IAIC Transactions on Sustainable Digital Innovation (ITSDI)
Vol. 4 No. 2 April 2023

p-ISSN: 2686-6285
e-ISSN: 2715-0461

Southeast Asia's Cyber Security Strategy: Multilateralism or Self-help

Anggy Giri Prawiyogi[1], Alwiyah[2]

Faculty of Teacher Training and Education, University of Buana Perjuangan Karawang[1]
Faculty of Economics and Business, Wiraraja University[2]

Jl. HS.Ronggo Waluyo, Puseurjaya, Telukjambe Timur, Karawang, Jawa Barat 4136[1]
Jl. Raya Sumenep-Pamekasan KM. 05 Patean, Panitian Utara, Patean, Batuan, Kabupaten Sumenep, Jawa Timur 6945[2]
Indonesia
e-mail: anggy.prawiyogi@ubpkarawang.ac.id[1], alwiyahmahdaliy@yahoo.com[2]

Author Notification
08 March 2023
Final Revised
12 March 2023
Published
13 March 2023

Prawiyogi, A. G., Alwiyah, A., (2023). Southeast Asia's Cyber Security Strategy: Multilateralism or Self-help. IAIC Transactions on Sustainable Digital Innovation (ITSDI),4(2), 119–127. https://doi.org/10.34306/itsdi.v4i2.581

Abstract

In terms of security research, cyber security is fundamentally a recent problem. When all facets of political, military, economic, social, and cultural life are connected to cyberspace, this problem occurs. Cyberterrorism, cybercrime, and cyberwar are all potential concerns in cyberspace. This threat cannot be separated from Southeast Asia, one of the main regions in the globe with a strong rate of economic expansion. This study aims to analyze the best approach for preserving cyber security in Southeast Asia. Neoliberalism and neorealism are common to mainstream methodologies scholars utilize to address the study subject. Simply put, ASEAN nations must advance their technology capacities while not underestimating the value of international cooperation.

Keywords: Security Studies, Southeast Asia, Neorealist, Neoliberal, Cyber Security

1. Introduction

Talking about security studies, this study in International Relations is very interesting. In his book Security: A New Framework of Analysis, Barry Buzan explains that during the Cold War, security studies only focused on the security sector in the political and military fields. However, in its development, the security sector has expanded with the inclusion of environmental, economic and social issues[1]. In an era that is increasingly digitized as it is today, the sector of security studies is also affected. The security sector is not only five but six sectors. Nye added in his book The Future of Power cyber (cyber) needs to get priority in security studies. He explained that the dimensions of the life of the nation-state, including the social order regulated within it, cannot be separated from the role of cyberspace. So like it or not, nation-states need to include it as a strategic priority for the country [2].

The definition of cyber security has a more stable definition. Just like the definition of security explained by Buzan, there is no definite explanation regarding what "security" is. Apart from all that, some literature attempts to explain cyber security. Roxana Radu explained that cyber security is a set of policies, tools, instruments, and risk management in preventing threats from cyberspace. Meanwhile, Madeline Carr explained in her journal, Crossed Wires: International Cooperation on Cyber Security, that cyber security is a post-state issue [3]. This means that cyber security is a threat that cannot be handled using the Westphalian paradigm, namely overcoming threats through state instruments such as the military. Carr emphasized

that threats coming from cyberspace are borderless and invisible, but their impact is very much felt [4].

What is the position of cyber security in the context of relations between countries? Nir Kshetri, in his article entitled Cyber Security and International Relations: The US Engagement with China and Russia, said that national security is not only on land, sea, air and military but also in cyberspace [5]. Furthermore, Kshetri said that bilateral relations between countries are currently very much affected by the activities carried out by these actors in cyberspace. One example is a form of cyber espionage or data theft and attempts to paralyze state information systems by other countries to gain political or economic advantage [6]. As previously explained by Nye, every dimension of life regulated and managed by the state has been digitized. Thus, threats coming from state actors in cyberspace can easily happen.

The typology of threats to cyber security can vary. Myriam Dunn Cavelty describes these threats into three typologies. Examples of this typology are cyber crime, cyber war and cyber terrorism. Cybercrime is a criminal activity that uses information technology to achieve economic interests carried out by criminal organizations. Meanwhile, cyber war is a digital version of Von Clausewitz's war [7], [8].

Meanwhile, cyber terrorism is the activity of hacking or disabling the nation-state information system carried out by terrorist groups. On the one hand, Jonathan D. Aronson provides three different typologies: intelligence gathering, hacking and cyber war [9]. Aronson described this typology as a threat involving digital espionage, hacking of information systems and the ability of nation-states to paralyze the country's defence system by other state actors [10].

The forms of threats described above can threaten anyone without exception, including countries in the Southeast Asian region [11]. ASEAN already has an ASEAN ICT Masterplan 2020, which aims to secure information systems in welcoming the 2025 ASEAN Economic Community [12]. Security of information systems is carried out using a knowledge-sharing format between ASEAN countries to help each other secure member countries' information system networks [13]. Ultimately, the ASEAN ICT Masterplan 2025 envisions achieving a seamlessly and comprehensively connected and integrated ASEAN that will foster greater competitiveness, inclusivity and a sense of Community. MPAC 2025 will focus on five strategic areas to achieve this vision: Sustainable infrastructure

However, the issue of cyber security in Southeast Asia still needs improvement. It should be emphasized that cyber security has a significant impact on the development of the digital economy in ASEAN [14]. By 2025, the development of the digital economy in ASEAN will reach 102 billion US dollars. This is relevant to what economists have explained: the digital economy's market share in 2018 alone reaped profits of up to 20 billion US dollars. Cyber attacks on information systems in Southeast Asia can at least cause disruption and disturbance to the digital economy in the region. Therefore, ASEAN member countries must recognize this cyber threat [15].

Currently, the mastery of information technology in Southeast Asia is controlled by Singapore. Even though Singapore is an IT hub across Southeast Asia, in reality, it is one of the targets of cyber attacks [16]. Based on data collected by the Tech Collective, Singapore in 2018 suffered losses when 19,000 of its customers' credit card data were leaked and traded on the Internet [17]. Singapore and Vietnam also had to experience a data leak when hackers hacked 410,000 Vietnam Airlines user data. Based on the investigation results, Malaysia also experienced a data leak in which thousands of Jobstreet.com users were stolen by hackers. Referring to the Asia Pacific Risk Center report, losses due to this cyber threat could cause US $ 2.1 trillion in losses in 2019[18].

The problem faced in Southeast Asia is that the information technology capabilities of each member country still need to be evenly distributed. Seeing this phenomenon, Southeast Asia has cyber security vulnerabilities that must be addressed. As previously explained, the mastery of technology is still focused on Singapore [19]. This technological inequality becomes a burden when it is not the country being threatened. What if cyber-attacks hit countries like Laos or Myanmar? Every emerging cyber threat is holistic. This means that the threat affects every country in Southeast Asia. Countries in Southeast Asia certainly need to develop their technological capabilities and build cooperation between countries. The

conditions of countries in ASEAN are faced with two choices. According to the school of neo-realism, especially the concept of defensive realism, all countries are interested in surviving in the global political order [20]. Referring to the basic assumptions of this concept, every country has the right to develop military, economic and technological capabilities not to become a revisionist state but to maintain its survival [21].

Contrary to defensive realism, neo-liberal institutionalism views threats as having to be countered by cooperation between countries, embodied in the form of international institutions/organizations. Robert Keohane clearly explained that mitigating threat risks relies on state self-help and requires coordination and cooperation between countries. However, which strategy is the best? This is the research question in this journal. The formulation of the problem presented in this journal is: what strategies can be used by countries to maintain cyber security in Southeast Asia? Is it the defensive-realism model of neo-realism or the multilateral cooperation version of liberal institutionalism?

The theory used in this research is neo-realism and neo-liberalism. Of the two major theories, researchers use the concepts of defensive realism and multilateralism. To answer the research question posed, the two theories above have different basic assumptions in viewing threats in security studies [22]. Theoretically, neo-realism is a derivative of realism which developed in the 1970s. Neo-realism appears through its main character, Kenneth Waltz, who rejects the realism assumption of Morgenthau's version, which states that the state's main goal in global politics is to achieve power. Waltz explained that power is just a tool to achieve the country's main goal: survival. Waltz himself is the "originator" of the emergence of defensive realism [23]. Three basic assumptions of defensive realism will be used in this study: countries can take advantage of technological capabilities and geographic aspects to assist their defence. The third point is to increase strength to support the status quo, not to become a revisionist state, because the state's main goal is to survive. These three basic assumptions will be used to analyze research questions related to how the state perceives threats and how to mitigate them.

In addition to using defensive realism, the author also uses the concept of multilateralism, often used by neo-liberal schools, especially institutionalism. Several basic assumptions are, of course, used as a reference for researchers to answer research questions through the perspective of neo-liberal institutionalism. Robert Axelrod explained that multilateralism encourages strategic cooperation between countries, especially in solving strategic issues. Another point explained by Axelrod is that the world's condition is anarchy, resulting in the country being in a prisoner dilemma. According to Axelrod, this position forces countries to work together because the issues and problems they face are increasingly complex, so countries will inevitably form international organizations [24].

On the one hand, Robert Keohane added that multilateral cooperation needs to be established through international institutions. The formation of institutions is inseparable from the ease of exchanging information and conflict resolution. Keohane emphasized that international institutions can run as they should by implementing diplomatic negotiations, strengthening agreements between countries and establishing international norms. Furthermore, this neo-liberal institutionalism sees that the state cannot resolve security issues in a self-help manner but instead need coordination and cooperation between countries [25].

2. Research Method

The paradigm in this study uses the pragmatism paradigm. What is the pragmatism paradigm? According to John W. Creswell, pragmatism is a research paradigm that focuses on research questions, not on methodological aspects, as focused by the positivism paradigm. The pragmatism paradigm will answer practical research questions that can be used as a solution. The advantage of this paradigm is that researchers are free to choose a methodology, method of data collection or analysis technique that suits their needs.

Another focus of this paradigm is formulating the problem in paradigm-based research focusing on "what" and "how" and what will be done from the research results. This research discusses how the strategy of nation-states in ASEAN anticipates threats that can disrupt the stability of

cyber security in Southeast Asia. Through the paradigm of pragmatism, the conclusions from the formulation of the problem can be one of the references in building a cyber security strategy among ASEAN member countries.

Researchers used a qualitative methodology to analyze the problems that exist in this study. Creswell said that qualitative methodology is used to analyze a social phenomenon using various theories or previous research and considering the importance of the point of view in seeing the problem being analyzed. The use of qualitative methodology cannot deny the aspect of reflexivity. A concept that confirms how the researcher's point of view views social phenomena that move from a theoretical approach, observational data or previous research. Through this methodology, researchers can elaborate on various kinds of data that can strengthen researchers' arguments in answering research questions related to cyber security strategy in Southeast Asia. The research approach uses a case study with embedded analysis as a research analysis technique. A case study is used to analyze, explain and describe social phenomena that occur in society and aims to find solutions or meaning from these phenomena. Meanwhile, embedded analysis is part of the analytical technique of a case study which aims to analyze a case in more depth, not holistically or broadly. In this study, researchers used a case study approach at the ASEAN regional level by analyzing the level of analysis, namely the nation-state as a unit as a member of the ASEAN organization.

3. Findings

3.1 Cyber Security Threats

Cyber threats disrupting ASEAN's political and economic stability can appear in various forms. One form of threat that can disrupt this stability is cyber terrorism. In a journal written by Kobuye Oluwafemi Samuel and Wan Rozaini Sheik Osman in their journal entitled Cyber Terrorism Attack of The Contemporary Information Technology Age: Issues, Consequences and Panacea said that cyber terrorism is an activity of a terrorist group that disrupts the security of a country's information technology by spreading a sense of afraid to gain political advantage. According to them, terrorist groups in today's digital era can cripple every country's information system or steal data without having to have sophisticated technological equipment. The research said that currently, there is a lot of malware being traded that can be used to cripple the country's information technology system. However, Joseph S. Nye doubts that cyberterrorism can paralyze a country's information, economic and defense systems due to limited resources. Even so, Nye continued to emphasize to the state not to turn a blind eye to the threat of cyber terrorism.

Another threat that countries in the Southeast Asian region need to watch out for is cyber war and cybercrime. According to Von Clausewitz, cyber war is a form of digitalization of war between countries. Cyber war can be a threat because, basically, in the current digital era, combat tools are connected to cyberspace. Daniel S. Papp and David Albert emphatically explained that the digital aspect had changed the war strategy between countries. If a country cannot secure digital aspects in the defence field, this does not rule out the possibility that other countries can exploit existing vulnerabilities. When a cyber war occurs, and the state cannot counterattack or defend itself, its military security will surely be threatened. Countries that cannot defend themselves from enemy attacks during a war are certain that other countries will easily control them. Therefore, the state needs to prepare itself for the threat of cyber war because, in the digital era, war is now more of a proxy war. The ability to paralyze other countries does not need to be done directly but by using satellite states, whether consciously or not. What's more, cyberspace has anonymous capabilities that can disguise traces of Internet users.

The state does not only need to be aware of the threat of cyber terrorism and cyber war. The social dimension is also threatened by the rise of cybercrime which is the main threat in cyberspace. Seeing the condition of ASEAN, which is now the centre of the e-commerce market, this potential can be exploited by criminal organizations to make profits in illegal ways. Research conducted by Lennon Chang with the title Cyber Crime and Cyber Security in ASEAN explains that the Southeast Asian region has detected a cyber crime population rate

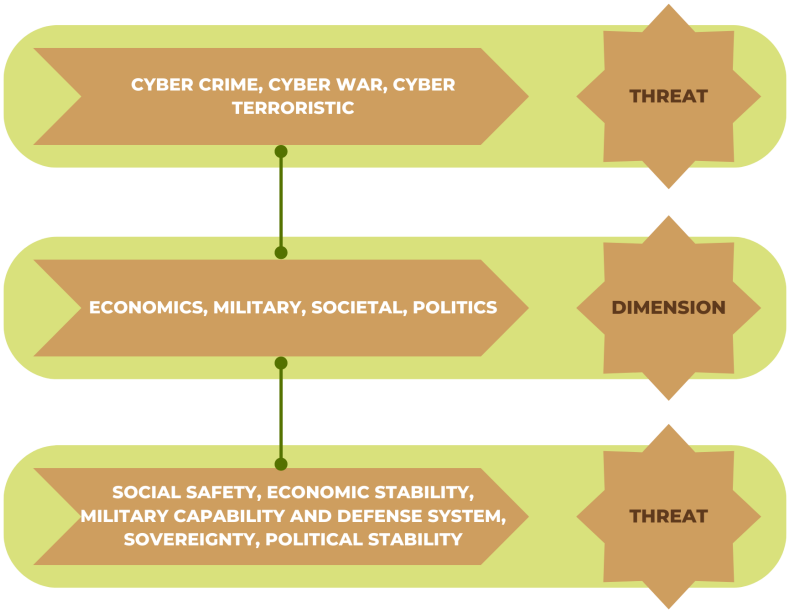
p-ISSN: 2686-6285
e-ISSN: 2715-0461

of 10 per cent throughout the Asia-Pacific region. Furthermore, Chang explained that Thailand and Malaysia indicated they had computers infiltrated by malware, with a total population of 35 per cent.

Meanwhile, the Philippines had a total malware population of 47.7%. Vietnam and Indonesia have malware populations of 50.7 and 60%, respectively. Malware is a computer program that infiltrates and steals data or financial information. Peter Hough argued that criminal organizations take advantage of the flexibility and anonymity of the Internet to hide their crimes. They not only steal money using encrypted communications but also cover up illegal transactions such as drug sales, human trafficking and the illegal sale and purchase of weapons.

Looking at the three major threats above, researchers see that cyber threats that can threaten the stability of the Southeast Asian region have different security dimensions. However, all of these dimensions of security are linked to one another. Cyberterrorism does not have an economic motive but a political one. Terrorist groups spread fear to disrupt political stability, which they will then change according to their political ideology. Regarding cyber war, countries remain a referent objects when other countries threaten their sovereignty. Cyber warfare threatens not only the country's political sovereignty but also the country's combat capability. When all defense systems have been integrated into an information system, vulnerabilities will appear, and their opponents can exploit that if their systems are not updated. On the other hand, the country's economy and citizen safety become referent objects when criminal organizations use technology to carry out their criminal acts. Thus, the cyber threat is no longer a perceived threat but has become a real threat that must get the attention of every ASEAN member country.

Systematically, cyber threats that have the potential to become a threat to ASEAN countries can be described in the flow below:



Picture 1. Potential Cyber Threats in Southeast Asia

In the 1990s, Kenneth Waltz said that the Cold War had lasted more than 30 years and ended. He explained that competition between countries would be more complex. The important point emphasized by Waltz is that nation-states are no longer fixated on arms competition but on the economy and technology. In his writings published in International Security, Waltz concluded that a country that can control political, military, economic and technological aspects would become one of the next superpowers. Seeing from the contemporary aspect, Waltz's opinion is not wrong. Currently, nation-states are competing to

become the foremost rulers in mastering technology. Currently, technology control is controlled by the United States, Japan and India.

Mastery of technology is, of course, also correlated with cyber security, which is the subject of discussion in this paper. The first basic assumption used as a reference in this research is "countries can take advantage of technological capabilities as well as geographical aspects to assist their defence." Technological capabilities in mitigating cyber threats that come and go can be developed by developing human resources. It cannot be denied that humans are the most important resource in advancing technology in every country in Southeast Asia. Innovations that emerge all the time are proof that a developed country is a country that cares about the development of its human resources. Countries in Southeast Asia should follow the example of India's program in advancing information technology in their country by providing a lot of training and scholarships. This has impacted many Indian diasporas who have become CEOs of technology companies, such as Sunai Pichai at Google or Satya Nadella at Microsoft.

The purpose of human development in defensive realism is inseparable from the state's interest in advancing technology in anticipating cyber threats. When a country can advance its technological capabilities, at least it can create innovations that can be implemented in the defence industry. Strategic industries such as defence need technology as one of the supports to maintain their sovereignty. In addition, the innovations carried out can also create technology that can anticipate cyber attacks such as malware or cyber espionage. When the state can develop technological human resource capabilities, at least it can be independent in a self-help way to safeguard its national interests. If a country completely depends on foreign technological assistance, the country's national interests can easily be intervened. At least in technology development, nation-states can start by developing their people first.

Countries that are technologically very advanced, at least their strength is starting to be considered. As previously explained by Kenneth Waltz, state power is no longer measured only by its military aspects but also by its technological capabilities. By the assumption of defensive realism, an increase in technological power is not destined to become a revisionist state. Technological improvements that need to be developed by countries in Southeast Asia are inseparable from their interests to survive the threat of cyber terrorism, cybercrime or cyber war. Culturally, countries in Southeast Asia are not expansionist countries with a very colonialistic pattern. They need to develop technological capabilities inseparable from cyber threats that can one day paralyze political, national and economic security stability in Southeast Asia. At the time of developing technology to mitigate cyber threats, countries in Southeast Asia also need to measure their ability not to be considered a revisionist state. However, the status quo state wants to maintain its influence at the current global political level. A country considered a revisionist state would be considered a threat that can disrupt its existence. The strength of the technology developed is intended as a reference for countries in Southeast Asia in maintaining their cyber security. The main goal is to survive and not become a revisionist state.

3.2 Multilateral Cooperation in Handling Cyber Threats

In his previous explanation, Robert Axelrod said that the nation-state is currently experiencing a prisoner dilemma. The threats that are coming are now increasingly complex and complicated. Robert Keohane also added that nation-states can no longer be self-help and must pay attention to cooperation between nations to overcome existing problems. In Southeast Asia, ASEAN has become one of the main pillars in developing strategic cooperation. The regional organization can become the main vessel in facilitating integrated multilateral cooperation in international institutions. Through multilateral cooperation at the ASEAN level, member countries can conceptualize strategic plans to maintain cyber security in Southeast Asia while at the same time encouraging the creation of a conducive ASEAN Economic Community.

This multilateral cooperation cannot be written off in building a cyber security strategy in Southeast Asia. Three points of view can be achieved from a researcher's point of view in achieving conducive cyber security. The first view cites the basic assumption of neoliberal

institutionalism itself that international institutions function to accommodate multilateral cooperation in achieving common interests. In the context of cyber security, countries can make
ASEAN a place to map threats originating from cyberspace. Through this pattern of cooperation, member countries can have the same perception regarding cyber threats that can disrupt
political and economic stability in Southeast Asia. Not only mapping threats, but ASEAN can also become a medium for finding the right solution to overcome cyber threats in each country's national interests.

The aspect of developing cooperation does not only aim to map cyber threats. The ASEAN can accommodate multilateral cooperation to bridge the technological gap between its member countries. As explained in the previous explanation, the technology owned by ASEAN member countries is very lame. Mastery of technology is currently still controlled by Singapore. However, ASEAN can bridge this gap by optimizing strategic technology-sharing cooperation. As a country with advanced technology, Singapore can be a leader in this cooperation. ASEAN organizations do not apply the principle of intervention. At least Singapore can become a mentor and guide in developing information technology among member countries. The method used can be in the form of technical assistance in making cyber security guidelines that can be adapted to the needs of each country. In addition, Singapore needs to make the country one of the hubs for developing human resources in information technology.

An aspect that is no less important in the development of multilateral cooperation in the field of cyber cooperation is information sharing. Referring to the basic neoliberal institutionalist assumption that international organizations need to be built to pursue common interests, ASEAN must become the protector of the cyber security of its member countries. In overcoming cyber threats, it is necessary to emphasize that threats in cyberspace are asymmetric and proxy. The threat is very difficult to recognize because it is anonymous. As the only regional organization in Southeast Asia, ASEAN must make guidelines on sharing information to ward off all cyber threats. Cyber threats are not a typology of threats that a country can resist individually. This threat needs to be countered through the active role of cooperation between ASEAN member countries. When an attack paralyzes one member country, the impact will affect other member countries. This encourages the importance of sharing information among ASEAN member countries to work together multilaterally to ward off cyber threats.

3.3 Policy Strategy Synergy

Talking about the policy strategies of ASEAN member countries in counteracting cyber threats, it cannot be denied that the sectors in security studies need to be considered. Based on the Copenhagen School approach, cyber threats can threaten referent objects in political, military, social and economic aspects. Each sector has a referent object that is different from one another. However, all these sectors are connected and must be maintained holistically. One destructive cyber attack can paralyze coordination among Southeast Asian countries. The state faces many choices as a very "sacred" IR actor. Countries can stand alone to maintain state security in cyberspace or exploit multilateral cooperation embodied under ASEAN institutions.

Examined in neorealist theory, the state has the right to develop its military, political, economic and socio-cultural capabilities to survive during an anarchic global political scene. Developing the state's information technology capability is seen as a step toward maintaining its existence and not becoming a revisionist state. ASEAN member countries do not have political influence and power like the United States or Russia. Nevertheless, the state has the right to develop its information technology capabilities. By developing this capability, at least the state can be independent in power and not rely too much on the role of other countries. Unfortunately, cyber threats cannot be taken care of alone. Such a self-help pattern is irrelevant in dealing with highly dynamic and anonymous cyber threats. State independence in developing power technologically can be strengthened through multilateral cooperation.

Cyber threats such as cybercrime, cyber terrorism or cyber war must be overcome using multilateral cooperation patterns. The researcher's point of view is inseparable from the form of threats which are real threats that all state actors must face. This means that any country has the same threat regarding cyber-attacks. The second point is that cyber threats cannot be faced alone because ASEAN member countries are interdependent. A single cyber attack on a technologically weak member state will, of course, directly impact a much stronger member state. The third point that should be studied as a strategic step for the state is cyber threats' asymmetric and proxy nature. Asymmetric threats in the digital era mean detecting who attacks which is very difficult. This inequality can be overcome through information sharing among ASEAN member countries. This information sharing will make it easier for ASEAN member countries to coordinate with each other. Therefore, the combination of cyber security development strategies in Southeast Asia is seen from a neorealist perspective and pays attention to the multilateral cooperation that ASEAN facilitates.

4. Conclusion

It is undeniable that the strategy that countries in Southeast Asia can develop in anticipating cyber threats is a combination of neorealist versions of self-help strategies and multilateral cooperation echoed by institutionalist neoliberals. Independently, the state needs to develop its power technologically. This is inseparable from the national interests of each country which has its preferences in developing its technology. However, anticipating dynamic cyber threats cannot be handled independently. The nature of interdependence that overshadows countries in the Southeast Asian region requires a pattern of multilateral cooperation that is coordinated with one another. Through this pattern of multilateral cooperation, at least ASEAN member countries can achieve the same common interest in dealing with cyber threats that can potentially disrupt Southeast Asia's political, military, economic and social stability.

References

[1] D. Marina, N. K. Pandjaitan, N. Hasanah, and G. P. Cesna, “Analysis of Lifestyle and Consumer Attitude Towards Intention to Purchase a Personal Car During Pandemic,” *APTISI Trans. Manag.*, vol. 7, no. 1, pp. 15–34, 2023.

[2] L. A. Faza, P. M. Agustini, S. Maesaroh, A. C. Purnomo, and E. A. Nabila, “Motives For Purchase of Skin Care Product Users (Phenomenology Study on Women in DKI Jakarta),” *ADI J. Recent Innov.*, vol. 3, no. 2, pp. 139–152, 2022.

[3] Y. K. Dwivedi *et al.*, “Artificial Intelligence (AI): Multidisciplinary perspectives on emerging challenges, opportunities, and agenda for research, practice and policy,” *Int. J. Inf. Manage.*, vol. 57, p. 101994, 2021.

[4] U. Rahardja, Q. Aini, Y. I. Graha, and M. R. Tangkaw, “Gamification Framework Design of Management Education and Development in Industrial Revolution 4.0,” in *Journal of Physics: Conference Series*, 2019, vol. 1364, no. 1, p. 12035.

[5] T. Stadelmann, M. Braschler, and K. Stockinger, “Introduction to applied data science,” in *Applied Data Science*, Springer, 2019, pp. 3–16.

[6] J. Paschen, “Investigating the emotional appeal of fake news using artificial intelligence and human contributions,” *J. Prod. Brand Manag.*, 2019.

[7] A. Nurhayati and F. Frencius, “Mapping perception of consumer antivirus software with multidimensional scaling method,” *APTIKOM J. Comput. Sci. Inf. Technol.*, vol. 4, no. 3, pp. 91–95, 2019.

[8] Y. Duan, J. S. Edwards, and Y. K. Dwivedi, “Artificial intelligence for decision making in the era of Big Data–evolution, challenges and research agenda,” *Int. J. Inf. Manage.*, vol. 48, pp. 63–71, 2019.

[9] R. J. Sipahutar, A. N. Hidayanto, U. Rahardja, and K. Phusavat, “Drivers and Barriers to IT Service Management Adoption in Indonesian Start-up Based on the Diffusion of Innovation Theory,” in *2020 Fifth International Conference on Informatics and Computing (ICIC)*, 2020, pp. 1–8.

[10] N. F. Syed, S. W. Shah, R. Trujillo-Rasua, and R. Doss, “Traceability in supply chains:

p-ISSN: 2686-6285
e-ISSN: 2715-0461

A Cyber security analysis," *Comput. Secur.*, vol. 112, p. 102536, 2022.
[11] E. Ukwandu *et al.*, "Cyber-security challenges in aviation industry: A review of current and future trends," *Information*, vol. 13, no. 3, p. 146, 2022.
[12] A. Corallo, M. Lazoi, M. Lezzi, and A. Luperto, "Cybersecurity awareness in the context of the Industrial Internet of Things: A systematic literature review," *Comput. Ind.*, vol. 137, p. 103614, 2022.
[13] D. Ghelani, "Cyber security, cyber threats, implications and future perspectives: A Review," *Authorea Prepr.*, 2022.
[14] J. Kaur and K. R. Ramkumar, "The recent trends in cyber security: A review," *J. King Saud Univ. Inf. Sci.*, vol. 34, no. 8, pp. 5766–5781, 2022.
[15] A. Reeves, P. Delfabbro, and D. Calic, "Encouraging employee engagement with cybersecurity: How to tackle cyber fatigue," *SAGE open*, vol. 11, no. 1, p. 21582440211000050, 2021.
[16] N. Chowdhury and V. Gkioulos, "Cyber security training for critical infrastructure protection: A literature review," *Comput. Sci. Rev.*, vol. 40, p. 100361, 2021.
[17] R. Al Nafea and M. A. Almaiah, "Cyber security threats in cloud: Literature review," in *2021 International Conference on Information Technology (ICIT)*, 2021, pp. 779–786.
[18] I. H. Sarker, M. H. Furhad, and R. Nowrozy, "Ai-driven cybersecurity: an overview, security intelligence modeling and research directions," *SN Comput. Sci.*, vol. 2, pp. 1–18, 2021.
[19] H. S. Lallie *et al.*, "Cyber security in the age of COVID-19: A timeline and analysis of cyber-crime and cyber-attacks during the pandemic," *Comput. Secur.*, vol. 105, p. 102248, 2021.
[20] R. V. Yohanandhan, R. M. Elavarasan, P. Manoharan, and L. Mihet-Popa, "Cyber-physical power system (CPPS): A review on modeling, simulation, and analysis with cyber security applications," *IEEE Access*, vol. 8, pp. 151019–151064, 2020.
[21] S. Acharya, Y. Dvorkin, H. Pandžić, and R. Karri, "Cybersecurity of smart electric vehicle charging: A power grid perspective," *IEEE Access*, vol. 8, pp. 214434–214453, 2020.
[22] A. Corallo, M. Lazoi, and M. Lezzi, "Cybersecurity in the context of industry 4.0: A structured classification of critical assets and business impacts," *Comput. Ind.*, vol. 114, p. 103165, 2020.
[23] E. Guustaaf, U. Rahardja, Q. Aini, H. W. Maharani, and N. A. Santoso, "Blockchain-based Education Project," *Aptisi Trans. Manag.*, vol. 5, no. 1, pp. 46–61, 2021.
[24] S. Porru, A. Pinna, M. Marchesi, and R. Tonelli, "Blockchain-oriented software engineering: challenges and new directions," in *2017 IEEE/ACM 39th International Conference on Software Engineering Companion (ICSE-C)*, 2017, pp. 169–171.
[25] R. Widhawati, A. Khoirunisa, N. P. L. Santoso, and D. Apriliasari, "Secure System Medical Record with Blockchain System: Recchain Framework," in *2022 International Conference on Science and Technology (ICOSTECH)*, 2022, pp. 1–8.