Geopolitics Quarterly, Volume: 20, No 2, Summer 2024 Scopus

PP 255-278

Interpreting the Role of State, Non-State, and International Organization to form Cybersecurity Governance in Southeast Asia

Iqba Ramadhan *- Ph.D. Candidate International Relations Department UNPAD and Lecturer at IR Department Universitas Pertamina, Indonesia.

R.Widya Setiabudi Sumadinata- Full Professor International Relations Department, Universitas Padjadjaran, Bandung, Indonesia.

Darmansjah Djumala- Associate Professor, International Relations Department, Universitas Padjadjaran, Bandung, Indonesia.

Wawan Budi Darmawan- Associate Professor, International Relations Department, Universitas Padjadjaran, Bandung, Indonesia.

Received: 26/06/2022 Accepted: 30/11/2023

https://doi.org/10.22034/igq.2024.198274

Abstract

Southeast Asia is a region undergoing economic development and technological advancement. This region's economic growth is supported by the digital world, which contributes in the form of a digital economy. However, as the digital economy grows, cyberspace lacks stable cyber security governance. As a result, this area is extremely vulnerable to all types of cyber threats. The author intends to interpret the role of state actors, non-state actors, and international organizations in developing cybersecurity governance in Southeast Asia through this article. In a conceptual framework, the preparation of regional governance must involve collaboration across actors due to their distinct functions. Such governance can maintain cyber security while also accommodating stakeholders in the Southeast Asian region through multi-sectoral collaboration. Therefor, the authors argued that the collaboration between state, non-state, and regional organization are needed to overcome cyber threats. In addition, regional cybersecurity governance should be a turning point to make more secure cyber space in Southeast Asia.

Keywords: Cybersecurity, Regional Governance, Southeast Asia, State Actors, Non-State Actors.

* E-mail : iqbal.ramadhan@universitaspertamina.ac.id

1. Introduction

Technology offers numerous advantages for the advancement of human life in the political, economic, and social spheres. According to Joseph S. Nye's book The Future of Power, technology is a new force that the state must control in the political, military, and economic fields (Nye Jr,2011:65). Nye believes that the state must master the power of technology because it faces cyberspace threats. According to Nye, the state now faces not only physical but also digital threats (Nye Jr,2011:65). Technology is like an arms race in today's digital age. Countries with technological clout have the potential to turn technology into a sophisticated weapon (Papp and Albert,2001:23). It is impossible to deny that technology has an impact on a country's foreign relations and the political order of a region kawasan (Cavelty and Egloff, 2019:37; Velasco,2022:413). For example, rivalry between Iran and Israel in the Middle East region exists in both the physical and cyber realms. To prevent Iran from developing nuclear technology, Israel is suspected of infiltrating malware into the Natanz nuclear reactor (Kausch,2017:2–3). Non-state actors, such as terrorist groups, can use technology to hack state-owned information systems, finance terrorist activities, recruit new members, and spread propaganda (Gultom and et al,2018:3289; Ramadhan, 2020:191).

Despite the growing digital threat, we cannot deny that technology provides tremendous benefits to a region's economic growth. One example is the incorporation of technology into economic activities, which gave rise to e-commerce as a measure of economic growth (Nengsi,2019:517). The European Union believes that digital commerce is inextricably linked to cybersecurity. They put in place the "EU Cybersecurity Strategy 2013" by focusing on three aspects of overcoming cyber threats: cyber resilience, reducing cybercrime rates, and cyber defense capabilities (Düll and et al,2018:314–17). Furthermore, the European Union recognizes that mitigating cyber threats in the European region is a form of collaboration. The European Union implements increased cybersecurity capabilities among its member states through its cyber policy strategy (Düll and et al,2018:320). According to the European Union, cybersecurity governance in the European region must be built on the fundamental pillars of freedom, economic growth, and security (Nagyfejeo,2021:4–6).

Not only will Europe benefit from the growth of the digital economy, but so will Southeast Asia. The increase has a significant impact on the growth of

Southeast Asia's digital economy, particularly in digital trade and online transportation businesses (Nengsi,2019:517; Yuniar,2017). According to economists, total trade in Southeast Asia will reach 102 billion US dollars by 2025 and the digital economy contributed $20 billion in economic growth to the region in 2018 (ASEAN-UP,2019; E-Trade for All,2018). Furthermore, the International Monetary Fund (IMF) stated that total digital trade in Southeast Asia could reach US$2.8 trillion in the coming years (Feng,2018). The digital economy in this region is irrevocably linked to the growing number of Internet users in ASEAN (Association of Southeast Asian Nations) member countries. For example, approximately 82 percent of Singapore's population has access to the Internet. Around 70% of the people in Malaysia, Thailand, Brunei, Indonesia, and the Philippines are connected to the internet (Chang,2017; ASEAN-UP,2019).

Although the Southeast Asia region is capable of digital development, it still faces critical cybersecurity issues. Unlike the European Union, which already has a cyber security mitigation strategy in place, ASEAN, as an important regional actor, lacks stable cyber security governance. ASEAN established an economic zone known as the ASEAN Economic Community in 2015. Integration of technology to support economic growth is one of the pillars. The 2012 ASEAN ICT Masterplan, in particular, emphasizes the importance of economic integration being supported by an established framework of information security cooperation (Ramadhan,2017:505). The lack of cybersecurity governance in this region certainly raises a number of issues. One of them is in the case of a cyber incident, such as cybercrime. ASEAN will eventually find it difficult to mitigate or resolve the problem (Noor,2020:110). Furthermore, without this cybersecurity governance, ASEAN will struggle to resolve cyber conflicts between its member countries as well as with non-state actors such as terrorist groups or criminal organizations (Manopo and Sari,2015:44–45).

Based on the perspective of security studies, non-traditional threats include cyber threats. ASEAN already has a framework of cooperation in place to deal with non-traditional threats. In the fight against terrorism, ASEAN has developed strategic policies outlined in the ASEAN Convention on Counter-Terrorism (Sudirman and Sari,2017:24). The regulation governs ASEAN member countries' cooperation mechanisms, particularly in the areas of terrorism financing, money laundering, and specific cooperation in the fields of politics, military, security, and law to mitigate threats posed by terrorist

groups (Sudirman and Sari,2017:24–25). ASEAN also has a cooperation framework outlined in the ASEAN Convention on Trafficking in Persons, Particularly Women and Children (ACTIP). This governance discusses ASEAN's efforts to eradicate human trafficking and protect human rights (Subono and Kosandi,2019:90). ACTIP also governs the Regional Consultation Process (RCP), a mechanism for resolving human trafficking in accordance with the national interests of ASEAN member countries (Yazid and Septiyana,2019:98). Another non-traditional threat regulated by the regional governance is the cooperation mechanism in combating illegal drug trafficking. In 1998, ASEAN member countries signed the Joint Declaration for a Drug-Free ASEAN. The goal is to have an ASEAN that is drug-free by 2020 (Mok,2020:35). This governance is furthered by China's inclusion as a strategic partner in the ASEAN-China Cooperative Operations in Response to Dangerous Drugs (ACCORD) agreement. Through this agreement, ASEAN and China are collaborating to address Southeast Asia's narcotics problem, particularly in Myanmar, Cambodia, and Laos (Harper and Tempra,2020:117). ASEAN, unlike the previous example, does not yet have standard rules for cybersecurity governance. This cybersecurity issue is only addressed in a joint statement issued by ASEAN leaders (ASEAN,2021b).

This lack of clarity in Southeast Asia's governance will undoubtedly spark debate. ASEAN, as a vital organization in the region, must anticipate potential cybersecurity issues in the political, security, and economic spheres. In the political realm, the absence of cybersecurity governance can jeopardize a region's geopolitical stability. For example, the European Union seeks to maintain the geopolitical stability of the European region from cyber threats through the Cybersecurity Strategy 2013, so that economic growth and citizen security are not jeopardized (Düll and et al,2018:320). This lack of governance allows terrorist organizations to use technology for terrorist purposes in the security sector. Terrorist groups can use the internet to seek funding, spread propaganda, and recruit new members (Ramadhan,2020:192–93). Because the impact will be felt, cybersecurity governance is critical in the economic field. According to IBM Security 2019, the most common cybercrime in Southeast Asia is the theft of credit card and medical record data (IBM Security,2019). This cybercrime has caused a total global loss of $400 million (McAfee,2014). Telecommunications companies, for example, lose at least $10,000 per hour

when a cyberattack cripples their critical infrastructure (Yadav and Gour, 2014:938).

In the internal context of ASEAN, the problem of a lack of cybersecurity governance cannot be separated from the existence of rivalry among member countries. ASEAN solidarity on cyber security remains very low. The ineffectiveness of the cyber security capacity-building program exemplifies this issue. Some countries are hesitant to implement information security cooperation because they are concerned about exposing state secrets to the public sphere (Manopo and Sari,2015:45). Another reason why cyber security governance is difficult to implement in Southeast Asia is the large technological gap between ASEAN member countries. The International Telecommunication Union (ITU) published data on countries with high cybersecurity maturity, including Singapore, Malaysia, Thailand, and Indonesia (ITU,2018). The four countries have a cyber maturity index that is greater than 0.775. Meanwhile, Vietnam, the Philippines, and Brunei Darussalam have middle-level cyber maturity. In the meantime, Laos, Myanmar, and Cambodia received cybersecurity maturity indexes ranging from 0.161 to 0.195 (ITU,2018). This disparity is inextricably linked to each country's ability to develop its information technology infrastructure. Despite these concerns, the development of cyber security governance is required. The economic growth is already heavily reliant on technology. It is appropriate for regional organizations like ASEAN to prioritize cyber security issues on their annual agenda. Furthermore, the role of non-state actors such as academia, the private sector, and businesses has not been given a fair share of consideration in the development of cybersecurity governance. Non-state actors are frequently regarded as more deserving of working on technical issues than on policy. As a result, state actors have a higher standing than non-state actors (Eggenschwiler,2020:91; Tanczer and et al,2018:61). The author intends to review how collaborations between state actors, non-state actors, and regional organizations such as ASEAN formulate inclusive cyber security governance in Southeast Asia through this scientific article.

2. Methodology

The author employs a qualitative methodology to elaborate on the roles of state, non-state, and regional actors in establishing cybersecurity governance. In this scientific article, the author employs a qualitative

approach. This method is used by the author to investigate patterns of interaction between factors in order to better understand social and political processes. In general, qualitative approaches are inextricably linked to the use of textual data, which researchers subsequently interpret to investigate interaction patterns between factors (Creswell,2015:25). Meanwhile, this form of research is known as a case study. A case study, according to Creswell, is a sort of research that investigates the relationship between one instance and other cases, both single and holistic (Creswell,2015:25). Case study research in International Relations examines the interaction of actors across borders on political, security, social, or economic issues (Roselle and Spray,2012). This research, by contrast, produces a strategic policy that focuses on identifying and describing strategies, developing new theories, or planning actions. In general, strategic research outputs will explain the actions that must be taken to be more effective or develop strategies such as what is required to deal with new problems (Ritchie and Spencer,2002). Meanwhile, the authors use secondary data from previous research collected from credible sources such as Scopus or Dimensions during the analysis stage (Creswell,2014). Furthermore, the authors employ a systemic review to create an analytical framework based on secondary data sources such as scientific journals. The author then applies the analytical framework to develop arguments in response to the research question (Snyder,2019).

3. Theoritical Framework

3-1. Cybersecurity as an Issue in International Relations Studies

Cyber security is a novel topic in the field of International Relations. Buzan explained that as global political actors evolve, so will issues. This is referred to as the expansion of issues and the deepening of security actors (Buzan and et al,1998:2). The phenomenon of cyber security is one of the issues that is experiencing a novelty. Cybersecurity is defined as a set of rules, regulations, and policies that protect an organization's cyber environment and all of its assets from cyberspace threats (Radu,2015:5–6). At the start of its evolution, cyber security was primarily concerned with technical issues. However, cyber security is now a cross-scientific issue because it necessitates perspectives from various fields of science (Lacy and Prince,2018:2). Because this phenomenon involves interactions between state and non-state actors, cyber security is becoming one of the issues in international relations. Furthermore, because the issue is cross-border,

stakeholders must work together to manage cybersecurity issues globally (Lacy and Prince,2018:2–3).

The emergence of cyber security issues as a phenomenon of international relations gave birth to a new paradigm known as the New Copenhagen School. This paradigm is based on Buzan's Copenhagen School, which addresses issues and threats in the military, political, social, economic, and environmental sectors (Buzan and et al,1998:4). One new security sector, namely cyber, has been added to New Copenhagen School (Kassab,2014: 65). The main reason why cyber has become one of the new sectors in security studies is that it has the potential to reduce the decency of people's lives, disrupt the country's political stability, and change the order of appropriate conditions of human social life. Furthermore, cyber security securitization can cover local, regional, and global areas (Kassab,2014:67). Threats from the digital world come in a variety of shapes and sizes. Countries securing critical infrastructure, for example, must contend with both structured and unstructured cyber threats. Structured cyber threats are typically perpetrated by state and non-state actors in a professional and organized manner. Moreover, countries must contend with the threat of sporadic unstructured cyberattacks such as hacktivism or website defacement. Cyberwar, cybercrime, and cyberterrorism are all examples of cyber attacks. All three are anonymous, and they cross state sovereignty lines (Dunn-Cavelty,2010:181–82).

3-2. Regional Governance

Regional governance is a concept studied in International Relations that aims to investigate the regulation of interactions between actors in a region. Regional governance is a synthesis of two concepts that seek to explain the participation of state actors, international organizations, and non-state actors in the formation of a coordination framework in a specific region (Willi and et al,2018:777; Veicy,2022:178). The concept of regional governance, which incorporates interactions among actors, represents a transition from the old regionalism concept to a new regionalism paradigm. According to Soderbaum, the old concept of regionalism focused on interactions between countries in the context of military politics, while the new concept focuses on the distribution of state power in a region. This shift in regionalism governance is inextricably linked to the evolution of issues within the region. As the Cold War, ended, state actors could no longer handle social, economic, political, and environmental issues alone. As a result, the

development of regional governance necessitates the participation of various actors (Soderbaum,2016:44–45). On a practical level, regional governance requires the role of regional organizations because they serve to accommodate member states' interests and oversee policies. Non-state actors participate in regional governance because they understand technical issues and community-level policy implementation (Foque and Steenbergen,2005: 54–57).

Various international relations schools hold opposing perspectives on the concept of regional governance. One of the approaches in this study, the school of neorealism, suggests that the state is the most important actor in the global political constellation. It means that, no matter how important an international organization's governance is, the nation-state will attempt to be autonomous and build its power without interference from other countries. According to the neorealism school, the state would eventually extend its power to the point of becoming a hegemon (Alhammadi,2022:152). In contrast to realism, which emphasizes power as the most important factor in a nation's survival, neoliberalism takes a different approach. In terms of global political arrangements, neoliberalism is the same as neorealism, which holds that the world is anarchic. Neoliberalism, on the other hand, sees these conditions as possibilities for countries to collaborate. It is inextricably linked to the reality that every state faces the same threats (Navari,2013). To counter this threat, states must work together to establish international institutions, regimes, and governance structures. Governance is regarded favorably by Neoliberalism. Regulations and governance are required in an anarchic environment to ensure that state action does not endanger each other (Navari,2013).

Tanja Borzel emphasized the significance of combining international, state, and non-state organizations in the formation of regional governance. International organizations are concerned with actors who develop regional policies, boost economic growth, and develop technology, including the reduction of transaction costs, as well as actors of integration in the socioeconomic field of politics (Borzel,2016:88). International organizations serve as a forum for convening and facilitating each country's national interests. Furthermore, international organizations have the authority to create and enforce their own rules (Archer,2001:93–100). At the regional level, the state represents its domestic interests (Borzel,2016:90). What is the purpose of a regional organization? This reason is inextricably linked to

the numerous state interests that can be obtained through multilateral cooperation mechanisms. At the regional level, states join an international institution to achieve national interests that would be impossible to achieve bilaterally (Navari,2013:44–45). States' interests differ from one another. As a result, in regional governance, the state serves as a gatekeeper, gathering each of its domestic preferences to be pursued at the regional level (Hofman and Merand,2012:141; Morgado,2023:272).

Non-state actors such as civil society, scholars, or businesses are the third pillar and one of the central actors in regional governance (Jakobi,2016:74–75). Non-state actors are important in developing regional governance because they operate at the micro-level, implement state policies, and are intimately familiar with the social conditions of the community (Borzel, 2016:94). Non-state actors play at least four important roles in the concept of regional governance: as part of public regulations, advocacy, regulatory partners, and delegation. Non-state actors can build state-private cooperation to prepare public regulations at the first level. Second, non-state actors serve as state consultants in preparing regional governance for collaboration. Non-state actors act as government partners at the third level by identifying community issues that must be resolved within a governance framework. Finally, non-state actors can be included in the delegation. This final function describes community-level efforts to socialize and raise awareness of regional governance (Jakobi,2016:74–76).

4. Southeast Asia's Cybersecurity Governance Development Timeline

The development of cyber security governance in Southeast Asia is interesting to observe. The authors has compiled the chronicle of cyber security issues in Southeast Asia. The timeline can be seen below:

Table (1): The Chronicle of Cybersecurity Issues in Southeast Asia

Years	Timeline Keywords	Definition
1996	The adoption of technology.	ASEAN member countries agreed in 1996, at the start of its development, that the internet could be a driving force for business growth, information exchange, and cultural exchange. This realization emerged in the mid-1990s, as the internet phenomenon gradually grew to become the primary medium of global information exchange (Noor,2020:108–12).
2003	Singapore Declaration 2003.	Further review uncovers that ASEAN has already issued the Singapore Declaration 2003. This declaration encourages Southeast Asian countries to establish Computer Emergency Response Teams (CERT). A non-governmental organization tasked with recovering from cyber-attack incidents and monitoring internet traffic. The goal of establishing CERT is to

		monitor and inform the government about cyber attacks that pose a threat to their country (Noor,2015:154). CERTs are already in place in nine ASEAN countries. These nine countries are also members of the organization Asia Pacific Computer Emergency Response Teams (APCERT) (Krisman,2013:43).
2004	UNGGE Drafting	UN Group of Governmental Experts (UNGGE), the UN began drafting the development in the Field of Information and Telecommunication in the Context of International Security in early 2004 At least two ASEAN countries have joined the group, Malaysia in 2004 and 2014, and Indonesia in 2012 and 2016 (Noor,2020:108–12).
2006	ARF Join Statement	In response to the formation of the UNGGE, ASEAN issued a joint statement in 2006 through the ASEAN Regional Forum (ARF) titled Cooperation in Combating Cyber Attacks and Terrorist Misuse of Cyberspace (Nasu,2019: 144).
2010	ARF's Cooperation in Ensuring Cyber Security.	ASEAN is committing to strengthening national and regional governance rules to prevent the use of the internet for criminal purposes through this statement. This ARF vision and mission were put into action at the following ARF meeting in 2010. The ARF stated Cooperation in Ensuring Cyber Security at this meeting (Nasu,2019:144).
2015	ASEAN ICT Masterplan 2012 in ASEAN Economic Community.	ASEAN adopted Cooperation in Ensuring Cyber Security as one of the main pillars in the preparation of the ASEAN ICT Masterplan to support the ASEAN Economic Community's integration in 2015 (Ramadhan,2017:550).

Regarding cybersecurity legislation in domestic level, ten ASEAN member countries already have electronic transaction protection legislation in place. In addition, eight ASEAN member countries have legal cyber security regulations (Noor,2015:155). ASEAN has organized a number of seminars and working groups with state actors from outside the Southeast Asian region in order to narrow the technological gap between its member countries. ASEAN-China cooperation in combating non-traditional threats, ASEAN-Japan cooperation in combating terrorism and transnational crime, and ASEAN-European Union cooperation in achieving security and stability in the Asia Pacific region are just a few examples (Manopo and Sari,2015: 45–46). Despite numerous initiatives to create a cyber-secure Southeast Asian region, ASEAN does not yet have standard rules that each member country can follow. Dr. Yacoob Ibrahim, Singapore's Minister of Communication and Technology, stated at the ASEAN Ministerial Meeting on Cybersecurity (AMMC) that this region requires adaptable cyber security norms and regulations that are in line with the interests of the country members. This issue arose as a result of ASEAN member countries'

disagreement in adopting the UNGGE text. Indeed, ASEAN is having difficulty reconciling the interests of its member countries in recognizing the economic, political, and social benefits of cybersecurity in Southeast Asia (Tran Dai and Gomez,2018:1–2).

5. Discussion

When it comes to achieving cybersecurity governance in Southeast Asia, the participation of state actors is critical. However, there are differences in how each country implements and views the phenomenon of cyber security. Singapore, for example, is a well-established country in terms of cybersecurity maturity. The country has set aside at least 38 million dollars to establish a National Cyber Threat Monitoring Center, a Cyber Security Agency, and funding for the Singapore Defense Cyber Organization (Aljunied,2020:6). Singapore is an active participant in raising cybersecurity awareness. His initiative to establish the ASEAN-Singapore Cybersecurity Center of Excellence (ASCCE) is one of his contributions. The initiative aims to bridge the technological gap, raise cybersecurity awareness among ASEAN member states, and position Singapore as the initiative's leader (Salsabila and et al,2020:5; Anshori and Ramadhan,2019:44–46).

Meanwhile, the Malaysian government is concerned with five issues: policy enforcement, economic effects, challenges, technological development, and modern threats (Oktaviani and Silvia,2021:76). Malaysia's government believes that the country requires a firm policy to combat cyber threats. They see the potential for cyber threats to disrupt economic interests. Because this issue cannot be separated from sophisticated cyber threats, state expertise in developing appropriate technology is required. As a result, the state is responsible for ensuring the security of its information technology (Oktaviani and Silvia,2021:76–78). Other empirical examples can be found in the Indonesian government's policies. In Indonesia, unlike Singapore and Malaysia, cybersecurity policies are still centered on specific ministries or government agencies. For example, the State Intelligence Agency has authority over cybersecurity counterintelligence (Yusuf,2022: 23). The Ministry of Defense of the Republic of Indonesia is in charge of cyber security issues related to national defense (Wahyuni and et al,2021: 514). Meanwhile, the Ministry of Technology and Information, the National Cyber and Crypto Agency, and the Indonesian *National Police* are in charge

of public cybersecurity and cybercrime issues (Wahyuni and et al,2021: 513–14).

From the standpoint of cyber security, ASEAN countries must base their participation in preparing cyber security governance on two factors. First, because cyber threats have the potential to endanger public safety, they must be mitigated. Second, cyber threats can jeopardize political stability, the economy, and the security of critical infrastructure (Farid and Adhisty,2019: 76). As a result, countries in Southeast Asia must prioritize cybersecurity governance in critical sectors such as banking, health, and critical infrastructure (Zahiroh,2020:55; Wilner and et al,2022:525; Heinl,2014: 136). One industry that is frequently targeted by cyberattacks is banking. Countries must ensure that their cybersecurity governance safeguards their citizens' critical data. Because financial data is extremely vulnerable to being traded, there must be governance in place to reduce cybercrime (Zahiroh,2020:55).

The state must pay attention to the health industry because cyberattacks have targeted it as a target. The Wannacry Ransomware, for example, afflicts patient data in hospitals in Singapore, Malaysia, Indonesia, and the Philippines (Chang,2017). In addition to patient data being vulnerable to identity theft, modern medical equipment is linked to the internet. As a result, if a medical device has a flaw, attackers can exploit it to sabotage it and endanger the patient's life (Wilner and et al,2022:525). Meanwhile, almost all industries have integrated their critical infrastructure systems into the internet. One of them is the oil and gas industry, which uses cloud computing to integrate exploration, exploitation, and production technology with the internet (Progoulakis and et al,2021:2–3). On the one hand, the *ASEAN* Trans Pipeline involves several ASEAN member countries. A project that integrates gas pipelines to meet the energy needs of the community. However, ASEAN lacks a consistent policy for protecting its critical infrastructure. On the other side, every human being requires energy (Borelli,2017:18). ASEAN countries' participation in the preparation of cybersecurity governance must cover the essential and critical dimensions of their social lives.

Several other empirical examples of how the state produces cyber security governance in Southeast Asia have been identified by researchers. Thailand established the ASEAN-Japan Cybersecurity Capacity Building Centre to promote constructive cooperation between ASEAN and Japan. This

collaboration aims to improve cyber security capacity through training for IT operators working in critical infrastructure, strengthening cooperation among government agencies, raising information security awareness, protecting personal data, and encouraging information sharing (ASEAN, 2019). Malaysia's government is strengthening cyber security capacity through the Malaysia Cybersecurity Strategy 2020-2024, which involves the United Nations (UN) as a global organization and ASEAN as a regional body (National Security Council,2020). Furthermore, the Singapore government has set aside 30 million Singapore dollars to support the ASEAN-Singapore Cybersecurity Centre of Excellence. Singapore is driving cyber security capacity building with three goals in mind: coordinating training and research, training CERT human resources in ASEAN countries, and encouraging information exchange among CERTs (CCDCOE,2022).

In practice, non-state actors can help to develop this governance from the ground up. This reason is inextricably linked to the increasing fluidity of interactions among state actors, non-state actors, and international organizations (Manley,2015:86). Non-state actors can thus interact with both the community and the state. Non-state actors, such as businesses, activist institutions, community organizations, and academics, value flexibility differently than the flow of state interactions, which is rife with bureaucratic elements. Non-state actors, for example, can be involved in the preparation of cybersecurity governance in Southeast Asia in the areas of awareness building, consultation, and policy advocates (Jakobi,2016:73; Willi and et al,2018:781). Non-state actors can play an important role in the preparation of consultations that are closely related to the community. At this point, the state can work with non-state actors like CERT to gather information about cybersecurity mapping, mitigation, and monitoring (Krisman,2013:43). Although each ASEAN CERT has its own perspective on cyber threats, the potential threats that countries face are similar. Phishing, hacking, banking data theft, Distributed Denial of Service (DDoS), ransomware, and cyber terrorism are all potential threats to Southeast Asia's stability (Mizan and et al,2019:113–14). Non-state actors, such as businesses or industries, typically use sophisticated technology and have direct contact with the community. As a result, they can provide an overview of the community's micro circumstance as well as any cyber

threats that have the potential to disrupt the country's economic condition (Guarda,2015:24).

Several more empirical studies demonstrate how non-state actors, particularly critical infrastructure, can contribute to cyber security governance advocacy. Critical infrastructure industries are generally the national backbone. Banking, energy, and health are examples (Maglaras and et al,2022; Baggott and Santos,2020; Gioulekas and et al,2022). In this case, the banking industry can be a good example. In the banking industry, all business processes have been digitized. As a result, the banking industry can play an important role in preparing governance and raising cybersecurity awareness. One of them is raising awareness about the importance of keeping confidential banking data, which is frequently used in digital transactions (Zahiroh,2020:55). On the other hand, energy-related enterprises can advise state actors on how to maintain the electric power network, which serves to provide housing and industry. Kraus underlined that industrial control systems (ICS) monitor the distribution of electricity flows, which are vulnerable to cyber attacks (Krause and et al,2021:1–3). Gioulekas' research in the health sector reveals that the health sector is similarly vulnerable to cyber-attacks. According to the research, around 27% of healthcare facilities in the European Union were subjected to cyberattacks in 2018 (Gioulekas and et al,2022:2). It is consistent with actual evidence from ASEAN, which shows that around 61% of Malaysia's health industry has been subjected to cyber attacks (Chandra,2021). Meanwhile, INTERPOL data suggests that in 2018, about 1.5 million SingHealth data files were successfully compromised using ransomware (INTERPOL 2020). Based on the empirical facts presented above, the health sector can advise state actors on how to limit cyber dangers in the protection of medical record data and internet-connected equipment.

ASEAN's main concern is the enormous technology disparity between its member countries. According to data issued by SEON, a technology business in Hungary, the Southeast Asian countries with the lowest degree of cyber security are Myanmar and Cambodia. On a scale of 1 to 10, Myanmar earned 2.5 points while Cambodia received 2.75 (Varga,2020). This data is related to the International Telecommunication Union (ITU) data published in 2018, which shows Laos (0.195), Myanmar (0.172), and Cambodia (0.161) as Southeast Asia countries with the lowest level of cyber maturity (ITU 2018). Another difficulty that ASEAN faces is the high level

of rivalry among its member countries. As a result, ASEAN will require assistance in reaching a consensus on implementing cyber security governance (Manopo and Sari,2015:45). ASEAN's efforts to reach this consensus are additionally hampered by consensus rules that differ from European Union voting procedures. Some critics argue that ASEAN accords are hampered by consensus because it is non-binding and tends to be flexible (Gerard,2018:211). It differs from the approach of the European Union, which is more binding and strict (Holzleitner and Reichl,2017:2). Agreements established by agreement at the ASEAN level are generally meant to meet all of the member nations' interests (Suzuki,2021:8).

Despite its shortcomings, ASEAN has an institutional advantage in forging a regional governance agreement that governs cybersecurity issues. The organization is frequently chastised for its haphazard policy outcomes. Since this issue is inextricably tied to ASEAN's consensus method, the policy appears to be informal and intermittent (Gerard,2018:211). However, following the 2008 ASEAN Declaration, this organization adopted a more formal consensus method based on the formulas "ASEAN Minus X" and "ASEAN X+2" (Feraru,2016:29). Any governance prepared by ASEAN can be implemented using this formula if two countries agree on the policy. Countries that have not been able to implement such governance can do so when they are ready in terms of politics, economics, and security (Feraru, 2016:29). Given the high technological disparity among its member countries, ASEAN needs to strengthen the formula for cyber security governance through consultation and assistance. As a result, regional consultation programs, capacity building for cybersecurity maturity, and strategic information technology cooperation must be prioritized in order for governance implementation to be successful (Watanabe,2020:106).

Another important point for ASEAN to remember is that the organization must provide equal access to participation in governance arrangements for both state and non-state actors (Willi and et al,2018:781). State and non-state actors have distinct roles to play in developing cyber security governance. In this regard, ASEAN sees itself as a socialization agent, an aggregator of interests, and a policy implementer (Archer,2001:100–102). Another aspect that should not be overlooked is that the organization's fundamental norms must serve as the foundation for determining governance. According to Amitav Acharya, institutionalized norms and ideas become the foundation of an organization when responding to issues

outside its scope (Acharya,2012:195). The principle of non-intervention was established as ASEAN's fundamental norm in the Treaty of Amity and Cooperation (TAC) in 1976. Thus, regional cyber security governance must respect sovereign rights of states, refrain from interfering in domestic affairs, and promote solidarity and harmony among ASEAN member countries (Manopo and Sari,2015:46).

So, how will ASEAN establish inclusive governance? The ARF (ASEAN Regional Forum) is an internal ASEAN institution that strives to synergize the interests of its member countries in inclusive governance, according to the ASEAN Cybersecurity Cooperation Strategy 2021-2025 whitepaper. In an effort to accelerate confidence in cyberspace, ASEAN must ensure that every citizen and businessperson in Southeast Asia has access to the digital world. Furthermore, ASEAN shall promote the rapid development of infrastructure and human resources in Southeast Asia with the objective to attain technical equality (ASEAN,2021a). Furthermore, the ARF in this document must promote inclusivity in elements of technological development by fostering dialogue collaboration with ASEAN cooperation partners (ASEAN,2021a). According to researchers, implementing inclusive governance can be successful if ASEAN attempts to bridge the region's technical gap. According to the researchers, establishing inclusive governance must rely on ASEAN norms. Until date, ASEAN has relied on the Treaty of Amity and Cooperation (TAC) rules to achieve policy consensus. Article 2 of the TAC states that ASEAN member countries recognize each country's integrity and sovereignty, the peaceful resolution of conflicts, and practical collaboration in each ASEAN member country (ASEAN,2018). It corresponds with the preamble to the 2008 ASEAN Charter, which explicitly states that ASEAN member countries must adhere to the TAC's principles, achieve consensus, resolve problems peacefully and nonviolently, and commit to achieving a safe regional area through the stability of the political-security, economic, and socio-cultural pillars (ASEAN,2008). Researchers conclude that establishing inclusive governance is possible if ASEAN depends on TAC standards and the ASEAN Charter in forming a secure cyberspace.

6. Conclusion

State actors, non-state actors, and international organizations must all be involved in cyber security governance. The cross-actor collaboration is significant because the three actors each have their own function in the

conceptual framework of regional governance. Given the current situation in Southeast Asia, which lacks cyber security governance, developing these regulations is a must. Whether or not this governance is effective in the future, the Southeast Asian region requires consistent governance in regulating behavior and protecting the country's interests in cyberspace. This cyber issue, like non-traditional threats such as narcotics or human trafficking, needs to be formally institutionalized by ASEAN in order to improve cyberspace in Southeast Asia. In practice, this research can help ASEAN work with all stakeholders, including both state and non-state entities. It must be separate from the roles of the state and industry, each of which serves a purpose.

7. Acknowledgment

The authors would like to express a gratitude to the Faculty of Politics and Social Sciences in Universitas Padjadjaran and International Relations Department in Universitas Pertamina for supporting this article. We also would like to thank to the Geopolitics Quaterly editorial team for their constructive comments and advice for this paper.

References

1. Acharya, A (2012). "Ideas, Norms, and Regional Orders." In International Relations Theory and Regional Transformation, edited by T V Paul, 210–32. United Kingdom: Cambridge University Press.
2. Alhammadi, A (2022). "The Neorealism and Neoliberalism behind International Relations during Covid-19." World Affairs 185 (1): 147–75. https://doi.org/10.1177/00438200211065128.
3. Aljunied, S.M.A (2020). "The Securitization of Cyberspace Governance in Singapore." Asian Security 16 (3): 343–62. https://doi.org/10.1080/ 14799 855.2019.1687444.
4. Anshori, M.F; Ananda Ramadhan, R (2019). "Kepentingan Singapura Pada Keamanan Siber Di Asia Tenggara Dalam Singapore International Cyber Week." Padjadjaran Journal of International Relations 1 (1): 39. https://doi.org/10.24198/padjir.v1i1.21591.
5. Archer, C (2001). International Organizations. 3rd ed. London: Routledge.
6. ASEAN-UP. 2019. "Overview of E-Commerce in Southeast Asia [Market Analysis]." 2019. https://aseanup.com/overview-of-e-commerce-in-southeast-asia./
7. ASEAN. (2008). "ASEAN Charter." 2008. https://asean.org/wp-content/uploads/images/archive/publications/ASEAN-Charter.pdf.
8. ———(2018)." Treaty of Amity and Cooperation." 2018. https://asean-aipr.org/wp-content/uploads/2018/07/Treaty-of-Amity-and-Cooperation-in-Southeast-Asia-1976-TAC.pdf.
9. ———(2019)." The ASEAN-Japan Cybersecurity Capacity Building Centre (AJCC BC)." 2019. https://asean2019.go.th/en/infographic/the-asean-japan-cybersecurity-capacity-building-centre-ajcc-bc./
10. ——— (2021a). "ASEAN Cybersecurity Cooperation Strategy." ASEAN.
11. ——— (2021b). "ASEAN LEADERS' STATEMENT ON CYBER-SECURITY COOPERATION." 2021. http://setnas-asean.id/site/ uploads/document/document/5b04cdc25d192-asean-leaders-statement-on-cybersecurity-cooperation.pdf.
12. Baggott, S.S; Joost, R.S (2020). "A Risk Analysis Framework for Cyber Security and Critical Infrastructure Protection of the U.S. Electric Power Grid." Risk Analysis 40 (9): 1744–61. https://doi.org/10.1111/risa.13511.
13. Borelli, M (2017). "ASEAN Counter - Terrorism Weaknesses." International Centre for Political Violence and Terrorism Research 9 (9): 14–20.
14. Borzel, T (2016). "Theorizing Regionalism: Cooperation, Integration, and Governance." In The Oxford Handbook of Comparative Regionalism, edited by Tanja A Borzel and Thomas Risse. United Kingdom: Oxford University Press.
15. Buzan, B; Weaver, O; Wilde, J.D (1998). Security: A New Framework of

Analysis. Colorado: Lynne Rienner.
16. Cavelty, M.D; Egloff, F.J (2019). "The Politics of Cybersecurity: Balancing Different Roles of the State." St Antony's International Review 15 (1): 37–57.
17. CCDCOE (2022). "ASEAN Cyber Developments: Centre of Excellence for Singapore, Cybercrime Convention for the Philippines, and an Open-Ended Working Group for Everyone." 2022. https://ccdcoe.org/incyder-articles/asean-cyber-developments-centre-of-excellence-for-singapore-cybercrime-convention-for-the-philippines-and-an-open-ended-working-group-for-everyone./
18. Chandra, G.N (2021). "Indonesia at Highest Risk Level of Cyber Threat: TrendMicro." Jakarta Globe. 2021. https://jakartaglobe.id/tech/indonesia-at-highest-risk-level-of-cyber-threat-trendmicro.
19. Chang, L (2017). "Cyber Crime and Cybersecurity in ASEAN." 2017. https://www.researchgate.net/publication/318474107.
20. Creswell, J (2014). Research Design: Qualitative, Quantitative and Mixed Methods Approaches (4th Eds). London: SAGE.
21. ——— (2015). Reserach Design: Qualitative, Quantitatve and Mix Methods Design (5th Eds). 5th ed. London: SAGE.
22. Düll, A; Schoch, A; Straub, M (2018). "Cybersecurity in the European Union." Central and Eastern European EDem and EGov Days 331: 313–23. https://doi.org/10.24989/ocg.v331.26.
23. Dunn-Cavelty, M (2010). "Cyber-Threats." In The Routledge Handbook of Security Studies, edited by Myriam Dunn-Cavelty and Victor Mauer, 180–89. New York: Rouledge.
24. E-Trade for All (2018). "ASEAN: E-Commerce Set to Dominate the Region in 2019." 2018. https://etradeforall.org/asean-e-commerce-set-to-dominate-the-region-in-2019./
25. Eggenschwiler, J (2020). "Expert Commissions and Norms of Responsible Behaviour in Cyberspace: A Review of the Activities of the GCSC." Digital Policy, Regulation and Governance 22 (2): 93–107. https://doi.org/10.1108/DPRG-03-2019-0019.
26. Farid, M; Adhisty, A.A (2019). "State Action as an Individual Security Threat in Case of Cybercrime Securitization." Jurnal Pertahanan 5 (3): 77. https://doi.org/10.33172/jp.v5i3.589.
27. Feng, J (2018). "On The Cusp." 2018. https://www.imf.org/external/pubs/ft/fandd/2018/09/pdf/aseandigital-economy-infographic-feng.pdf.
28. Feraru, A.S (2016). "ASEAN Decision-Making Process: Before and after the ASEAN Charter." Asian Development Policy Review 4 (1): 26–41. https://doi.org/10.18488/journal.107/2016.4.1/107.1.26.41.

29. Foque, R; Steenbergen, J (2005). "Regionalism: A Constitutional Framework for Global Challenges." In Global Politics of Regionalism: Theory and Practice, edited by Mary Farrell, Bjorn Hettne, and Luk Van Langenhove. London: Pluto Press.
30. Gerard, K (2018). "ASEAN as a 'Rules-Based Community': Business as Usual." Asian Studies Review 42 (2): 210–28. https://doi.org/10.1080/10357823.2018.1444016.
31. Gioulekas, F; Stamatiadis, E; Tzikas, A; Gounaris, K; Georgiadou, A; Michalitsi-Psarrou, A; Doukas, G; et al (2022). "A Cybersecurity Culture Survey Targeting Healthcare Critical Infrastructures." Healthcare 10: 1–19.
32. Guarda, N.D (2015). "Governing the Ungovernable: International Relations, Transnational Cybercrime Law, and the Post-Westphalian Regulatory State." Transnational Legal Theory 6 (1): 211–49. https://doi.org/10.1080/20414005.2015.1042226.
33. Gultom, R.A.G; Supriyadi, A.A; Kustana, T (2018). "A Strengthening Asean Cyber Cooperation in Countering Cyber Terrorist Groups Activities on the Internet by Implementing the Six-Ware Cyber Security Framework." International Journal of Management & Information Technology 13: 3288–3300. https://doi.org/10.24297/ijmit.v13i0.7624.
34. Harper, N; Tempra, N (2020). "Drug Trafficking in the Golden Triangle: The Myanmar Problem and ASEAN Effectiveness." Jurnal Sentris 1 (1): 116–24. https://doi.org/10.26593/sentris.v1i1.4171.116-124.
35. Heinl, C.H (2014). "Regional Cybersecurity: Moving Toward a Resilient ASEAN Cybersecurity Regime." Asia Policy 18 (1): 131–59. https://doi.org/10.1353/asp.2014.0026.
36. Hofman, S.C; Merand, F (2012). "Regional Organization a La Carte: The Effects of Institutional Elasticity." In International Relations Theory and Regional Transformation, edited by T V Paul, 133–57. United Kingdom: Cambridge University Press.
37. Holzleitner, M.T; Reichl, J (2017). "European Provisions for Cyber Security in the Smart Grid – an Overview of the NIS-Directive." Elektrotechnik Und Informationstechnik 134 (1): 14–18. https://doi.org/10.1007/s00502-017-0473-7.
38. IBM Security (2019). "Cost of Data Breach Record".
39. INTERPOL (2020). "ASEAN Cyberthreat Assessment 2020".
40. ITU. (2018). "Global Cybersecurity Index 2018." https://www.itu.int/dms_pub/itu-d/opb/str/D-STR-GCI.01-2018-PDF-E.pdf.
41. Jakobi, A.P (2016). "Non-State Actors and Global Crime Governance: Explaining the Variance of Public-Private Interaction." British Journal of Politics and International Relations 18 (1): 72–89. https://doi.org/ 10.1111/1467-856X.12064.

42. Kassab, H.S (2014). "In Search of Cyber Stability: International Relations, Mutually Assured Destruction and the Age of Cyber Warfare." In Cyberspace and International Relations: Theory, Prospects and Challenges, edited by Jan-Frederik Kremer and B Muller, 59–76. Bonn: Springer.
43. Kausch, K (2017). "Cheap Havoc: How Cyber-Geopolitics Will Destabilize the Middle East." United States.
44. Krause, T; Ernst, R; Klaer, B; Hacker, I; Henze, M (2021). "Cybersecurity in Power Grids: Challenges and Opportunities." Sensors 21 (18): 1–19. https://doi.org/10.3390/s21186225.
45. Krisman, K (2013). "A Secure Connection: Finding the Form of ASEAN Cyber Security Cooperation." JAS (Journal of ASEAN Studies) 1 (1): 41. https://doi.org/10.21512/jas.v1i1.60.
46. Lacy, M; Prince, D (2018). "Securitization and the Global Politics of Cybersecurity." Global Discourse 8 (1): 1–16. https://doi.org/https://doi.org/10.1080/23269995.2017.1415082.
47. Maglaras, L; Janicke, H; Ferrag, M.A (2022). "Cybersecurity of Critical Infrastructures: Challenges and Solutions." Sensors 22 (14): 2–5. https://doi.org/10.3390/s22145105.
48. Manley, M (2015). "Cyberspace's Dynamic Duo: Forging a Cybersecurity Public-Private Partnership." Journal of Strategic Security 8 (5): 85–98. https://doi.org/10.5038/1944-0472.8.3S.1478.
49. Manopo, B.Y.W; Sari, D.A.A (2015). "Asean Regional Forum: Realizing Regional Cyber Security in Asean Region." Belli Ac Pacis 1 (1): 44–51. https://jurnal.uns.ac.id/belli/article/view/27366.
50. McAfee. (2014). "The Economic Impact of Cybercrime and Cyber Espionage." California.
51. Mizan, N.S.M; Ma'arif, M.Y; Mohd Satar, N.S; Shahar, S.M (2019). "CNDS-Cybersecurity: Issues and Challenges in ASEAN Countries." International Journal of Advanced Trends in Computer Science and Engineering 8 (October): 113–19. https://doi.org/https://doi.org/ 10.30534/ijatcse/2019/1781.42019.
52. Mok, Sh.Y (2020). "ASEAN and Transnational Crime: Gains and Challenges in Tackling Drug Trafficking." Wimaya 1 (01): 31–38. https://doi.org/10.33005/wimaya.v1i01.13.
53. Morgado, N (2023). "How Can Geopolitical Agents Restrain an Emerging Power's Global and Regional Leadership? Evidence from Brazil." Geopolitics Quarterly 18 (68): 268–98.
54. Nagyfejeo, E (2021). "EU's Emerging Strategic Cyber Culture(S)." Policing: A Journal of Policy and Practice 15 (1): 79–102. https://doi.org/ 10.1093/police/pay092.

55. Nasu, H (2019). The Legal of Authority of ASEAN as Security Institution. England: Cambridge.
56. National Security Council (2020). "Malaysia Cyber Security Strategy 2020-2024." Putrajaya.
57. Navari, C (2013). "Liberalism." In Security Studies: An Introduction, edited by Paul Williams, 2nd ed., 32–47. New York: Routledge.
58. Nengsi, F (2019). "The Women's Participation in Digital Economy in ASEAN." Journal of Islamic World and Politics 3 (1): 516–36. https://doi.org/10.18196/jiwp.3128.
59. Noor, E (2015). "Strategic Governance of Cyber Security : Implications for East Asia." In Navigating Change: ASEAN-Japan Strategic Partnership in East Asia and in Global Governance, edited by Rizal Sukma and Y Soeya, 150–63. Japan: JCIE.
60. ———(2020)." Positioning ASEAN in Cyberspace." Asia Policy 15 (2): 107–14. http://asiapolicy.nbr.org.
61. Nye Jr, J (2011). The Future of Power. New York: Perseus Group.
62. Oktaviani, P.B; Silvia, A (2021). "Strategi Keamanan Siber Malaysia." Jurnal Kajian Ilmiah 21 (1): 69–84. https://doi.org/10.31599/jki.v21i1.447.
63. Papp, Daniel S, and D Albert. 2001. Information Age: Anthology (Eds). USA: CCRP.
64. Progoulakis, I; Nikitakos, N; Rohmeyer, P; Bunin, B; Dalaklis, D; Karamperidis, S (2021). "Perspectives on Cyber Security for Offshore Oil and Gas Assets." Journal of Marine Science and Engineering 9 (2): 1–27. https://doi.org/10.3390/jmse9020112.
65. Radu, R (2015). "Power Technology and Powerful Technologies: Global Governmentality and Security in the Cyberspace." In Cyberspace and International Relations: Theory, Prospects and Challenges, edited by Jan Frederik Kremer and Benedikt Muller, 3–20. Bonn: Springer.
66. Ramadhan, I (2017). "Peran Institusi Internasional Dalam." Populis 2 (4): 495–508.
67. ———(2020)." Cyber-Terrorism in the Context of Proselytizing, Coordination, Security, and Mobility." Islamic World and Politics 4 (2): 185–203. https://doi.org/10.18196/jiwp.4252.
68. Ritchie, J; Spencer, L (2002). "Qualitative Data Analysis for Applied Policy Research." In Analyzing Qualitative Data, edited by Alan Bryman and Robert G Burgess, 173–94. London: Routledge.
69. Roselle, L; Spray, Sh (2012). Research and Writing in International Relations. Boston: Pearson Longman.
70. Salsabila, A.S; Fikri, M.D; Andika, M.S; Harahap, N.A (2020). "Potential and Threat Analysis towards Cybersecurity in South East Asia." Journal of ASEAN Dynamics and Beyond 1 (1): 1–12.

71. Snyder, H (2019). "Literature Review as a Research Methodology: An Overview and Guidelines." Journal of Business Research 104 (August): 333–39. https://doi.org/10.1016/j.jbusres.2019.07.039.
72. Soderbaum, F (2016). "Old, New, and Comparative Regionalism: The History and Scholarly Development of the Field." In The Oxford Handbook of Comparative Regionalism, edited by Tanja A Borzel and Thomas Risse. United Kingdom: Oxford University Press.
73. Subono, N.I; Kosandi, M (2019). "The Regionalism Paradox in the Fight against Human Trafficking: Indonesia and the Limits of Regional Cooperation in ASEAN." Journal of Leadership, Accountability and Ethics 16 (2): 89–98.
74. Sudirman, A; Sari, D.S (2017). "Membangun Keamanan Regional Di Asean Dalam Menanggulangi Ancaman Terorisme." Jurnal Wacana Politik 2 (1): 22–32. https://doi.org/10.24198/jwp.v2i1.11276.
75. Suzuki, S (2021). "Can ASEAN Offer a Useful Model? Chairmanship in Decision-Making by Consensus." Pacific Review 34 (5): 697–723. https://doi.org/10.1080/09512748.2020.1727553.
76. Tanczer, L.M; Brass, I; Carr, M (2018). "CSIRTs and Global Cybersecurity: How Technical Experts Support Science Diplomacy." Global Policy 9 (November): 60–66. https://doi.org/10.1111/1758-5899.12625.
77. Tran Dai, C; Gomez, M.A (2018). "Challenges and Opportunities for Cyber Norms in ASEAN." Journal of Cyber Policy 3 (2): 217–35. https://doi.org/10.1080/23738871.2018.1487987.
78. Varga, G (2020). "Global Cybercrime Report: Which Countries Are Most at Risk?" 2020. https://seon.io/resources/global-cybercrime-report./
79. Veicy, H (2022). "The Policies of Russian Regionalism and the Eurasian Economic Union." Geopolitics Quarterly 18 (68): 2023–2177.
80. Velasco, J.Ch (2022). "Sino-ASEAN Geopolitical Relations through International Student Mobility: Manifestations of Soft Power through Education." Geopolitics Quarterly 18 (68): 412–29.
81. Wahyuni, R.A.E; Waluyo, S.D; Simatupang, H (2021). "STRENGTHENING THE CYBER DEFENSE CENTER OF THE MINISTRY OF DEFENCE OF THE REPUBLIC OF INDONESIA (PUSDATIN KEMHAN) TO SUPPORT THE INDONESIAN DEFENSE DIPLOMACY IN CYBER DEFENSE SECURITY COOPERATION IN ASEAN." Jurnal Pertahanan 7 (3): 511–25.
82. Watanabe, S (2020). "Strategic Analysis of Capacity Building for the Cyber Security of the United States in Asia." Jurnal Asia Pacific Studies 4 (2): 100–111. https://doi.org/10.33541/japs.v4i2.2800.

83. Willi, Y; Pütz, M; Müller, M (2018). "Towards a Versatile and Multidimensional Framework to Analyse Regional Governance." Environment and Planning C: Politics and Space 36 (5): 775–95. https://doi.org/10.1177/2399654418760859.
84. Wilner, A.S; Luce, H; Ouellet, E; Williams, O; Costa, N (2022). "From Public Health to Cyber Hygiene: Cybersecurity and Canada's Healthcare Sector." International Journal 76 (4): 522–43. https://doi.org/10.1177/00207020211067946.
85. Yadav, H; Gour, Sh (2014). "Cyber Attacks: An Impact on Economy to an Organization." International Journal of Information & Computation Technology 4 (9): 937–40.
86. Yazid, S; Septiyana, I (2019). "The Prospect of ASEAN Migration Governance." Journal of Indonesian Social Sciences and Humanities 9 (2): 95–112. https://doi.org/10.14203/jissh.v9i2.155.
87. Yuniar, R.W (2017). "Uber Rival Grab Rolls Out Indonesia Investment Plan." 2017. https://www.wsj.com/articles/uber-rival-grabtaxi-rolls-out-indonesia-investment-plan-1486012764.
88. Yusuf, M.S (2022). "Optimalisasi Layanan Publik Badan Intelijen Negara Dalam Perspektif Global Cybersecurity Index." Al Ulum Jurnal Sains Dan Teknologi 7 (1): 21–26. https://doi.org/10.31602/ajst.v7i1.5643.
89. Zahiroh, M.Y (2020). "Cybersecurity Awareness and Digital Skills on Readiness for Change in Digital Banking." Li Falah: Jurnal Studi Ekonomi Dan Bisnis Islam 5 (2): 53. https://doi.org/10.31332/lifalah.v5i2.2271.