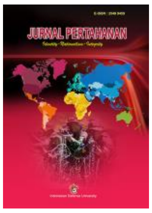
Jurnal Pertahanan

Media Informasi tentang Kajian dan Strategi Pertahanan
yang Mengedepankan *Identity*, *Nationalism* dan *Integrity*
e-ISSN: 2549-9459
http://jurnal.idu.ac.id/index.php/DefenseJournal



CYBER COOPERATION IN THE FRAMEWORK OF THE ASEAN REGIME

Dedy Obet[1], Suharto[2], Henri Mujoko[3]
Indonesian Naval Command and Staff College
Ciledug Raya Street No. 2, Seskoal Area, South Jakarta, DKI Jakarta, Indonesia 12230
debetmerauke@gmail.com[1], suharto@idu.ac.id[2], henrymujoko@gmail.com[3]

Article Info

Article history:
Received : June 25, 2021
Revised : July 7, 2021
Accepted : August 28, 2021

Keywords:
ASEAN Regime,
ASEAN Regional Forum,
COVID-19 Pandemic,
Cooperation,
Non-Traditional Security,

DOI:
http://dx.doi.org/10.33172/jp.v7i2.1264

Abstract

The COVID-19 pandemic has a given significant impact on both economics and internet-based digital services in Southeast Asia. It also applied to cross-border nontraditional security issues such as cyber-attacks that evolve continuously. The complexity of prevention acts towards cyber threats in Southeast Asia is quite complicated. Therefore, the ASEAN countries should form strong cooperation due to many anonymous and impromptu attacks. This research aims to analyze cyber cooperation within the ASEAN framework. The method applied in this article is the qualitative method, by accumulating data through earlier literature and studies. The outcome of this analysis shows the mechanism to perform cyber cooperation is through the ASEAN regional forum known as ARF (ASEAN Regional Forum) as the organizer of ASEAN countries' interactions in eliminating cyber-attacks. This research gives conclusions that the proposed mechanism should be flexible, multi-dimensional, and taking accounts from the economics point of view.

INTRODUCTION

The COVID-19 pandemic has given a significant impact on both economics and internet-based digital services in Southeast Asia. The dependency on computers and the internet makes cyber-attacks seemingly prevalent in society today. The transnational security issues originated from cyber threats seem to be endless (Caballero-Anthony, 2016). The development of technology and the internet generates huge impacts on society today. Most activities relying on humans slowly transferred into digital. Not only that, the internet simplifying our way of life daily in retrieving any information easily.

In 2020, 40 million people are using the internet in Southeast Asia, out of over 100 million new users joined over the previous five years within 2015–2019. This remarkable growth shows 70% of the population in our region uses the internet (Davis et al., 2020). Previous research by Google and Temasek found smartphones users access the Internet tremendously, around 90 percent only in Southeast Asia. The Hootsuite study found most internet users in Indonesia, the Philippines and Malaysia spend 4 hours accessing the internet through their mobile daily. Meanwhile, Thailand users spend the longest time in Southeast Asia, which is 4 hours 56 minutes daily (Kemp, 2018).

The complexity of geopolitical discourse increases considering the world is currently in the Fourth Industrial Revolution. In this new order, Artificial Intelligence (AI), Internet of Things (IoT), Big Data, cloud, and mobile technology changed the equation in the economy, business, politics, and cultural aspects to people's lives in the simplest way (Soepandji & Farid, 2018). Although ASEAN countries are confident in their cybersecurity systems, 58% believe that the systems are vulnerable to any cyber threats. The network and malware threats are seen as major hazards across the region including Southeast Asia.

Our conditions require different preventive strategies considering differences of view between the fourth and fifth generations. The previous generation has a concept of conflict more conventionally and physically, while the newer generation has a concept in an interconnected network, cross-country, and based on technology. As the world's largest cyber user, ASEAN is vulnerable to many kinds of cyberattacks. Therefore, this research aims to offer solutions to strengthen the cooperation anticipating cyber attacks. To achieve the objectives, the writers will explain the cyber threat's complexity in Southeast Asia, analyze cyber cooperation within the ASEAN framework and offer recommendations as to the conclusions.

Disruption due to the COVID-19 pandemic has made the cyber world more dangerous. The COVID-19 crisis is both an information crisis and a crisis of trust. Since the start of the pandemic, there has been a tremendous increase in cyberattacks. During the pandemic, most cyberattacks were caused by human actions as well as system and technology failures. Sources of intentional (theft, sabotage, fraud, and

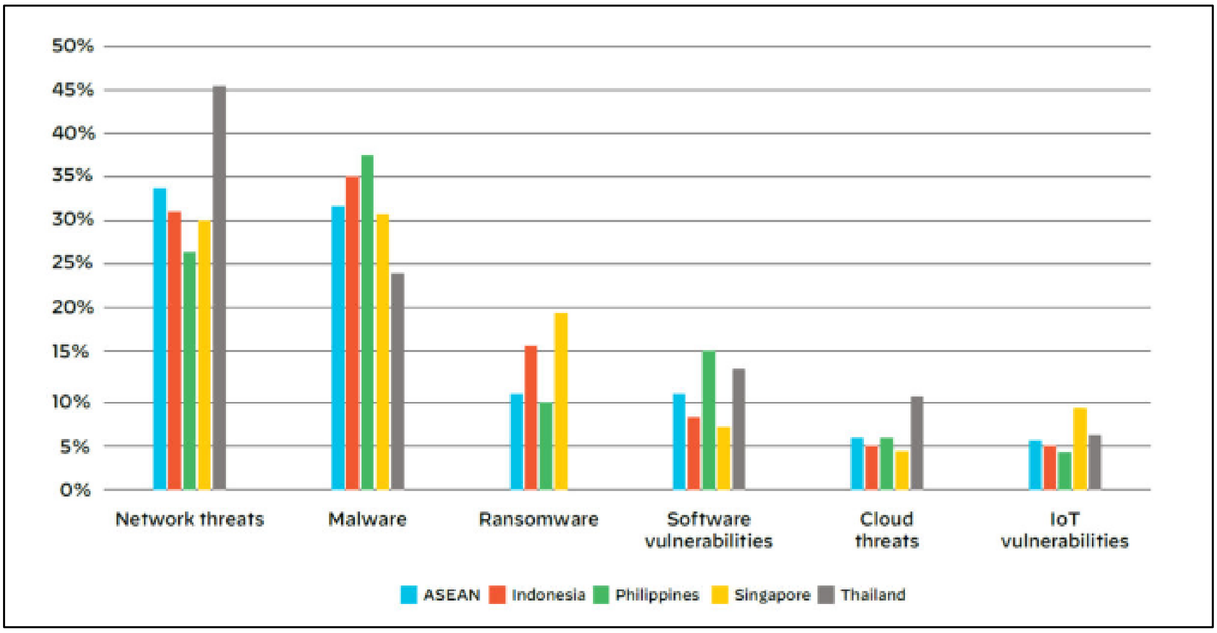


Figure 1. Cyber Attacks Threats within ASEAN
Source: Palo Alto Networks, 2020

vandalism) and unintentional actions (negligence and error). Cybercrime also occurs in software (coding practices, testing, security settings, change control, configuration management, and compatibility), hardware (capacity, performance, maintainability, and obsolescence), and systems (specifications, design, integration, and complexity) (Yadav, 2021).

This proves that a pandemic can also be a momentum used by hackers to exploit the cyber world. Research shows that 70% of organizations have increased their expenses in cybersecurity to prevent and narrow their vulnerabilities, thus representing the importance of this issue to be studied (Nallainathan, 2021). Although technology helps in preventing cyber-attacks in various ways, attackers or hackers around the world especially in ASEAN have made the pandemic a great opportunity to carry out various malicious activities and attacks for financial gain and to promote their malicious claims. Most governmental and public systems (economics, public health, cyberspace, defense, etc.) are vulnerable to cyber attacks due to the increase of complexity in those system’s dependency. The pandemic shows such complexity and is now a worldwide issue, especially in the ASEAN region. On the other hand, it sparks an online revolution across the globe with new opportunities, risks, threats, and dangers (Tsekeris & Mastrogeorgiou, 2020). Therefore, the ASEAN countries should form strong cooperation due to many anonymous and impromptu attacks. This research aims to analyze cyber cooperation within the ASEAN framework

METHODS

This research is using the qualitative method. Creswell (2017) stated that qualitative method is a form of scientific research based on text to analyze and understand cases, phenomena, and/or social problems. Accumulating data through earlier literature and studies as well as other secondary resources. The output of literature is based on actual reports by governmental and non-governmental agencies, international treaty documents, moreover by online news relevant to cybersecurity issues and cooperation in ASEAN.

RESULT AND DISCUSSION

Cybersecurity Complexities in ASEAN

The internet usage expansion creates more vulnerability in Southeast Asian countries to cyberattacks, causing data breaches and/or system failures (Raska & Ang, 2018). The Philippines, Singapore, Vietnam, and Indonesia, are prone to cyber risks. Singapore (as well as Australia, Japan, New Zealand, and South Korea) is one of the ‘Cyber Five’ more vulnerable to cyber attacks due to their dependency on technology. Since they have the susceptible infrastructure, ASEAN countries are used to construct mechanisms securing the systems from cyber-attacks by having a well-connected hub to eliminate them (Raska & Ang, 2018).

The complexity to eliminate cyber threats in Southeast Asia is quite complicated. Therefore, The ASEAN countries should form strong cooperation due to anonymous and prompt attacks. The main part of eliminating cyber threats in Southeast Asia is to retrieve the most basic question like, how many cases are there in one region? By AT Kearney found that ASEAN countries experienced various malware attacks, especially ransomware and software that encrypts and locks many servers and computers. ASEAN's investment in cybersecurity systems reaches US$1.9 billion, contributed 0.06% by gross domestic product (GDP). It takes at least US$191 billion or 0.35% of GDP to secure the network within the ASEAN environment. Ironically, most of ASEAN's economic growth comes from digital trade (Ramadhan, 2020a).

On the other hand, they spend around 0.06% of their GDP, which is deficient should they experience cyberattacks (The ASEAN Post Team, 2019). Therefore, the investment in cybersecurity becomes a major concern in Southeast Asia mainly due to continuous attacks over the year. Stuxnet broke into Iran's nuclear reactor cooling system in 2009. As Advanced Persistent Threats known as APT, it shuts down cooling systems and crashes all industrial production. Stuxnet is an intelligent malware which attacks certain targets (Ramadhan, 2020a). Within time, a similar issue will occur in Southeast Asia. IBM Security published, many states in Southeast Asia have a lot of financial and reputational problems (IBM, 2019).

Based on the largest American technology company known as Cisco, business activities in Singapore experienced expansions in facing cyber security challenges because most people work from home since the COVID-19 pandemic. Nearly 3,200 companies from 21 countries in the survey from June 16 to September 4, Singapore made the most major shift on remote work throughout Asia-Pacific. Six in 10 organizations announce they experienced at least a 25 percent increase in cyber threats since the pandemic. These threats range from connections to malicious sites on the Internet and phishing attacks (Shiying, 2020).

According to a global cybersecurity firm known as Kaspersky, over 20 million cyber threats alone had happened in Thailand by 2020. Kaspersky Security Network (KSN) detected 20,598,223 cyber threats transmitted via the Internet to computers with KSN installed in Thailand last year. Reaching 28.4% of Thai users were vulnerable to online threats last year. Data shows over 2.7 million threats were detected on consumer products and 856,000 detected on enterprise products in Thailand (Nguansuk, 2021). The Philippines stood in 64th place globally in cyber threat observations with 8,998,044 threats detected in Q4 2019, decreasing significantly from 74th place with 11,757,863 threats detected in Q4 2018. The detected threats seem to outnumber the solved threats; however, data shows fewer local threats (76,900 incidents) recorded in the last quarter of 2019, compared to the same period in 2018 (453,788 incidents) (Cisomag, 2020).

National Cyber and Crypto Agency (BSSN) in Indonesia reported 290,3 million cyberattacks in 2019. Compared to 232.4 million cases in the previous year, this result increases significantly. Furthermore, Indonesian National Police-Criminal Investigation Agency (Bareskrim) too had announced the increase of cybercrimes reports. In 2019, a total of 4,586 reports were submitted through patrols, Bareskrim (Patrolisiber) website announced that cybercrimes expand from 4,360 reports in 2018. Cybercrimes are attacks on computer systems or networks to authorized access to targeted systems. Cybercrimes are defined as an illegal activity that uses and regulates the system (Anjani, 2021).

Based on several cyber security issues described previously, the issue of cyber security in Southeast Asia lies in the effectiveness of mechanisms in ASEAN as organizations with essential functions. Marguerite Borelli suggests in her research known as The ASEAN Counter-Terrorism Weakness, that ASEAN is very vulnerable once attacked by terrorist groups in the cyber world (Borelli, 2017). ASEAN constructed some essential projects to connect members and provide solutions needed such as transportation of natural. Trans ASEAN Gas line Pipes is expected to be one of the successful ASEAN projects (Borelli, 2017). However, Borelli explained that ASEAN does not have strong regulations to ensure the distribution is free of cyber-terrorist attacks. In the end, when there are no strong regulations, obstacles in establishing strategic cooperation between countries within the ASEAN framework occurred. ASEAN needs to develop strong regulations, establishing a task force to secure them from cyber-attacks (Krisman, 2013).

There are challenges to improve cybersecurity in Southeast Asia, includes: (Raska & Ang, 2018)

1. The lack of strategic mindset in most Southeast Asia countries, compliance, and institutional supervision of cybersecurity. Responsibility can be delegated and/or took place between the national police (focusing on cybercrimes), ministry of internal affairs (focusing on critical infrastructures), ministry of telecommunications (focusing on violations), and military (focusing on cyber conflicts), with little or zero coordination. The absence of a united framework resulting from the lack of investments.
2. The lack of considerations in the private sector, explaining that cyber threats are a part of information technology (IT) issues rather than business issues, resulting in regional businesses constructing a less comprehensive cybersecurity approach.
3. The lack of information sharing regarding intelligence threats within Southeast Asian countries, often due to mistrust and minimum transparency.
4. The lack of keeping up against rapid evolution in technology, resulting from difficulties in responding and monitoring cyber threats, especially with stronger encryptions, clouds computing, and expansions of the Internet of Things (IoT).

Developing Cyber Cooperation within the ASEAN Framework

The International relations studies announce there are terms applied in international law related to international organizations, known as an international regime. The institution's response to the actions between ASEAN countries on certain issues. In the absence of a comprehensive system, countries bounded by bilateral agreements, and the management of these agreements around the world becomes very complicated (Inoguchi & Le, 2020). The international regime correlates with principles, norms, rules, decision-making processes, both explicitly and implicitly, related with expectations and/or expectations of party, taking accounts of international relations point of view (Krasner, 1982). The regime also influences the behavior generated by international organizations on other parties, especially the parties in states focusing on other parties' expectations. In contrast to other legislative institutions concentrating more on what is happening within the organization than the influence of international organizations on other parties (Barkin, 2015).

Based on previous explanations, it is crucial for Southeast Asia to have a potential role as a significant neutral region in terms of international cybersecurity cooperation. The ASEAN cybersecurity regime is a general condition formed in Southeast Asia facing non-traditional forms of threats rising in such uncertain situations. The regime will calculate results obtained by a party, in this case, a regional institution, in uncertain situations (Chang, 2017). Therefore, by constructing a security regime in the region, ASEAN should manufacture regulations, procedures, and norms to control the behavior of regime members by strengthening forums and dialogue.

ASEAN constructed a regional forum known as ARF (ASEAN Regional Forum) as the organizer of ASEAN country's interactions in eliminating cyber-attacks. Unlike the security cooperation constructed by NATO (North Atlantic Treaty Organizations) which was formed based on a post-World War II defense agreement or alliance, ARF is intended to build mutual trust within ASEAN and ASEAN partners. ARF focuses more on dialogue and involvement of all members to prevent conflict, unidentical with NATO which focuses more on military power (Hemmer & Katzenstein, 2002). Thus, the ARF concept can be used as the main capital formation of a regional regime.

The ARF began in 2006 through the

joint statement in Malaysia and reaffirmed at the ARF Statement Cooperation in Ensuring Cybersecurity in Phnom Penh, 12 July 2012 focusing on cyber security initiative, with the following contents:

1. Promote further consideration of vision and strategy to address emerging threats in this area through the basis of international law and the basic norms and principles that apply consistently;
2. Promote the confidence-building measures (CBM), risk eliminations, and stability measures to overcome implications of information and communication technology (ICT) usage by external ARF participants, including potential conflicts of ICT use reviews;
3. Promote and enhance cybersecurity partnerships in the region;
4. Promote and develop ARF work plan on ICT safe use, focusing on practical collaboration in CBM, setting proper targets within implementation timeframes;
5. Review the possibility to explain common terms and definitions relevant to the use of ICT.

The threats of Information and Communication Technology (ICT) usage in ASEAN are in line with the expanding number of internet users. However, this has not been in line with the priority of infrastructure vulnerability in each country. An examination from ASEAN documents related to cyber remains ambiguous. In the 2020 ARF, Ministers in ASEAN countries recognized the importance of ICT security towards the economic aspect, regional and global challenges, and the dependency on ICT to eliminate the impact of COVID-19 (ASEAN Regional Forum, 2020). This research analyzes the outcome is that ASEAN should improve more proactive strategy based on the awareness that cyberspace is a tool in developing economic progress and improving the standards of the ASEAN community and the world. ASEAN's official cybersecurity mechanism to consider and decide interrelated cyber diplomacy, policy, and operational issues has not yet been fully established (Timur, 2017). This research gives the conclusion that the proposed mechanism should be flexible, multi-dimensional, and taking accounts from the economics point of view. Fundamental norms like trust and resilience between policymakers and non-state parties with an active defense approach must be applied in the region. The research recommends cyber security applied in the future with new concepts:

1. ASEAN should construct more comprehensive and practical agreement documents to overcome cyber threats,
2. ASEAN should develop cyber-attack guidelines, for example, forming Cyber Crime Strategy Handbook to improve each country's national cybercrime strategy that leads to cybercrime response efficiently and effectively,
3. ASEAN should establish trend-based cybercrime workshops and training sessions to eliminate information gaps between countries by involving non-state parties such as professionals, cyber employees, and corporate agencies within the state, and students.

ASEAN is investing heavily in the cyber domain. This is indicated by the creation of cyber norms in the ASEAN region. Despite these positive developments, this study illustrates that ASEAN's unique characteristics pose significant barriers to the emergence and eventual internalization of cyber norms. Although the possibility of common norms in ASEAN remains uncertain, the suggested approach could lead to the emergence of different norms yet congruent. Speaking of the policy strategies of ASEAN member countries in dealing with cyber threats, it cannot be denied that sectors in security studies must be taken into an account. In the Copenhagen School approach, cyber threats can threaten political, military, social, and economic objects. Each sector has a different reference object. However, all these sectors are interrelated and must be maintained holistically. Cyberattacks can cripple coordination between countries in Southeast Asia. Despite the possibility that viewed from the view of neorealism, the state can stand alone to maintain state security (Ramadhan, 2020b).

This study examines a strategy that can be developed by countries in Southeast Asia in anticipating cyber threats is the incorporation of a neorealist version of ‘self-help’ strategy but also needs to be focused on multilateral cooperation developed by institutionalist neoliberal views (Irawan, Subagyo, & Oktaviani, 2017). Multilateral cooperation patterns must be used to overcome cyber threats such as internet crimes, cyber terrorism, or cyber wars. The form of cyber threats is essentially a real threat to every stakeholder. Cyber threats cannot be overcome by a single ASEAN member since they are interdependent. A cyberattack against a technologically frail member of the ASEAN will inevitably have a direct impact on a much stronger member country. In addition, the asymmetric nature of cyber threats and actors must be studied as a strategic step for ASEAN countries. Asymmetric threats in the digital age are increasingly difficult to detect who is attacking whom. This inequality can be overcome by sharing information amongst ASEAN member countries. This mutual sharing of information will facilitate coordination between the members. Therefore, the cybersecurity development strategy in Southeast Asia should also be attention to the neorealism aspect of institutionalism, by paying attention to multilateral cooperation facilitated by ASEAN.

CONCLUSIONS, RECOMMENDATION AND LIMITATION

The cross-border non-traditional security issues on cyber-attacks evolve continuously. The complexity of prevention acts towards cyber threats in Southeast Asia is quite complicated. Therefore, The ASEAN countries should form strong cooperation due to anonymous and prompt attacks. This analysis shows the mechanism to perform cyber cooperation is through the ASEAN regional forum known as ARF (ASEAN Regional Forum) as the organizer of ASEAN country's interactions in eliminating cyber-attacks. This research gives the conclusion that the proposed mechanism should be flexible, multi-dimensional, and taking accounts from the economics point of view.

REFERENCES

Anjani, N. H. (2021). *Perlindungan Keamanan Siber di Indonesia*.

ASEAN Regional Forum. (2020). *Chairman’s Statement of the 27th Asean Regional Forum* (pp. 1–11). pp. 1–11. Seoul, Korean.

Barkin, J. (2015). *International Organization: Theories and Institutions*. Springer.

Borelli, M. (2017). ASEAN Counter-terrorism weaknesses. *Counter Terrorist Trends and Analyses*, *9*(9), 14–20.

Caballero-Anthony, M. (2016). *An introduction to non-traditional security studies: a transnational approach* (1st ed.; M. Caballero-Anthony, Ed.). Singapore: Sage.

Chang, L. Y. C. (2017). Cybercrime and cyber security in ASEAN. In *Comparative criminology in Asia* (pp. 135–148). Springer.

Cisomag. (2020, January). Philippines – The Two Time Winner of Most Vulnerable Tag in SEA.

Creswell, J. W., & Creswell, J. D. (2017). *Research design: Qualitative, quantitative, and mixed methods approaches*. Sage publications.

Davis, S., Sipahimalani, R., Baijal, A., Cannarsi, A., Neves, N. C., & Dhanuka, R. (2020). e-Conomy SEA 2020: Resilient and racing ahead — What marketers need to know about this year’s digital shifts. In *e-Conomy SEA 2020 Report*. Jakarta.

Hemmer, C., & Katzenstein, P. J. (2002). Why is there no NATO in Asia? Collective identity, regionalism, and the origins of multilateralism. *International Organization*, *56*(3), 575–607.

IBM. (2019). Cost of a data breach report. In *IBM Security*. New York.

Inoguchi, T., & Le, L. T. Q. (2020). Sovereign States' Participation in Multilateral Treaties. In *The Development of Global Legislative Politics* (1st ed., pp. 33–71). Switzerland AG: Springer. https://doi.org/10.1007/978-981-32-9389-2_4

Irawan, F. L. P., Subagyo, A., & Oktaviani, J. (2017). Faktor-Faktor Penghambat Asean Intergovernmental Commission On Human Rights (Aichr) Dalam Penegakan Hak Asasi Manusia Di Asia Tenggara. *Jurnal Dinamika Global*, *2*(01), 48–81.

Kemp, S. (2018, January). Digital in 2018: World's internet users pass the 4 billion mark. *We Are Social*, pp. 1–18. New York.

Krasner, S. (1982). *Structural Causes and Regime Consequences: Regimes as Intervening Variables*. New York: Cornell University Press.

Krisman, K. (2013). A Secure Connection: Finding the Form of ASEAN Cyber Security Cooperation. *JAS (Journal of ASEAN Studies)*, *1*(1), 41–53.

Nallainathan, S. (2021). Analysis onto the Evolving Cyber-Attack Trends during COVID-19 Pandemic. *International Journal of Science and Research (IJSR)*, *10*(4). https://doi.org/10.21275/sr21403140109

Nguansuk, S. L. (2021, April). Fight to foil cyberthreats intensifies.

Palo Alto Networks. (2020). The state of cybersecurity in financial services. *Finextra*, pp. 1–8. Santa Clara: Palo Alto Networks.

Ramadhan, I. (2020a). Building Cybersecurity Regulation in Southeast Asia: A Challenge for the Association of Southeast Asian Nations (ASEAN). *Journal of Social and Political Sciences*, *3*(4). https://doi.org/10.31014/aior.1991.03.04.230

Ramadhan, I. (2020b). Strategi Keamanan Cyber Security di Kawasan Asia Tenggara. *Jurnal Asia Pacific Studies*, *3*(2), 181–192. https://doi.org/10.33541/japs.v3i1.1081

Raska, M., & Ang, B. (2018). Cybersecurity Asia in Southeast. In *Asia Centre*. National Technology of.

Shiying, W. (2020, October). Cyber security threats on the rise as more people work from home: Cisco survey, Singapore News & Top Stories - The Straits Times.

Soepandji, K. W., & Farid, M. (2018). Konsep Bela Negara dalam Perspektif Ketahanan Nasional. *Jurnal Hukum & Pembangunan*, *48*(436–456). https://doi.org/http://dx.doi.org/10.21143/jhp.vol48.no3.1741

The ASEAN Post Team. (2019, October). Southeast Asia's Internet Economy Booming | The ASEAN Post.

Timur, F. G. C. (2017). The Rise of Cyber Diplomacy ASEAN's Perspective in Cyber Security. *KnE Social Sciences*, 244–250.

Tsekeris, C., & Mastrogeorgiou, Y. (2020). Contextualising COVID-19 as a Digital Pandemic. *Homo Virtualis*, *3*(2), 1. https://doi.org/10.12681/homvir.25445

Yadav, R. (2021). Cyber Security Threats During Covid-19 Pandemic. *International Transaction Journal of Engineering Management \& Applied Sciences \& Technologies*, *12*(3), 1–14. https://doi.org/10.14456/ITJEMAST.2021.59