International Journal Of Humanities Education And Social Sciences ***(IJHESS)*** *E-ISSN:* **2808-1765**
Volume 4, Number 1, August 2024, *Page. 140 – 150*
Email : editorijhess@gmail.com

Digital World Threat Preparedness For Digital Transformation Acceleration Policy In Indonesia

Dwi Jati Marta[1)*], IDK Kertra Widana[2)], Adi Subiyanto[3)], Pujo Widodo[4)], Kusuma[5)]
[1,2,3)] Disaster Management Study Program, Faculty of National Security, Indonesia Defense University

*Corresponding Author
Email: dwijati73@gmail.com

Abstract

Digital transformation is a must for Indonesia in facing global dynamics in this digital era. Through the digital transformation acceleration policy, Indonesia seeks to accelerate economic growth, improve the quality of public services, and strengthen national resilience in the digital era. The purpose of this paper underlines the importance of Indonesia's preparedness in facing the threats of the digital world, both in terms of cybersecurity, data privacy violations and other negative impacts. The method used is a qualitative research method with data reviewed through literature studies. The results show that the importance of this preparedness covers various aspects, ranging from cybersecurity infrastructure to community digital literacy to overcome challenges and risks in building a strong digital defense. In addition, there is a need for concrete steps to overcome obstacles and challenges in implementing digital transformation acceleration policies. This includes strengthening technological infrastructure, improving digital literacy, encouraging the involvement of all stakeholders, and ensuring supportive regulations and adequate privacy protection. Throughout the analysis, it is important to understand that digital transformation is not an end goal, but an ongoing journey. By identifying and addressing the challenges and risks that arise, Indonesia can optimally utilize the potential of digital transformation to achieve sustainable development and protect people's security and privacy in this digital era.

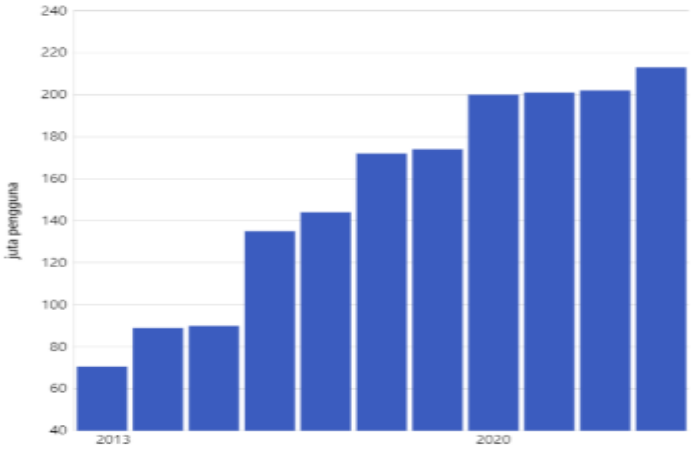
Keywords: Digital Transformation, Digital World, Preparedness, Threats

INTRODUCTION

Amid the rapid pace of digital technology development, Indonesia is embracing a grand ambition to achieve progress through digital transformation policies. This transformation is a key driver to achieve inclusive economic growth, sustainable innovation and improved national competitiveness. By utilizing advances in information and communication technology, Indonesia is entering the era of society 5.0, along with the acceleration of digital transformation in all fields (Ibnu, 2023). This opportunity is taken during the pandemic emergency response, where forcing and changing people's habits can coexist with the digital environment. Therefore, digital transformation is a necessity and no longer an option (Deja, et al., 2021).

The results of the We Are Social report published in the databoks.katadata.co.id article, the number of Indonesians using the internet has increased by 5.44% compared to the previous year, reaching 213 million people in January 2023, or 77% of Indonesia's total population, which previously amounted to 276.4 million. By January 2022, the number of people using the internet had reached 202 million, an increase that has been a steady trend in recent years (Mutia, Cindy, 2023). According to reports, 98.3% of Indonesians who use the internet in Indonesia use mobile phones. On the other hand, Indonesians use the internet for an average of 7 hours and 42 minutes every day. Despite this, a large number of Indonesians are still not connected to the internet, totaling 63.51 million people in 2023. This is the eighth largest number in the world, with 730.02 million people in India.

Figure 1. Number of Internet Users in Indonesia (January 2013-January 2023)

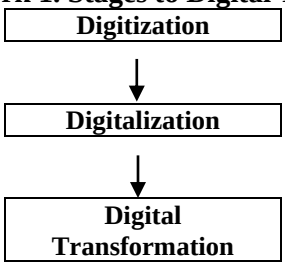


Source: Datadoks.Katadata.co.id (Mutia, Cindy: 2023)

In the era of globalization and advances in information technology, digital transformation is a necessity to ensure the resilience of a country in the midst of the dynamics of the digital world. Indonesia as a developing country with great potential in the utilization of information technology needs to have policies that can accelerate digital transformation. Through policies that target the improvement of digital infrastructure, the quality of human resources and digital governance, it is expected to be able to answer various problems in accelerating digital transformation in Indonesia.

Although the term "digital transformation" was first used in the late 1990s and repeated in the mid-2000s, the terms "digital" and "information technology" have different meanings today. Today, a digital strategy for business effectively drives the company's roadmap and goals, from processes to services and products. The stages of digital transformation are depicted in Framework 1.

Framework 1. Stages to Digital Transformation



Digitization is the activity of converting analog information to digital, converting analog tasks or processes, or using traditional paper into digital formats so that computers can access, store, and move information is called digitization (Verhoef, et al., 2021). Additionally, digitization can be defined as the act of converting information, tasks, or processes from analog to digital form (Bloomberg, 2018).

Digitalization on the other hand is formed and processed for personal, ethical, discourse purposes and the amount of algorithm data that composes it (Andersson et al., 2022). It refers to how information technology or digital technology can change the way existing businesses operate. Therefore, digitalization can occur after the completion of the digitization process.

Digital transformation is defined as a process of change involving the use of digital technologies or the development of new digital business models that create and deliver more value for the company, improve customer experience and improve business outcomes (Verhoef, et al., 2021). Digital transformation is the use of digital to significantly enable new innovation

and creativity in a particular field, rather than just improving and supporting traditional methods (Vezyridis, 2011). Digital transformation is defined as a change process that involves the use of digital technology or the development of new digital business models that create and provide more value to the company, improve customer experience, operational processes and business models that create customer value (Morakanyane., et al, 2017).

According to Nasiri et al. (2020), the digital transformation perspective is considered a tool for transforming inconsistent business processes. Service and manufacturing companies are forced to use digital technologies and adapt their business models by finding new loopholes to synergize the latest technologies with their processes and products (Reis, et al., 2020).

To meet people's expectations of government public services, which provide critical real-time digital services, governments are changing standard operating procedures to improve public services with the aim of increasing transparency and citizen satisfaction. Influenced by both external and internal parties, public sector digital transformation is a comprehensive organizational approach, and does not only include creating online forms or converting public services from analog to digital. External parties require continuous changes to processes, services, and products to meet external needs (Mergel et al., 2019).

The government's policy to accelerate digital transformation to improve the performance of public services requires digital transformation and the readiness of the public to receive digital services in various fields. To make digital transformation a success, the government sector must develop effective data governance. This is because they face several challenges that can arise during the digital transformation process, such as data issues and the adoption of new technologies (Al-Ruithe, 2018). On the other hand, barriers for corporations include fierce business competition between companies (Sayabek et al., 2020).

The Indonesian government in this case has committed to encouraging digital transformation in order to reach all corners of the country. In addition, Presidential Regulation No. 39/2019 on One Data System has begun to be implemented, but behind the uproar, there is one thing that cannot be left out because it has a very important role. Digital transformation will be detrimental if done without considering cybersecurity. In the midst of global technological developments and the era of the Industrial Revolution 4.0, cybersecurity is very important to support the digital transformation process in the country. Moreover, the rapid development of the use of information technology and the internet. On the one hand, it also has a major influence on the increasing threat of cybercrime (Kelana, 2021).

Cyber security must be a concern which has a huge impact and results in the security of information and people. Mistakes occur because of humans, starting from thoughts then channeled through the internet or technology massively affects humans. Currently, in Indonesia everything is digital, so digital transformation is necessary, but it requires qualified cybersecurity. Therefore, cybersecurity is part of digital transformation and a necessity that we must implement together to create digital transformation.

One of the goals of the ongoing digital transformation is to increase national economic growth. Resolving challenges in this transformation, such as cybersecurity and personal data protection, is considered important and needs to be a priority for the government. This accelerated adoption of digital technology will impact the growth of the digital economy in Indonesia. Currently, Indonesia's digital economy is growing significantly as reflected in a study by Google, Temasek, Bain & Company (2022) which states that 40% of the transaction value of the ASEAN digital economy is contributed by Indonesia (Rahma & Harini, 2023).

Digital ecosystem security is an important asset in driving digital economic transformation. Along with technology adoption, data movement is also increasing. The high activity of data movement is reflected in the Global Cybersecurity Outlook report, World Economic Forum

(2022) which states, globally, in 1 minute there are 197 million emails sent, 69 million WhatsApp messages, 500 hours of YouTube content uploaded and US$1.6 million used for online shopping.

With the massive movement of data in circulation, cyber threats also feel more real. According to IDC's Future Enterprise Resiliency and Spending Survey 2022, 65% of companies in the Asia/Pacific region experienced ransomware attacks or incidents that blocked systems and data access. As many as 83% of compromised businesses experienced downtime and business disruption for several days to weeks. The financial loss from such targeted cyber attacks could cost up to US$109,000 for the enterprise segment by 2022. This figure includes reputational damage due to confidential data being leaked or sold to other cyber threat actors.

With this, it seems that the threat from cyber is not playing games as reports related to data leakage cases are also increasingly widespread. According to data from cyber security company Surfshark, Indonesia ranks third, the country with the highest number of data leakage cases in the world. In Indonesia itself, based on the Indonesian Cyber Security Landscape Report (2022) published by BSSN, there are generally five cyber threats faced by Indonesia, namely data leakage, ransomware, phishing, advanced persistent threat and web defacement.

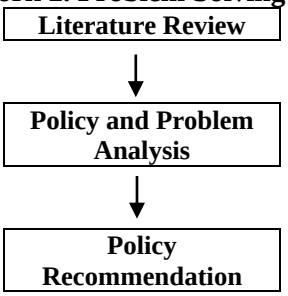
From the background that has been explained, this paper aims to analyze Indonesia's level of preparedness in facing the threats of the digital world, both cyber, data privacy violations, and other potential negative impacts. In this context, various aspects of preparedness will be explored, including cyber security infrastructure, supporting regulatory policies, and public digital literacy. An in-depth analysis of the gaps that may exist will serve as the basis for formulating recommendations and strategies that can improve overall preparedness.

RESEARCH METHODS

The method used in this writing is a research method that uses a qualitative approach, with data studied through literature research. By using a qualitative approach, researchers try to explore the subject's perspective and understand the social and cultural context that influences complex and diverse phenomena from the point of view of the subjects involved in the research. Furthermore, qualitative approaches are commonly used in research related to anthropology, psychology, education, sociology, even social and humanities (Creswell, 2018). This writing uses literature such as books, journal articles, research reports, and other documents (Melfianora, 2019). Literature studies are used to analyze because the author cannot access the subjects involved in the observed phenomenon. For this study, the research methods used included literature review, policy analysis, and policy recommendations (Framework 2).

First, the author reviews the literature regarding Indonesia's level of preparedness in facing the threats of the digital world with the digital transformation acceleration policy. Second, the author assesses how much impact the digital transformation acceleration policy has on development and social welfare in Indonesia. Third, the author finds obstacles and challenges in implementing the digital transformation acceleration policy in order to achieve development and social welfare. And finally, the author identifies obstacles and challenges in the implementation of digital transformation acceleration policies in order to achieve sustainable development and maintain human security in Indonesia.

Framework 2. Problem Solving Method



RESULT AND DISCUSSION

Indonesia's Preparedness for the Threats of the Digital World

Various aspects of people's lives around the world have been transformed by rapid advances in information and communication technology. Digital transformation is no longer just an option, but an urgent necessity to ensure the viability and relevance of various entities in this modern era. Here, the digital transformation acceleration policy has a favorable potential as it enables the acceleration of digital transformation in Indonesia through four policy steps. To start, an equitable and quality telecommunications and informatics infrastructure must be completed. Next, technologies that support the acceleration of digital transformation must be developed.

Third, the implementation of adequate and sustainable human resources (digital talent). Finally, the completion of basic legislation and increased international cooperation. Facing this policy cannot be separated from the potential threats of the digital world. The threat of the modern digital world is a call to reflect deeply on the challenges and opportunities that arise along with the dynamics of these changes.

Today, various sectors such as business, government, education, and healthcare increasingly rely on digital technology to improve efficiency, innovation, and service quality. However, this progress is also inseparable from the increasingly complex risks and threats in the digital world. Data security, privacy, and resilience to cyberattacks are aspects that need serious attention in designing a digital transformation strategy.

Amidst the technological revolution sweeping the world, digital transformation is not just an option, but a necessity for every country to ensure economic growth, efficiency and resilience to global changes. Indonesia, a developing country with a large population and huge economic potential, has chosen digital transformation as one of the key pillars to achieve its long-term development vision. Nonetheless, the journey towards digital transformation is inseparable from the complexity of threats that arise in a dynamic digital world.

In an era dominated by advances in digital technology, Indonesia has identified digital transformation as a key driver to achieve sustainable economic growth and improve national competitiveness. While digital transformation offers many opportunities for progress, it is inevitable that the digital world also brings threats and risks that need attention. Digital world threat preparedness for Indonesia's digital transformation acceleration policy reflects an urgent need with the aim of understanding and addressing the risks that may arise during the digital transformation journey in Indonesia.

In Indonesia, many parties are involved in digital transformation, including the community, private sector and government. The digital transformation acceleration policy is designed to improve digital infrastructure, technological literacy and explore the economic potential that can be generated by digital innovation. Undoubtedly, significant technological advancements, especially during the COVID-19 pandemic, have greatly helped individuals in their daily

activities, such as going to school, working, and buying things. Despite the many conveniences available, we must remain vigilant of the increasing number of crimes that utilize digital technology. This is because irresponsible people can misuse complete personal information.

With its digital economy booming in Southeast Asia, Indonesia must strengthen its preparedness to face the threats of the digital world, or cyber disasters. Given that the world is largely dependent on technology, it is likely that these non-natural disasters will occur (Muraida, 2022). The threat of the digital world is more about digital information security, which also leads to a person's sense of security, known as human security.

The threats in question reported by Silmi Nurul Utami (2023) in Kompas.com are 10 (ten) threats as follows:

a. Malware, a danger that threatens digital data security through malicious software such as viruses, trojans, spyware and ransomware.
b. Hacking, information security threats carried out by individuals to hack passwords so that unauthorized access to systems or networks with the aim of stealing data or spreading malware.
c. Data leakage, a digital data security threat when digital data is leaked intentionally or unintentionally through system or network security errors.
d. Malicious insiders, the next threat can come from unscrupulous insiders, be it contractors, former employees, or business associates who have legal access to data systems. However, this can be used to steal and destroy data or sabotage systems, which is clearly detrimental to digital information security.
e. Data deletion, a threat to the removal of vital or important digital information.
f. Account intrusion, the threat of someone who is not a user using an account to steal data and result in different losses, including financial losses.
g. Phishing, the threat of targeting and contacting people via email, phone or text message by someone claiming to be an official institution and asking for digital information such as banking details, personal identities and different passwords, which are then used for theft of important accounts and financial theft.
h. Privilege elevation is when attackers gain privileges they should not have, which can result in data theft and other losses.
i. Attacks by foreign countries, cyberattacks have been used by some countries to conduct foreign policy. Vital infrastructure, private companies, and government data are their targets. These types of actions can jeopardize international stability and national security.
j. Internet of Things (IoT) attacks, attacks on increasingly used IoT devices can cause serious privacy and security issues.

Here are some of the Indonesian Government's preparedness in increasing digital defense from the threat of the digital world that the author summarizes (Oktaviano, 2023), namely:

a. Strengthening Critical Infrastructure
   In the face of increasing malware and ransomware attacks, the Digital Crimes Unit (DCU) is working proactively to eradicate cybercrime on a global scale. In collaboration with Indonesia's National Cyber and Crypto Agency (BSSN), the Cyber Threat Intelligence Program (CTIP) was implemented. CTIP provides intelligence on cyber threats and helps identify compromised infrastructure quickly.
b. Compliance with Regulations Relating to Personal Data Protection
   On 20 September 2022, Indonesia enacted Law No. 27 of 2022 on Personal Data Protection thereby providing a comprehensive approach to personal data protection and providing clarity to organizations on data ownership rights and obligations. Companies like Microsoft

are committed to maintaining data privacy and supporting organizations in complying with regulations such as the PDP Law.

c. Strengthening Information Security Capacity
Through strengthening information security capacity and preparedness for threats in the digital era, communities can participate in ensuring Indonesia's national resilience. With this step, national resilience can be maintained in the current digital era.

d. Cooperation between Government and Private Sector
Bold measures are taken through cooperation between the public and private sectors. The active involvement of the private sector ensures a quick response to cyber threats and fosters a mutually supportive digital security atmosphere. Regular communication, information exchange, and strategic collaboration are the cornerstones to building a solid cyber defense. Indonesia must continue to adapt and collaborate with stakeholders to effectively face the threats of the digital world. All parties need to work together in building strong cyber resilience and maintaining data security and privacy. Therefore, having a good digital transformation plan, involving stakeholders, considering security, and ensuring that technological changes are well integrated in the business context are important.

e. Development of Local Expertise in Security Technology and Innovation
The Indonesian government recognizes the importance of expertise in cybersecurity, so they established special education and training programs to train professionals. In addition, investment in research and development of cybersecurity technologies encourages innovation to counteract increasingly complex cyberattacks.

f. Increased Education and Awareness
It is important to increase cyber security education and awareness among the general public and workers. Efforts by providing training and awareness campaigns can help reduce threat risks and cyber threat preparedness.

g. Expand International Cooperation
In terms of the context of cooperation between countries, it is very important to deal with cyber security threats that are cross-border in nature with efforts to exchange information and joint resources that can help overcome attacks originating from abroad.

h. Investment in Technology Security
Companies and institutions must continue to invest in security technologies that can detect and prevent attacks. The role of the government in terms of uncomplicated regulations so that companies (startups) do not feel unreasonably burdened.

Artificial Intelligence and Disasters in Digital Transformation

Artificial Intelligence (AI) is usually defined as the ability of a machine or computer to mimic human intelligence in various ways, such as pattern recognition, experiential learning, and making decisions based on data (Arifin, 2023). Although artificial intelligence (AI) is a necessity, it is also a challenge for those of us living in the 21st century. The reason is, although this AI has various benefits for the life of the nation and is a barometer of the progress of human civilization, it cannot be denied that the development of AI can be a serious threat and disaster for human life itself.

Facing various AI challenges such as the use of AI in certain security systems can lead to a significant risk of data hacking.In addition, data collection and analysis for the benefit of certain groups using personal information that should be private and confidential can be easily accessed using this AI. What is even more frightening is the increase in unemployment among the public due to the presence of AI. The reason is, many jobs that are currently done by human labor and thoughts will be replaced by a machine called Artificial Intelligence.

Politically, the use of AI that does not adhere to the principles of truth, honesty and justice will lead to bias and discrimination in the use of unfair data in determining policies that create discrimination, harm other groups and ultimately disrupt the political stability of the country.

As criminals become more sophisticated in their cyber actions, defenses are seeking AI-based resilience. Cyber defenders need to further strengthen their security posture by using AI technology, which can help them improve their capabilities and resources through factors such as:

a. AI-based detection, used to monitor and analyze large volumes of data, can help experts identify anomalies, patterns, and threat indicators faster and gather threat intelligence faster. AI can also help defenses detect unrecognized threats.
b. Artificial intelligence-based response, can be used to automate and supplement their incident response processes.This includes creating alerts, prioritizing actions, conducting tests and validations, and implementing corrective measures. In addition, AI can provide contextual information and recommendations, which help experts deal with incidents faster and more effectively.
c. AI-based protection, can be used to prevent cyberattacks against users and their assets by implementing policies, rules, and controls. AI can also help law enforcement protect users by verifying their behavioral data and preventing data from being leaked or extracted. In addition, AI can always help education to improve the security and resilience of the online ecosystem.

Obstacles and Challenges in Implementing the Digital Transformation Acceleration Policy

The digital transformation acceleration policy in Indonesia is considered to be progressing and has great potential to increase the acceleration of economic growth, especially in the creative economy sector. However, in implementing the policy in the future there will definitely be several obstacles that need to be overcome from various aspects such as:

a. Not yet fully adequate technological infrastructure and stable internet connectivity.
b. Lack of understanding and literacy of digital technology can hinder policy implementation.
c. Lack of active engagement and support from all stakeholders so that the transformation may not reach its full potential.
d. Supportive policies and clear regulations are needed for digital transformation initiatives to run smoothly and influence the implementation of digital transformation.
e. Emerging security and privacy protection issues are becoming serious in the face of cyber threats.
f. Organizational and employee resistance because they have not fully accepted the change well.
g. Organizations are too focused on technology adoption without fully understanding how the technology can support business goals resulting in an imbalance between technology investment and the business value generated.
h. System integration difficulties because they often involve replacing or upgrading existing systems with new systems where the infrastructure will experience operational disruptions and decreased productivity.
i. Technical issues such as hardware or software failure, lack of maintenance which can lead to operational disruption and failure to implement digital solutions.
j. Lack of mature, clear and sustainable planning and strategy can result in uncertainty and implementation failure.

Digital transformation brings many potentials and advantages, but it also has risks and challenges that are considered during the acceleration of digital transformation including:

a. Ethics and Responsibility

In the development and implementation of new technologies, it is important to consider aspects of ethics and responsibility. Steps need to be taken to ensure that the technology is used for good and does not harm society.

b. Appropriate Regulation
Digital transformation requires effective regulation to address risks and ensure safety. It must balance technological innovation with protection against potential man-made disasters.

c. Community Education and Awareness
Community education and awareness about the potential risks and benefits of digital transformation is essential. People need to understand how to use technology wisely to avoid adverse consequences.

d. Expert Shortage
There is a shortage of cybersecurity professionals, with stronger skills needed to deal with threats as software and networks become more complex.

e. Vulnerability of IoT Devices and Devices
Improving the security of IoT devices and devices is crucial as insecure software and hardware can be used as entry points for attackers.

f. Personal Data Protection
Companies and organizations must carefully safeguard their customers' data to avoid violating the law, especially as the EU's GDPR regulations pay more and more attention to personal data protection.

By paying attention to these aspects, it can be expected that digital transformation can have a positive impact on disaster management and reduce the risk of man-made disasters, while keeping in mind the existing challenges and considerations.

CONCLUSION

In an era of globalization that is increasingly connected through digital technology, awareness of the importance of preparedness for the threats of the digital world is crucial. The policy of accelerating digital transformation in Indonesia has a strategic role in facing challenges and taking advantage of opportunities. Thus, let us embrace the future wisely and adapt to inevitable changes. The results show that policies that accelerate digital transformation have great potential to increase the acceleration of economic growth, especially in Indonesia's creative economy. However, challenges such as lacking infrastructure and limited access to technology must be overcome. To boost the growth of the creative economy, this policy enables government, business and society to work together.

In this research, Indonesia's preparedness for the threats of the digital world and the extent to which policies can support the acceleration of digital transformation have been analyzed. From the various aspects evaluated, it can be concluded that Indonesia's preparedness still faces significant challenges, although positive steps have been taken. Digital threats require a holistic and continuous response for Indonesia to reap the full benefits of digital transformation.

Indonesia's overall preparedness for digital threats needs to be strengthened in terms of policy, technology and human capacity. These aspects are interconnected and support each other. The success of accelerating digital transformation is highly dependent on the role of supportive policies, including regulations that promote innovation, data protection and cybersecurity. Cross-sector cooperation and community involvement are needed to create a safe and supportive digital ecosystem. In addition, investment also needs to be increased in cybersecurity education and training so that the workforce has the necessary skills.

The central government, which is responsible for setting policy, should study specific elements of preparedness such as analysis of cybersecurity regulations, data protection, or case studies of successful policy implementation. To gain a broader perspective, this preparedness can involve various stakeholders, including the government, private sector and civil society.

There is a need to build predictive models or scenarios to measure the potential impact of digital threats and the effectiveness of policies in dealing with them. In addition, it is hoped that there will be an international comparative study by examining and comparing Indonesia's preparedness with other countries experiencing similar digital transformation to evaluate strengths and weaknesses. By making these efforts, it is hoped that greater contributions will be made by future research.

REFERENCES

Al-Ruithe, M., Benkhelifa, E., & Hameed. K. (2018). Key Issues for Embracing the Cloud Computing to Adopt a Digital Transformation: A Study of Saudi Public Sector. *Procedia Computer Science Volume 130*. https://doi.org/10.1016/j.procs.2018.04.14.

Anderson, D., & Kelliher, C. (2020). Enforced Remote Working and the Work-Life Interface During Lockdown. *Gender in Management, Vol. 35 No. 7/8, pp. 677-683*. https://doi.org/10.1108/GM-07-2020-0224

Arifin, Bustomi. (2023). Artificial Intelligence (AI): Menghadapi Tantangan dan Membuka Peluang Baru Dalam Era Digital. Accessed on February 7, 2024. https://retizen.republika.co.id/posts/231580/artificial-intelligence-ai-menghadapi-tantangan-dan-membuka-peluang-baru-dalam-era-digital.

Bloomberg, J. (2018). *Digitization, Digitalization, And Digital Transformation: Confuse Them at Your Peril*. Accessed on February 6, 2024. https://www.forbes.com/sites/jasonbloomberg/2018/04/29/digitization-digitalization-and-digital-transformation-confuse-them-at-your-peril.

Creswell, J. W., & Creswell, J. D. (2018). *Research Design: Qualitative, Quantitative, And Mixed Methods Approaches*. Los Angeles, California: Sage Publications.

Deja, M., Rak, D., & Bell, B. (2021). Digital Transformation Readiness: Perspectives on Academia and Library Outcomes in Information Literacy, *The Journal of Academic Librarianship, Volume 47, Issue 5, 102403, ISSN 0099-1333*, https://doi.org/10.1016/j.acalib.2021.102403.

Fauzan Akbar, Ibnu. (2023). *Keamanan Cyber di Indonesia: Membangun Pertahanan Digital di Era Masyarakat 5.0*. Accessed on February 7, 2024. https://www.kompasiana.com/ibnu1030/658060c312d50f6ea21f9d22/keamanan-cyber-di-indonesia-membangun-pertahanan-digital-di-era-masyarakat-5-0.

Indonesia News Center. (2023). *Mengamankan Dunia Digital Kita Bersa dengan Dukungan AI*. Accessed on February 7, 2024. https://news.microsoft.com/id-id/2023/10/18/mengamankan-dunia-digital-kita-bersama-dengan-dukungan-ai/.

Kelana, Irwan. (2021). *Keamanan Siber Makin Penting pada Era Transformasi Digital*. Accessed on August 2, 2024. https://tekno.republika.co.id/berita/r4jmmm374/keamanan-siber-makin-penting-pada-era-transformasi-digital.

Mardiyansyah, Khafid. (2023). *Ancaman Dunia Digital Untuk Indonesia Dari Kehajatan Siber Hingga Persaingan Geopolitik*. Accessed on February 5, 2024. https://nasional.okezone.com/read/2023/11/14/337/2920450/ancaman-dunia-digital-untuk-indonesia-dari-kejahatan-siber-hingga-persaingan-geopolitik.

Melfianora. (2019). *Penulisan Karya Tulis Ilmiah Dengan Studi Literatur*. Accessed on February 8, 2024. http:// banjirembun.blogspot.co.id/2012/04/penelitian-kepustakaan.html.

Mergel, I ., Edelmann, N., & Haug, N. (2019). Defining Digital Transformation: Results From Expert Interviews. *Government Information Quarterly*. 36. 101385. http://dx.doi.org/10.1016/j.giq.2019.06.002.

Morakanyane, R., Audrey, G., & Phillip, O. (2017). Conceptualizing Digital Transformation in Business Organizations: A Systematic Review of Literature. http://dx.doi.org/10.18690/978-961-286-043-1.30.

Muraida, Binti. (2022). *Siap-siap! Indonesia Bakal Dihantam Bencana Siber di Era Digitalisasi*. Accessed on February 7, 2024. https://www.idxchannel.com/economics/siap-siap-indonesia-bakal-dihantam-bencana-siber-di-era-digitalisasi.

Mutia Annur, Cindi. (2023). *Pengguna Internet di Indonesia Tembus 213 Juta Orang Hingga Awal 2023*. Accessed on February 6, 2024. https://databoks.katadata.co.id/datapublish/2023/09/20/pengguna-internet-di-indonesia-tembus-213-juta-orang-hingga-awal-2023.

Nasiri, M., Ukko, J., Saunila, M., & Rantala, T. (2020). Managing The Digital Supply Chain: The Role of Smart Technologies. *Journal Technovation*. http://dx.doi.org/10.1016/j.technovation.2020.102121.

Octaviano. Ricky. (2023). *Transformasi Ekonomi Digital di Indonesia: Peluang dan Tantangan*. Accessed on February 8, 2024. https://www.kompasiana.com/ricky52295/652aa651ee794a0f5a120d02/transformasi-ekonomi-digital-di-indonesia-peluang-dan-tantangan.

Rahma, N.N., & Harini, F. (2023). *Keamanan Siber Jadi Tantangan Transformasi Digital*. Accessed on August 2, 2024. https://validnews.id/ekonomi/keamanan-siber-jadi-tantangan-transformasi-digital.

Reis, João & Amorim, Marlene & Melao, Nuno & Cohen, Yuval & Rodrigues, Mário. (2020). Digitalization: A Literature Review and Research Agenda. http://dx.doi.org/10.1007/978-3-030-43616-2_47.

Santoso Puji, Setyo. (2021). *Ancaman Dunia Digital dan Pentingnya Menjaga Informasi Pribadi*. Accessed on February 7, 2024. https://teknologi.bisnis.com/read/20211012/84/1453403/ancaman-dunia-digital-dan-pentingnya-menjaga-informasi-pribadi.

Sayabek, Z., Suieubayeva, S., & Utegenova, A. (2020). Digital Transformation in Business. http://dx.doi.org/10.1007/978-3-030-27015-5_49.

Setu, Ferdinandus. (2020). *Mendorong Akselerasi Transformasi Digital: Siaran Pers No. 86/HM/Kominfo/07/2020*. Accessed on February 7, 2024. https://www.kominfo.go.id/content/detail/27979/mendorong-akselerasi-transformasi-digital/0/siaran_pers.

Utami Nurul, Silmi. (2023). *8 Macam Ancaman pada Keamanan Informasi Digital*. Accessed on February 7, 2024. https://www.kompas.com/skola/read/2023/01/28/150000069/8-macam-ancaman-pada-keamanan-informasi-digital.

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, Volume 122, Pages 889-901*, ISSN 0148-2963, https://doi.org/10.1016/j.jbusres.2019.09.022.

Vezyridis, P., Timmons, S., & Wharrad, H. (2011). Going Paperless at The Emergency Department: A Socio_Technical Study of An Information System for Patient Tracking. *International Journal of Medical Informatics, Vol. 8(7, Pages 455-465, ISSN 1386-5056*. https://doi.org/10.1016/j.ijmedinf.2011.04.001.