovation in various industries. Internet and mobile technology have revolutionized the trading sector by driving the growth of

e-commerce and mobile commerce. Companies that adopt such technology can reach consumers more widely and simplify payment and delivery processes. In the financial sector, technology has also played a crucial role in developing fintech and digital banking. Digital banking applications facilitate transactions and payments, while blockchain technology can be used to facilitate safer and more efficient transactions. In the manufacturing sector, technology such as robotics and artificial intelligence can improve efficiency and accelerate production. Meanwhile, in the agricultural sector, sensor technology and the Internet of Things (IoT) can help improve efficiency and productivity in agricultural production (OECD, 2020).

One of the greatest innovations resulting from technological development is the digital economy. The digital economy refers to economic activities related to the use of digital technology such as the internet, computers, and mobile devices to conduct business. The digital economy has changed the way we shop, pay, and even communicate. In the digital economy, businesses can reach consumers worldwide via the internet, and customers can buy products and services online. This allows businesses to expand their markets and increase revenue, while enabling customers to buy products and services from anywhere and anytime (Westerman, Bonnet, & McAfee, 2014).

Indonesia is one of the countries in Southeast Asia with great potential in developing the digital economy. Based on data from the Association of Internet Service Providers in Indonesia (APJII) in 2021, the number of internet users in Indonesia reached 196.7 million people or about 72% of the total population. This makes Indonesia one of the countries with the largest number of internet users in the world (Kominfo, 2020).

The development of the digital economy in Indonesia has been seen through the emergence of many digital platforms such as e-commerce, travel booking, and fintech. Some popular e-commerce platforms in Indonesia include Tokopedia, Shopee, and Bukalapak. These platforms enable small and medium-sized enterprises (SMEs) to market their products online and expand their markets (Sianturi, 2017).

In addition, fintech has also been rapidly developing in Indonesia with platforms such as OVO, GoPay, and Dana providing digital payment solutions and online loans. This fintech development has made it easier for people to conduct transactions without having to carry cash, and has opened up opportunities for SMEs to access business capital (KPMG, 2019).

The Indonesian government has also taken steps to support digital economic transformation in Indonesia. In 2016, the government launched the "Making Indonesia 4.0" program aimed at promoting digitalization in the manufacturing and industrial sectors in Indonesia. In addition, in 2020, the government launched the "Roadmap for Indonesia's Digital Economy 2020-2024" which sets out strategies and targets to accelerate digital economic transformation in Indonesia.

Digital economic transformation has become an ongoing trend in various countries, including Indonesia. One important factor enabling the development of the digital economy is the existence of cyberspace or virtual space that can be utilized by business actors to interact and conduct business activities.

Cyberspace or cyberspace is a digital space that has characteristics different from physical space, such as not bound by geographic boundaries, accessible globally, and capable of accommodating various forms of interaction and activity. Cyberspace is also considered a form of "virtual reality" that can provide experiences or simulations of the real world. In recent decades, cyberspace has developed and requires coordinated efforts from central governments, government agencies, and relevant organizations/companies to keep it secure. With the increase in internet usage, cyberspace has developed globally where everyone is connected to each other through routers, cables, and international internet networks. In short, many people and companies have used cyberspace to develop their industries globally. In today's world,

most people use the internet to work and it has created a social space that is connected to our daily lives. Everyone uses the internet in their daily lives, while subnational groups and government organizations use cyberspace for national development in various ways. On the other hand, terrorist groups use cyberspace to recruit and train their groups. These terrorist groups use cyberspace to attack their target organizations or a country by threatening the infrastructure owned by that country (Harmon & Castro-Leon, 2015).

In the context of digital economic transformation, cyberspace plays a critical role in building an effective and efficient digital business ecosystem. Within cyberspace, business actors can offer their products and services online, connect with customers from different regions, and expand their market reach.

One example of utilizing cyberspace in digital economic transformation is in e-commerce. E-commerce businesses use cyberspace to facilitate online transactions between sellers and buyers. Customers can easily and quickly purchase products online without having to visit physical stores. Meanwhile, sellers can promote their products online, expand their market reach, and obtain customer data that can be used to develop their businesses. Moreover, cyberspace is also crucial in building fintech businesses. Fintech businesses leverage digital technology to provide financial services such as digital payments, online loans, and investments. In cyberspace, fintech businesses can offer easily accessible financial services to the public without requiring physical infrastructure like offices or ATM machines (Kshetri, 2018).

However, like any form of economy, the digital economy also faces challenges and risks. One of the major challenges is the digital divide between developed and developing countries. Developed countries have better access to digital technology and the internet than developing countries, which can hinder the growth of the digital economy in those countries. Additionally, data privacy and security are also crucial issues in the digital economy. With the increasing use of digital technology, more personal data is generated and collected, which can increase the risk of identity theft, cybercrime, and privacy breaches. Therefore, it is essential for governments and companies to protect data privacy and enhance digital technology security.

Based on the above explanation, this study is expected to understand the nature of cyber threats and to implement comprehensive strategies to manage and address them, ensuring that Indonesia's digital economy remains secure and resilient.

RESEARCH METHODS

This research is written using a qualitative method with a descriptive analysis approach. In this research, secondary data obtained through a literature review of books, journals, and other relevant secondary data related to the research problem were used. Furthermore, the data was processed and analyzed so that it could be presented in the form of narrative text.

RESULT AND DISCUSSION

The development of information technology, particularly internet communication, has caused rapid social, economic, and cultural changes. To address cybercrime, the government has issued laws to effectively and quickly store, process, generate, and disseminate information to the public. This technology is believed to be the main alternative for implementing social,

economic, and governance activities. However, current information technology has become a "double-edged sword," which can contribute to improving welfare, progress, and human development, as well as serve as an effective means for committing crimes.

Cybercrime, also known as computer crime, refers to criminal activities that target or use computer systems, computer networks, or network devices. Most cybercrimes are committed by cybercriminals or hackers who seek financial gain, although some may also have other motivations such as destroying or damaging electronic systems in wireless networks. Cybercrime can be committed by individuals or organizations, with some cybercriminals utilizing highly sophisticated techniques. However, there are also beginner hackers who engage in cybercrime. In rare cases, cybercrimes are committed for reasons other than financial gain, such as political or personal motives (Hatta, 2020).

Cybercrime that disrupts users from using machines or networks, or prevents businesses from providing software services to their customers, is called a Denial-of-Service (DoS) attack. Cybercrime that uses computers to commit other crimes may involve the use of computers or networks to spread malware, illegal information, or illegal images. Sometimes cybercriminals engage in both categories of cybercrime simultaneously. They may first target computers with viruses, and then use them to spread malware to other machines or throughout a network. Cybercriminals may also engage in what is known as a Distributed-Denial-of-Service (DDoS) attack. This is similar to a DoS attack, but cybercriminals use many compromised computers to carry it out (National Crime Agency, 2020).

The world of cybercrime is evolving rapidly, with new trends constantly emerging. Cybercriminals are becoming more agile, exploiting new technology at lightning speed, adapting their attacks using new methods, and collaborating with each other in ways we have not seen before. In other words, cybercrime will continue to evolve in line with the development of technology that is present and used by society. As a result, the threat of cybercrime will only increase over time (Interpol, 2020).

The Indonesian government has taken steps to reduce and prevent cybercrime by issuing Law Number 19 of 2016, which amends Law Number 11 of 2008 concerning Electronic Information and Transactions (commonly known as the ITE Law). The purpose of this law is to promote the safe use of the internet and prevent its misuse. However, this law alone may not be sufficient to address all cyber threats, which necessitates additional government efforts and policies related to cyber defense.

As the economy undergoes digital transformation, there is a shift towards an electronic-based system for goods and services, facilitated by information and communication technology (ICT) such as internet technology. This digital economy is integrated with the global economic and social network. However, it also presents security risks that can threaten national defense through security gaps in its digital network.

Cyber threats that affect the digital economic transformation can be considered a threat to the nation-state because they can have a significant impact on the country and its people. Cyber threats for a country can be identified as Malware and Zero-Day Attack (Teoh & Mahmood, 2017). The global proliferation of harmful software or malware has increased the threats and risks in the cyber world. Malware has also started to infect mobile devices, with more than 8 million malware samples in 2015. Currently, malware is designed to be sophisticated and efficient (Symantec, 2016). The number of malwares continues to increase, with reported malware reaching the threshold of 2 billion in January 2016 (Symantec, 2016). Malware is a convenient and efficient tool to execute cyber-attacks. The demand for malware remains high as the motivation for cyber-attacks shift from curiosity and seeking fame to dark financial gains (Czech Republic, 2015).

Organized cybercrime has increasingly utilized the internet as a means and location for their crimes. Organized cybercrime can pose a serious threat, as it can cause greater damage or losses to a country. For example, in the UK, internet banking fraud increased to 133.5 million pounds in 2015, and companies lost up to 37 billion euros per year. In 2016, the Banswift Group launched a cyber-attack in Bangladesh, stealing USD 81 million from the country's central bank. In other words, organized cybercrime is a criminal group that can cause harm to a country and thus can be positioned as a serious threat to Indonesia's digital economic transformation (Choo, 2011).

State-sponsored or state-directed cyber-attacks are a form of offensive action aimed at weakening, controlling, and damaging the target of the attack. Such attacks are typically aimed at critical national infrastructure such as government, defense, finance, energy, and telecommunications sectors. The connectivity of national critical infrastructure strengthens the cascading effect and the impact of damage to the country's infrastructure, as the damage will affect the entire population that uses or accesses these infrastructure services. State-sponsored cyber-attacks pose a serious threat to the digital economic transformation of Indonesia (Teoh & Mahmood, 2017).

Data and Information Theft, information is the driving force of the digital economy in maximizing its function to develop a sustainable economic system. The flow of information in the implementation of the digital economy is a target that can be attacked by hackers to be exploited or traded. Vulnerability to personal information security is a major problem in implementing the digital economic transformation as it concerns the security of personal data in carrying out economic activities (McAfee, 2014).

The risk and threat of information can arise from dependence on complex information systems, including hidden factors such as information overload, human factors, system interdependence, and information failure. With the introduction of digital technology, they are also associated with failures, errors, misuse, and other problems inadvertently caused by consumers, users, technology breakdown, or employees.

The main source of information risk is information assets, which encompass all information and data in digital form (digital models of business processes, digital services, digital content, digital databases, web resources, software, digital data from various sensors, electronic media data, information processed in information systems, and transmitted through data transmission channels). The main manifestations of information risk are breaches of the integrity, reliability, and availability of information assets (resources). These manifestations can be associated with the reliability of information system hardware components and the likelihood of their failure, software failures, and non-compliance with the requirements of various standards in the operation of information systems and digital services, the inability and erroneous actions of personnel (internal environment, contractors, and suppliers of information systems and resources (external environment), the possibility of undocumented opportunities in the system, imperfections in the organizational structure of information systems, and non-compliance with standard requirements at the design, production, and operation stages of the system.

Based on their nature, information risks and threats can be divided into organizational and technical risks, hardware and software risks. Organizational risks are caused by inadequate efficiency of the developed rules that regulate the activities of personnel operating and servicing information systems, as well as by problems with internal control systems. Technical risks are related to the equipment and software environment of information systems or digital resources and their operation, directly related to the life cycle of information systems and, in turn, divided into hardware risks, related to the failure of information system components, such as servers, personal computers, network switches and routers, production equipment, machine equipment,

etc.; software risks, directly related to the failure and errors of the system in functioning software; and project risks, system errors in setting objectives and goals for designing information systems, formulating requirements for the functions and characteristics of digital process or object solutions, determining the conditions and parameters of the external environment in which the information system will be used; algorithmic design errors in direct algorithmic functions of software and database, determining the structure and interaction of complex software components, and when using information from the database; programming errors in program text and data description, as well as in the sources and documentation produced for information system components; software risks, directly related to the failure and errors of the system in functioning software (Derbin & Klimov, 2013).

The risk of external information is not dependent on the internal environment of the company and is not directly related to its activities. It is difficult for companies to influence them, as they are conditioned by the political and socio-economic situation in the country. Internal information risks are directly related to the company's activities and personnel and depend on factors such as production and human resources, the level of technical equipment and technology, and the development of information infrastructure and security organizations. The vulnerability risk to digital information security systems can cause direct or indirect losses to the digital economic transformation. Risk and threats to information security systems differ from information threats and risks. Information risks are the result of intentional impacts on information, data in digital form, information resource functions, and systems in digital space. The mechanism of the impact of information security risks in digital economic transformation is the largest classification group of information threats and risks, including (Kuznetsova, 2022): Loss of information sources; Loss of access to information sources, consumer data and economic actors, and information availability in general; Theft of information and data in digital format; Intentional distortion of information; Hardware and software failure in information systems (Kuznetsova, 2022).

Low information security will increase the threat of unauthorized or illegal access and alteration of data. Such situations include risks and threats related to leaks or misuse that may create opportunities to exploit the vulnerabilities of the information system for certain parties' interests. At the same time, protected leak sources are carriers of secret information that attackers have successfully accessed. This situation can create the possibility of theft and forgery of digital data in the digital economic information system. Theft and forgery can directly cause damage to the country because of illegal or criminal activities such as fraud through data forgery (Kirishchieva, Skorev, Mishchenko, & Grafova, 2021). To address security threats in Indonesia's digital economic transformation, several measures need to be taken, including: Enhancing data security, Companies must ensure that user data is securely protected. This can be accomplished by encrypting data, regularly backing up data, and limiting data access to authorized personnel. Continuous monitoring, Companies must continuously monitor their systems for cyber-attacks or other suspicious activity. Advanced security technologies such as network security systems and intrusion detection can aid in identifying and preventing cyber-attacks. Raising awareness of cyber security, Companies must train their employees to be more aware of cyber security threats. This can be accomplished by providing training on actions to prevent security breaches and by frequently reminding employees of best practices for data security.

The Indonesian government has taken several measures to address security threats in Indonesia's digital economic transformation. Some of these efforts are:

1. Providing digital security infrastructure
   The government has increased investment in digital security infrastructure to protect Indonesia's digital systems from cyberattacks. One example is the development of

the National Security Operation Center (SOC), which functions to detect, analyze, and respond to cyberattacks across Indonesia.

2. Regulations and policies related to cybersecurity
   The government has issued several regulations and policies related to cybersecurity, such as the ITE Law and Presidential Regulation No. 53 of 2017 on Cybersecurity. These policies provide a clear legal framework and strengthen cybersecurity protection in Indonesia.
3. Encouraging interagency cooperation
   The Indonesian government has encouraged interagency cooperation in strengthening cybersecurity, such as cooperation between the Ministry of Communication and Information Technology and law enforcement agencies to combat cybercrime.
4. Training and human resource development
   The government has provided support for training and development of human resources in cybersecurity. This includes training and certification for cybersecurity experts and the development of educational curricula in information technology and cybersecurity.
5. Encouraging collaboration between government and the private sector
   The government has encouraged collaboration between the government and the private sector in strengthening cybersecurity. This includes government programs to encourage companies to increase investment in cybersecurity and cooperation between the government and industry to address potential cyber threats that could harm Indonesia's digital economy.

These government efforts provide hope for digital security in Indonesia, but there is still much work to be done to address the rapidly evolving cybersecurity threats. The role of the government, society, and industry in increasing awareness and cybersecurity protection will be key in ensuring Indonesia's digital economy remains safe and prosperous.

CONCLUSION

The introduction of digital technology in the implementation of digital transformation can bring new risks and threats caused by new technology and features in the digital economy. As the executor and regulator of the economy, identifying possible risks and threats is one of the most important tasks for the government in ensuring the security of the economy in the implementation of digital economic transformation. The efficiency of the measures developed and implemented to minimize risks and eliminate threats to national economic security depends on the quality and accuracy of the policies implemented. The risk and threat analysis approach of companies in the digital economy should be comprehensive and cover all aspects of the economy, particularly the relationships between the actors involved in the economic process.

REFERENCES

Choo, K.-K. (2011). The cyber threat landscape: Challenges and future research direction. *Computer & Security*, 719-731.

Czech Republic. (2015). *National Cyber Security Strategy of the Czech Republic (2015-2020).* Czechia: Czech Republic.

Derbin, E. A., & Klimov, S. M. (2013). *Organizational basis for ensuring the information security of an enterprise.* Moscow: Financial University.

Harmon, R. R., & Castro-Leon, E. (2015). Smart cities and the Internet of Things. *PICMET Annual Conference Proceedings.* Portland: Portland International Center for Management of Engineering and Technology.

Hatta, M. (2020). Efforts to Overcome Cyber Crime Actions in Indonesia. *International Journal of Psychosocial Rehabilitation*, Vol. 24, Issue 03.

Interpol. (2020). *Cyberattacks know no borders and evolve at a rapid pace*. Retrieved Maret 20, 2022, from interpol: https://investor.id/market-and-corporate/291115/dikabarkan-akan-rights-issue-dan-ekspansi-tambang-saham-harapan-duta-hope-bakal-dikerek-ke-rp-2000

Kirishchieva, I., Skorev, M., Mishchenko, O., & Grafova, T. (2021). Risks and threats to economic security in the digital economy. *ICEMT* , 110.

Kominfo. (2020). *Infografis Statistik Transformasi Digital Indonesia 2020.* Jakarta: Infografis Statistik Transformasi Digital Indonesia 2020.

KPMG. (2019). *The Pulse of Fintech: Indonesia.* Jakarta: KPMG.

Kshetri, N. (2018). Blockchain's roles in meeting key supply chain management objectives. *International Journal of Information Management*, 80-89.

Kuznetsova, M. A. (2022, Maret 22). *ndustry 4.0 Risks and Their Impact on Industrial Organizations - Economy: Problems, Solutions and Prospects*. Retrieved from Cyberleninka: https: // cyberleninka / article / n / riski-industrii-4-0-i-ih-vliyanie-na-promyshlennye-organizatsii.

McAfee. (2014). *Net losses: Estimating the Global Cost of Cybercrime.* California: McAfee.

National Crime Agency. (2020). *Cyber crime*. Retrieved 20 Maret, 2022, from National Crime Agency: https://www.nationalcrimeagency.gov.uk/what-we-do/crime-threats/cyber-crime

OECD. (2020). *Digital Transformation and COVID-19: Impacts and Policy Responses.* Jakarta: OECD Publishing.

Piliang, Y. A. (2012). Masyarakat Informasi dan Digital: Teknologi Informasi dan Perubahan Sosial. *Jurnal Sosioteknologi*, 155.

Sianturi, P. (2017). Peran Ekonomi digital dalam mendorong pertumbuhan ekonomi nasional. *Jurnal Inspirasi*, Vol 8 No. 2. Hal – 52.

Symantec. (2016). *Internet Security Threat Report.* California: Symantec.

Teoh, C. S., & Mahmood, A. K. (2017). National Cyber Security Strategies For Digital Economy. *Journal of Theoretical and Applied Information Technology*, Vol.95. No 23.

Westerman, G., Bonnet, D., & McAfee, A. (2014). *Leading digital: Turning technology into business transformation.* Cambridge: Harvard Business Press.

World Economic Forum. (2019). *Fourth Industrial Revolution: Beacons of Technology and Innovation in Manufacturing.* Cologny: World Economic Forum.