Journal of Social Studies (JSS), ISSN: 1858-2656 (p); 2721-4036 (e)
Vol. 18. No. 1 (2022), pp.1-26 doi: 10.21831/jss.v18i1.39637. 1-26

Cyber resilience revisited: Law and international relations

Ika Riswanti Putranti
Universitas Diponegoro, Indonesia
Email: ikariswantiputranti@lecturer.undip.ac.id

Marten Hanura
Universitas Diponegoro, Indonesia
Email: martenhanura@lecturer.undip.ac.id

Safrida Alivia Sri Ananda
Universitas Diponegoro, Indonesia
Email: safridasriyono@gmail.com

Gawinda Nura Nabila
Universitas Diponegoro, Indonesia
Email: windarnbl@gmail.com

Abstract

Cyber space is increasingly playing an important role in the global world, affecting the pattern of relations between countries. The issue of non-traditional security threats is shifting towards the threat typology associated with cyber space. The concept of national security began to be complemented by a national cyber security strategy to support the security of its national interests. Where the country needs to ensure the security of cyber ecosystems to maintain national economic stability. The large flow data and information increasingly large and complex, and brings hidden costs in the form of cyber security threats. Cyber security concepts that are considered not responsive and resilient in dealing

with and overcoming cyber attacks can occur at any time with patterns and types that continue to evolve. The concept of cyber security should begin to be developed into cyber security that has patterns of recovery, adaptation, and evolution so as to be able to answer the dynamics of challenges in international trade. Interrupted cyber systems in international sphere will potentially cause disruption of international relations because the threat of losses caused not only affects one country. The increasingly complex international law context and involving big data should be one of the top priorities for cyber resilience strategies. This paper starts by explaining the state of play of cyber resilience in international relations and law. Next, analysis why the concept of cyber resilience in the perspective of international relations and international law needs to be re-visited to face challenges in the digital economy.

Keywords: Cyber Resilience; Cyber Security; International Relations; Law; Digital Economy.

Introduction

In an era of increasingly complex digitalization and the existence of interconnected cyber systems, society is dependent on technology to facilitate their daily life activities. From managing personal finances to controlling critical infrastructures, i.e: air traffic networks; digital information systems and software have been integrated at almost all levels of individual and collective activity (Wall, 2001). Although the form of digital integration and smart automation can facilitate human work to be more effective and efficient, it is also the target of various threats from cyber attacks. Attackers and targets for attacks vary widely, from individuals to international companies and national government agencies. Cyber incidents (attacks or system failures) are inevitable, especially when financial institutions are increasingly digitally interconnected. At the individual level, thousands of private details including personal mastercard information and property are stolen a day . At the enterprise level, hacks targeted at large companies Equifax, Sony Corporation and other similar organizations indicate the vulnerability and potential for hackers to accumulate sensitive information stored in corporate databases or referred to as Big Data apparently has affected the safety of many users (Kott et al, 2019). Thus, risk control and defense efforts against threats, vulnerabilities, and consequences that rely on threat identification— only based on traditional Cyber Security are now no longer sufficient. Departing from this reason, Cyber Resilience refers to the ability of a system to prepare for, respond to, recover, and adapt continuously

to deliver the intended outcome despite adverse cyber events (Kahan et al, 2009; Bodeau et al, 2011). According to The State of Email Security Report 2020 Mimecast, 31% of organizations experienced data loss due to a lack of cyber resilience preparedness (IT Governance UK, 2021). Simply put, cyber resilience helps protect against cyber risks, sustain and limit the severity of attacks, and ensures its continued survival despite an attack. Serious cyber threats involving interstate targets can possibly be addressed through international cooperation (Shad et al, 2018). Therefore, in the evolving nature of cyber threats, new management approaches in international relations and trade law have to be developed involving full range of efforts in building cyber resilience to tackle the dynamic challenges in the international trade system.

Putranti, I.R., (2015) has study regarding Developing of Cyber Resilience System of the International Trade Facilitations: Specific reference Indonesia, in this paper analyzed about the importance to developing the cyber resilience in trade facilitation coping with the challenge of Mega FTA. The digitalization of trade facilitation demanding secure hub and the mature awareness of cyber resilience both of government agency and economic operators. Putranti, I.R. et.al (2020) study on *Cyber Resilience of Small and Medium Enterprises in Semarang City*, analyzed cyber resilience of small and medium enterprises of handicraft under the scheme of Semarang City smart economy platform. The findings that most of the enterprises are not well prepared for the cyber system and has less ability to employ the facilities provided by the government. In the other hand, the government need to provided adequate governance and legal framework to provide secure environment that supports the development of cyber resilience in smart public services. Putranti, I.R. et.al (2020), study Smartcity : Model Ketahanan Siber Untuk Usaha Kecil Dan Menengah, where this article seeks the model of cyber resilience for Small and Medium enterprise with SMEs were have a very limited in access to the development of networks and resources coping with the issues of cyber threat and cyber resilience. This paper seek to examine the state of play of cyber resilience in international relations and law, where the concept of cyber resilience needs to be revisited to face challenges in the digital economy.

Methods

This paper is a descriptive qualitative type of research paper under the paradigm of law and international relations. This study is a descriptive type of

study that attempts to explore the object of research with a descriptive-qualitative approach. In the legal paradigm, this research employs the normative juridical approach and the legal sociological approach in order to provide systematic legal findings. The data collected from primary and secondary legal materials and documents are systematized and analyzed in order to answer the questions raised.

The normative juridical approach used in this paper are the statute approach and the comparative law approach. The statute approach is carried out by reviewing laws and regulations related to the legal issues being handled. Law is viewed by researchers as a closed system with comprehensive, all-inclusive, and systematic qualities. The statute approach is employed for legal dogmatic level panels. Legislation is a written regulation made by a governmental agency or authorized official that applies in general. The legal issues being handled in this paper is the issue of cyberspace in law and international relations perspective. This study attempts to review the regulations of cyber domains across levels ranging from international, regional, and national level. The current cyber security concepts in those regulations are considered not responsive and resilient in dealing with and overcoming cyber attacks that can occur at any time with evolving patterns and types.

On the other hand, the comparative law approach is carried out by comparing laws or regulations in a country or region with the national legal regime of another country or other regional regime. As applied to law, the act of comparison provides insight into the other law, our own law and, as importantly, our own perceptions and intuitions, as a self-reflection that often can yield insight into our view of the law (Eberle, 2007). This legal approach is used by the researcher as an instrument of learning and knowledge in order to comprehensively understand and appreciate the difference of other legal cultures that could be enriching. The act of comparison in this study would give a wider exposure about different legal cultures that commonly refers to "patterns of order that shape people, institutions, and society in a jurisdiction" in the cyber security domain ranging from international, regional, and national level.

The researcher examines how the Budapest Convention, International Convention on Cyber Crime, and International Telecommunication Union emphasize and implement collaboration with other state parties and public-private partnerships in safeguarding citizens' and legitimate interests from cybercrime, thereby encouraging international cooperation. On a regional level,

this paper focuses on reviewing the cyber space regulations under ASEAN. Accorrding to the World Economic Forum, The "Digital ASEAN" initiative is a type of reaction by regional partners, both public and commercial, to solve the ASEAN region's digital economy issue in order for it to become an inclusive force. Meanwhile, at the national level, this article seeks to evaluate the legislation and compare national cyberspace regulations in Indonesia and Singapore. Researchers sought to put the efficacy of Indonesian Act in terms of the government's initial efforts to build a resilient digital economy, as well as Presidential Regulation Number 53 of 2017 and Amendment Number 133 of 2017 governing national cybersecurity legal framework, to the test.

The second approach in the legal paradigm used in this research is the legal sociological approach. According to a social-legal approach, analysis of law is directly linked to the analysis of the social situation to which the law applies, and should be put into the perspective of that situation by seeing the part the law plays in creation, maintenance and/or change of the situation (Schiff, 1976). In this research study, the analysis of the law as a social institution in the regulation of the cyber security domain is considered not responsive and resilient in dealing with and overcoming cyber attacks that can occur at any time with evolving patterns and types. Therefore, it needs to be re-visited in order to be adequate and relevant in facing the evolving nature of cybercrime as part of the social challenges.

In international relations perspective, this research paper uses regime theory in analyzing the issue being raised. Regime theory is an approach within international relations theory, a sub-discipline of political science, which seeks to explain the occurrence of co-operation among States by focusing on the role that regimes play in mitigating international anarchy and overcoming various collective action problems among States (Bradford, 2007). The theory of regime is closely related with the concept of regime itself in which the definition is still under debate. But, the concept of regime commonly refers to a set of 'principles, norms, rules and decision-making procedures around which actors' expectations are covered in a given area of international relations'. Therefore, a regime would create convergence of expectations, establish standards of behavior, and cultivate a general sense of obligation.

International relations paradigm aims to help international lawyers to understand patterns of behavior in inter-State relations though regime theory. In this research, regime theory would give a more comprehensive explanation

of the structure and the function of international rules and institutions in the cyber security domain and analyze the ways international regimes can shape international law and international relations in this particular domain.

According to Manheim, "Research is the careful, diligent and exhaustive investigation of a specific subject-matter, which has as its aim the advancement of mankind's knowledge" (Soren, 2021). Therefore, this legal and international relations research was conducted for the purpose of discovering new facts about the cyber security domain in both perspectives in order to contribute to the body of knowledge in legal and international relations fields or subjects. The collaboration between law and international relations perspective in this research would give a rich and more comprehensive solution through a socio-legal finding.

Results and Discussion

Cyber Resilience Concept

Everyone is becoming more and more reliant on the interconnected cyber system in conducting daily activities. From personal finance to managing defense capabilities to controlling a vast web of aircraft traffic, digitized information systems and software packages have become integrated at virtually all levels of individual and collective activity (Linkov & Kott, n.d.). The nature of cyberspace and everyone's growing reliance upon it is constantly changing the way advanced users operate in modern, decentralized cyberspace environment provides good cover and anonymity for an intelligent foe, making the attribution of any cyber attack very difficult to pinpoint (Harrop & Matteson, n.d.). In dealing with the threats of cyber attacks, society needs a more agile approach rather than relying on traditional protection. All levels of society must have an adequate ability to react to these attacks. Therefore, we need to build a more robust organizational structure that recalls the concept of resilience.

In order to survive in the ever-changing cyber ecosystem, organizations should have the ability to adapt and recover quickly from unforeseen events targeting them. The concept of cyber security is no longer relevant in dealing with the evolving cyber nature. A distinction between safety and resilience: the first one focuses on the protection of systems from threats or events, while the second one is the ability to prepare and adapt to changing conditions, to resist and to recover quickly from interruptions (Roege et al., 2017). The cyber-security approach based on risk management focuses on achieving security through the prevention or

protection against intrusions (avoiding risk) is outpacing and no longer provide the adequate protection required. Differently, an approach based on resilience is concerned with ensuring the continuity of functions and critical services and continuously improving the overall context (Annarelli et al., n.d.). Hence, the inclusion of risk resilience to manage, respond, and withstand any negative impacts of cyberspace activity is necessary to the longevity of an organization.

The concept of cyber resilience has been introduced at the 2012'World Economic Forum meeting in Davos. Although the concept of cyber resilience is still in its infancy, this area has been of growing importance to all global actors. The term 'resilience' itself is not a new concept, it has been used in psychological studies since the 1940s. Initially, the term was used in psychological studies that were trying to find out what makes people able to cope with personal misfortune and unpredictable hardships (Hanisch, 2016). In the cyber domain, resilience refers to the ability of an organization to continuously deliver the intended outcome despite adverse cyber events that cause a negative impact on IT systems. One of cyber resilience benefit is that it enables complex organizations to prepare for adverse events and to keep operating under very challenging circumstances (Dupont, 2019). Cyber resilience is way more complex and needs a build-in approach rather than an add-on approach, require multi-layered protection, and a holistic approach in an organization.

Cyber resilience refers to "the system's ability to recover or regenerate its performance to a sufficient level after an unexpected impact procedure a degradation of its performance. It is characterized by [four] abilities: to plan/ prepare, absorb, recover from, and adapt to known and unknown threats" (Cassleman, 2020). Hence, the four aspects of cyber resilience are – (1) prepare, (2) withstand (a.k.a absorb), (3) recover, and (4) adapt (Onwubiko, n.d.). The prepare aspect of cyber resilience encompasses planning, anticipation, and prediction of a potential cyber-attack towards the organizations. The withstand (a.k.a absorb) aspect is the ability to maintain business operations in the face of cyber incidents even when the system component damaged (failure until loss functionalities). The recover aspect is the ability of organization to restore operations, services, and functionalities after a cyber incident. And the adapt aspect emphasizes the modification and improvement of the organization systems following a cyber incident.

In order to develop a cyber resilience system in society, we need to address it holistically on several levels. Building resilience requires real commitment throughout the society (Hanish, 2017). Each level of society needs to take

an appropriate role in building cyber resilience. Its because each of them is received unique and challenging threats that need to be handled. To be effective and efficient a holistic approach need to be taken from the most basic technical level including IT system and network. Furthermore, cyber resilience also must be addressed at another level such as organizational, regional, national, and even supranational levels. Every level of society must highly concern and continuously implement cyber resilience strategies in order to keep strive and gain maturity in the challenging cyber environment.

As described earlier, a resilient system is the core requirement in modern society that attached to cutting-edge technologies. A resilient system is the main characteristic of a robust organization in the interconnected digital world. Therefore, every organization must clearly aware of its system resiliency. Woods (2012) identified several desirable traits for resilient systems, citing their ability to (Roege et al., 2017):

1. Recognize the signs that adaptive capacity is falling;
2. Respond to the threat of exhausting buffers or reserves;
3. Shift priorities across goal tradeoffs;
4. Make perspective shifts and contrast diverse perspectives that go beyond their nominal position;
5. Navigate changing interdependencies across roles, activities, levels, goals; and
6. Learn new ways to adapt.

Cyber resilience is a preferred strategy that necessary to be adopted by every modern organization and entity in the interconnected digital world. Its because cyber resilience is not merely consider the nature of the hazards from cyber incidents. But it also deeply consider the assessment of the system's capacities in response to change pre-, during, and post-event of cyber incidents. Although cyber resilience is way more complex than cyber security, it brings more comprehensive protection and benefits to the organization. Attention paid by companies to resilience is not only vital for the sustainability and growth of their business models but also a source of competitive advantage (Annarelli et al., n.d.). Therefore, adopting cyber resilience strategies and operations will ensure success when operating in a hyper-connected system.

Cyber Resilience as Non-Traditional Threat

The development of computer technology and the internet of things

has challenged the global actors to solve the evolving cyber threats that spill over borders and arising conflicts from the misuse of cyberspace. Although the benefits brought by computer technology and the internet of things is undeniable to society, this cutting-edge technology also brings dangerous threats to society. However, although this technology has allowed for many advances in global terms, the openness and philosophy of freedom that underpins the use of the network, also have negative consequences and challenge the global authorities to think of new ways to solve the damages experienced because of the use of cyberspace for bad purposes (Bechara & Schuch, 2020). This is becoming a current dilemma that demands dialogue and research about the transition of global structure to a new era of post-territorial systems.

Achieving security means eliminating every threat towards it. The idea of security in international relations clearly embedded with military and non-military threats. This concept was established with the Westphalian peace treaty in 1648 and has remained a respected element of security doctrine into the twentieth and twenty-first centuries (Causevic, 2017). From a traditional perspective, the threat is roughly defined as "hard" threats that are military induced threats towards states. In the twenty-first century, threats are becoming more extensive by the emergence of non-traditional threats. The non-traditional threats is harder to define and requires more complex strategies because the close alignment of technologies with global structure potentially rising various non-military threats lurking on it. The existence of evolving cyber nature in the international system added unforeseen events that potentially threaten every actor operating in a hyper-connected system.

The increasing reliance upon technology in modern society makes them vulnerable to cyber threats. Various types of cyber threats including cybercrime, cyberterrorism, cyberwar, and cyber espionage will potentially disrupt the use of the cyber environment. The cyber threat is an action that may result in unauthorized access to, exfiltration of, manipulation of, or impairment to the integrity, confidentiality, or availability of an information system or information that is stored on, processed by, or transiting an information system (Reich & Gelbstein, 2012). In general, the cyber threat may take forms in a cyber attack or cyber exploitation. Cyberattack is defined as a cyber operation conducted to alter, disrupt, deceive, degrade, or destroy computer systems or networks or the information and/or programs resident in or transiting these systems or networks (Russel, 2014). In another hand, cyber exploitation involves confidential information covertly obtained through cyberspace (Shad, 2019).

Cyber threats might be taken by individuals or organizations in various actions, for example, hacking, breaching, infecting, etc.

Cyber incidents have rapidly grown in the cross border area that urges cooperation between countries to conduct coordinated action to mitigate the threats. The question that arose from the international point of view in the misuse of cyberspace is how to regulate the cyber environment and resolve the possible conflicts between different countries in the unbounded territorial boundaries of cyberspace. In this context, cooperation between nations is increasingly necessary to give traction to discussions on global cyber governance, aiming at the conclusion of international agreements capable of establishing mutual assistance to guarantee digital inclusion, for the sharing of information and collaboration in investigations of cybercrimes, as well as for the harmonization and guarantee of enforcement regardless of territorial limits imposed by traditional regulatory models (Bechara & Schuch, 2020).

As discussed earlier, the concept of cybersecurity is outpacing and no longer provides adequate protection against the evolving nature of cyber threats. In another hand, cyber threat is evolving into more dangerous threats that able to harm a society just as hazardous as catastrophic events. This is a serious threat that significantly danger many countries, citizens, and businesses in general. Global actors need to strengthen their strategy in order to ensure their security and maturity in operating in the interconnected digital world. Hence, the ability to react to these attacks and to design and implement a more robust organization recalls the concept of resilience, known in physics as the assumption of sustaining crashes without breaking (Annarelli et al., n.d.). Therefore, building cyber resilience holistically in all levels of society is the answer in dealing with cyber threats as non-traditional threats that threaten global actors operating in the interconnected digital world.

The foremost action must be taken in cross-border cooperation since the threat exists in the borderless cyber ecosystem. Cooperation among nations in conducting coordinated action against cyber threats must include risk resilience to manage, respond, and withstand any negative impacts of cyberspace activity. Cyber resilience is a condition for continuous existence and competitive advantage, so the trend is towards adopting resilient strategies and operations to ensure success when operating in a hyper-connected system (Annarelli et al., n.d.). In order to strive, every single actor in the digital global system must deeply aware of the danger of cyber threats as emerging non-traditional threats and implement all aspects of the cyber resilience including constant evolving,

adapt quickly, react to the ever-changing environment, and recover from massive unforeseen events in cyberspace. Therefore, building cyber resilience will guarantee the longevity and safeguard the underpinnings of the modern interconnected society.

International Cooperation Legal Frameworks

The Organization for Economic Cooperation and Development (OECD) defines digital economy enables and executes the trade of goods and services through electronic commerce on the internet. This includes the embedding of connected sensors (IoT), new end-user devices (mobile phones, laptops, 3D printers), and new digital models (cloud, digital platforms, and services) growing intensity of data usage through spread of big data and algorithmic decision making, automation, and robotics technologies (OECD, 2015). This definition comes at the same time by the Internet's ability to optimize the customer experience with commercial transactions (Srinivas & Yasmeen, 2017).

According to a World Bank report, Indonesia's digital economy, the largest in Asia, is worth US $40 billion. By 2025, that number could reach $133 billion even though the threat of an economic recession from COVID-19 seems inevitable for all countries. Although, according to the Minister of Finance the economic contraction was 0.4%, the existence of the internet and digitalization has minimized this impact and Indonesian e-commerce is able to control two-thirds of the country's digital economy (The Jakarta Post, 2020). Supporters of this growth include SMEs, and most of them are online sellers. Platforms such as *Tokopedia*, *Lazada*, and *Shopee* host digital microbusinesses operating across platforms. The government's initiative in digitizing SMEs requires a sustainable implementation of regulations coupled with competition for the presence of domestic global players who become a barrier to growth. Local companies, even e-commerce start-ups and unicorns that do not take advantage of software with facilities that are supported by data analysis, cloud computing, and artificial intelligence (AI) would be also disrupted (Siciliano & Gaudenzi, 2018). Free flow of data creates new threats such as violations of intellectual property and foreign interference. As a result, national digital policies are needed to give consumers choice and control as well as harmonize international best practices and standards.

Nowadays resilience is built through internal and external initiatives, including cooperation with international partners. Moreover, third countries support increase the level of cybersecurity globally. Promoting cooperation in

the whole-of-society model, capacity building, and increasing cyber resilience are also part of the overall goal to maintain an open, stable and safe virtual world, and to build bridges between all actors, both from the government, the private sector, civil society, technical community, users, and academia for the address challenges faced need to be taken in account. In this case, the global cyber resilience framework or regime contribute to a strategic framework for conflict prevention, cooperation, and stability in cyberspace that is based on the application of existing international law, in particular of the UN Charter in its entirety, development and implementation of universal norms on responsible state behavior, and regional trust-building measures between countries.

International Dimension

Digital economy and inclusive trade seeks to simplify procedures for transit of goods and flow of foreign trade traffic, create standardization, and harmonize regulations and laws by using the sophistication of information technology. The international trade interface is divided into two aspects, tangible and intangible (Riswanti, 2019). The intangible aspects of supply chains consist of transportation, storage, geography, and physical inspection of goods and documents by expert authorities. Expectations of trade facilitation in domestic processes and international trade will significantly reduce the transaction costs of participants in foreign economic activity (Ahmedov, 2020). In a publication entitled 'World Trade Report 2020: Government Policies to Promote Innovation in the Digital Age,' finds that 115 countries have instituted industrial policies and development strategies to foster a transition on a digital economy. For example, tax breaks to facilitate digital innovation and technological hubs to maximize knowledge dissemination (WTO, 2020). The report concludes that international cooperation play a key role for countries to accelerate digital transitions and protect privacy.

Budapest Convention

Article 23 - General Principles relating to International Cooperation

> "The parties shall cooperate with each other, in accordance with the provisions of this chapter, and through the application of relevant international instruments on international cooperation in criminal matters, arrangements agreed on the basis of uniform or reciprocal legislation, and domestic laws, to the widest extent possible for the purposes of investigations or proceedings concerning criminal offences

related to computer systems and data, or for the collection of evidence in electronic form of a criminal offence."

Article 25 - General Principles relating to Mutual Assistance

"It states in the point 3 that each party in urgent circumstances may make request for mutual assistance or communications, to the extent that such means provide appropriate levels of security and authentication (the use of encryption) where required by requested Party."

Article 34 - Mutual Assistance regarding the Interception of Content Data

"The parties shall provide mutual assistance to each other in the real-time collection or recording of content data of specified communications transmitted by means of a computer system to the extent permitted under their applicable treaties and domestic laws."

As stated in the *preambule* of the Budapest Convention, it emphasizes that recognizing the value of fostering cooperation with other States parties and private industry is aimed at protecting society and legitimate interests against cybercrime, namely by adopting appropriate laws and fostering international cooperation. This agreement covers online norms regarding copyright infringement, computer-related fraud, child pornography and network security breaches (Budapest Convention, 2001). For example, the Gulf Cooperation Council (GCC) aspires to expand "smart infrastructure", but infrastructure components still have poor security and are vulnerable to cyberattacks.

International Convention on Cyber Crime

Countries such as the United States and others that are technologically advanced, the Group of Eight (G-8) and private groups rely on multilateral efforts to improve cyber security. However, Drew C. Arena, Senior Counsel to the assistant attorney general U.S. The Department of Justice, stated that until now there has been no idea to negotiate the standards and obligations that are legally mandated in international agreements (Sofaer, n.d.). Abraham D. Sofaer, examined The Stanford Draft differs from the draft COE Convention on Cyber-Crime a.k.a Budapest Convention, where the Stanford Draft covers action restrictions on attacks on critical infrastructure and violations of anti-terrorist conventions. In addition, the Stanford Draft co-founded an international body to increase the effectiveness and steps of the investigation,

while the COE offered cooperation without such a process. The International Civil Organization (ICAO) and International Telecommunication (ITU) are regimes that deal with technology regulation to create security and efficiency as a multilateral solution to cybercrime and terrorism. These entities are designed for countries to protect their strategic interests.

International Telecommunication Union

As international concerns regarding, infrastructure protection, and cyber-war began to escalate, a second major update to ITU cyber security treaty provisions was introduced and adopted at the 1998 Minneapolis Plenipotentiary Conference (Rutkowski, 2011). As a public international law related to cyber security, it must be increasingly evolving combined with universal state signatories.

Regional Dimension

While the region is poised to take its position amongst the world top digital economies, the doors are wide open for cyberattacks. The digital economy in ASEAN has the opportunity to increase $1 trillion to GDP over the next 10 years (Kearney, 2021). However, cyber risks hinder cyber resilience in the world of the digital economy and prevents the region from realizing its full digital potential. ASEAN has become the target of cyberattacks that strike strategic and vulnerable infrastructure. Unfortunately, the resilience of cyberspace is still low and each country has a different level of readiness. Increased capital flows, trade, and the use of IT increase the complexity of the region's cyber security challenges. In fact, 1,000 ASEAN companies could lose $750 billion in market capitalization and impact the failure of the digital innovation agenda as the foundation of the digital economy (Kearney, 2021).

Indonesia has been considered as one of the five founding fathers of ASEAN and played an important role in the region's countries. ASEAN seeks to realize the goal of peaceful coexistence, by formulating legal documents regarding cybersecurity, but no concrete efforts have yet been made. So far, ASEAN cyber development still focuses on the military sector and paid less attention to the public sector. Cyberattacks have not only hit America and the West, but also ASEAN countries. As reported last May 2017, Indonesia, Malaysia, Thailand and Vietnam have been attacked by ransomware (The Straits Times Asia, 2017). ASEAN is feared as a region vulnerable to cyber threats due to the following reasons: 1) Approximately 2.1 million internet users,

922 million users are from the ASEAN region and this number is estimated to increase every year (European Commission, 2013); 2) ASEAN is the largest regional organization in the Asia Pacific region which enables economic and market interactions to take place digitally connected in critical infrastructure such as transportation, mining, energy, banking to increase cross-border crime. At the bilateral and regional levels, many actions have been taken, including the AEC Blueprint 2025, the Masterplan on ASEAN Connectivity 2025, and the e-ASEAN Framework Agreement (ASEAN Studies Centre, 2020).

In the article Caitríona H. Heinl (Heinl, 2014), outlines the main cybersecurity issues faced by the Association of Southeast Asian Nations (ASEAN) and outlines policy options for creating a more resilient cybersecurity regime at the regional level. Until now, national and regional efforts adopt a comprehensive cybersecurity strategy have tended to be slow and split into several parts, resulting in the collaboration of ASEAN members through new national and international initiatives in realizing the 2015 ASEAN Community. This was proven by the holding of the The 32nd ASEAN Summit with theme Building Resilience and Innovated ASEAN to encourage the development of 100 smart city networks by promoting the use of technology based on local wisdom (Media Indonesia, 2018). Thus, the performance system of ASEAN partners could improve training and capacity building, defense cooperation, and protect supply chains.

One of them is the "Digital ASEAN" initiative, which is a form of response from regional partners, both public and private, to address the digital economy issue of the ASEAN region to become an inclusive force (Weforum, 2021). These initiatives include the Pan-ASEAN Data Policy, ASEAN Digital Skills, ASEAN e-Payments, and ASEAN Cybersecurity which successfully launched the ASEAN Digital Skills Vision 2020 program and made commitments with BigPay, Cisco, Facebook, LinkedIn, *Tokopedia*, etc. (ASEAN, 2020).

Recently, Indonesia which is supported by the National Cyber and Crypto Agency met online at the ASEAN Ministerial Conference on Cybersecurity (AMCC) which is the 5th ASEAN Ministerial Conference attended by ten ASEAN countries Indonesia, Brunei, Cambodia, Laos, Malaysia, Myanmar, the Philippines, Singapore, Thailand and Vietnam discussed regional cyber security issues in Southeast Asia. According to the Minister of Communication and Information, Singapore, S. Iswaran, stated that AMCC is collaborating to establish the Operational Technology Cybersecurity Expert Panel (OTCEP) and the Cybersecurity Labeling Scheme (CLS) (BSSN, 2020b). The CERT to CERT

collaboration is a useful program to improve response times for handling attacks and cybercrimes against Indonesia's national critical information infrastructure sector.

National Dimension

The global police agency, INTERPOL warned of an increase in cyber crime during the pandemic and found a shift in targets that initially attacked small businesses or MSMEs and individuals are increasingly daring to attack large companies, governments and infrastructure. Even in April 2020, there was an increase in ransomware which resulted in users having to bail out money to cyber attackers to get their data back. Hoaxes or the spread of fake news in the media have disrupted the computer system (Sekretariat Nasional ASEAN-Indonesia, 2020). It has been recorded that since January to date, there have been 1,093 issues, 1,960 hoax-related content from four social media in Indonesia, namely, Instagram, Facebook, Twitter and YouTube. Then it was identified by a crawler machine and taken down by the Ministry of Communication and Information and law enforcement efforts were made by the Criminal Investigation Agency of the Indonesian National Police (Kominfo, 2020). The Ministry also massively conducts campaigns, educational classes, and trainings on digital literacy through the National Movement on Digital Literacy—*Siberkreasi*. Responding to this warning, Indonesia established a national agency, the National Cyber and Crypto Agency, to create a strategic cyber environment and safe electronic system operation, foster a digital economy with cyber innovation and competitiveness, and increase sensitivity and resilience in cyber space through Presidential Regulation Number 53 of 2017 and amendment number 133 of 2017 established the State Cyber and Crypto Agency (BSSN, 2020a) that one of its main role is to implement cyber security effectively and efficiently by utilizing, developing and consolidating all elements related to national cyber security. In order to provide a strategic reference of cybersecurity policy, BSSN prepares the Indonesian Cyber Security Strategy. This security strategy includes five aspects such as, sovereignty, independence, security, togetherness, and adaptive.

The government's initial efforts to build a resilient digital economy based on these following legal bases (Indonesia Act, 2008):

1. Indonesia Act Number 36/1999 concerning Telecommunication.
2. Indonesia Act Number 11/2008 concerning Information and Electronic Transactions.
3. Indonesia Act Number 3/2002 concerning National Defense.

4. Indonesia Act Number 7/2014 concerning Trade.
5. International Act Number 24/2000 concerning International Agreements.
6. Indonesia Act Number 17/2011 concerning State Intelligence.

State of Play: Factors that Hinder Cooperation in Increasing Cyber Resilience

Indonesia is the 15th largest country with promising economic potential and opportunities. Abundant resources, cultural and linguistic diversity, and strategic geographic could be potential for advancing the economy (Sindo News, 2015). Unfortunately, economic development in Indonesia is not fully evenly distributed, particularly access to infrastructure and technology is only centered in cities. Based on research from the Indonesian Central Statistics Agency in 2012-2018, the average internet usage in urban areas is 72%, but in rural areas it is 40-48% (Kemenkeu, 2020). The digital gap then encourages the Indonesian government to liberalize the economy by developing economic activities (e-commerce, marketplace, fintech), strategic sectors, and public services to be digitalized and integrated using cyber systems. Although digital ecosystems provide benefits, nonetheless it is still vulnerable to the threat of cyberattacks.

The existence of malicious cyber operations by states, state proxies or state-sponsored actors, and private actors have a destabilizing impact and constitute a risk or potential threat to international peace and security (Pauletto, 2020). The more digitalized government services, the more challenges government faces to step up protection of a country's critical infrastructure. Efforts were made not only at the national level, but also need to be upgraded to regional and international levels, even multilateral. Differences in complexity, interests, capacities, and common language are gaps in addressing cybercrime in cyberspace. Cyber power is closely linked on country's sovereignty. As a result, the state needs to implement the Department of Defense or the Intelligence Community. The government needs to focus on cyber security particularly critical national security issues. Prioritization and allocation of resources including technology, government, business, and human resources need to be developed so that the significant process can be made— cyber trustworthy use substantially enhanced (Kramer, 2010). The technical underpinnings in security overlap between national security and the broad cyber arena. Thus, Public-Private Partnership (PPP) based Cybersecurity is needed in policy planning,

incident reporting, awareness raising, and cybercrime prevention strategies (Chang & Coppel, 2020; Watanabe, 2019). There are some reasons why the concept of cyber resilience need to be revised in the perspective of international relations and trade law to face challenges in the digital economy:

First, either states or organizations and firms need to become much more cyber-resilient. They need to broaden their risk management focus, such as reputation and customer channels, and recognize the unintended business consequences from activity in cyberspace. A key finding of the ISF cyber-resilience report is that no organization could respond effectively to threats from cyberspace. The organization should work with others to leverage the knowledge and resources of numerous stakeholders. This would help to prevent attacks (or minimize the impact) and improve cyber-resilient (Crespigny, 2012). Organizations would benefit from partnering with others by sharing intelligence and influencing the adoption of best practice across cyberspace. By taking a broader view of cyberspace and cybersecurity, it would be better able to understand the true nature of the threats, in the context of business opportunity, and respond accordingly. For example, the CyberEast project, which builds on the objective of capacity building for the joint efforts of the European Union and the Council of Europe within the framework of a cybercrime project that targets strengthening international cooperation on cybercrime and electronic evidence, achieving public-private partnerships between criminal justice authorities and the internet industry and facilitating legal reform to achieve better compliance with the Budapest Convention on cybercrime in the six eastern partnership countries. The risk of cyber incidents is inevitable because financial institutions are digitally connected, requiring firms to be ready to stand them and maintain operations. The financial community is currently debating how regulators should develop new tools to ensure operational resilience across jurisdictions (Hausken, 2020). Achieving operational resilience requires a comprehensive approach to prevention, adaptation, response, recovery and learning. It has been proven by examining European guidelines for resilience and cyber-security, i.e: the European Union Network and Information Security Agency (ENISA), the EU's cyber-security organization has released 'enabling and managing end-to-end resilience'. It is the ability to assure end-to-end security and continue high levels of functionality in the face of abnormal traffic loads, malicious attacks, accidents, or human error is vital for the economy and society (Devine, 2011). In Indonesia, the COVID-19 outbreak exploited by certain actors to seek profit. The Work from Home (WFH) policy mechanism leads to more network usage.

Lack of literacy and awareness of cybersecurity due to low levels of education has further increased the number of cases of cyber incidents, including breached data of 15 million users on online shopping such as *Tokopedia* (Kompas, 2020). Proactive actions could be done such as backing up data, installing up-to-date software, changing passwords regularly, not plugging in a USB flash drive carelessly, and not clicking on unsafe or unknown links.

Second, the existing cyber resilience of multinational corporations is arguably typically inadequate and in the context of digital supply chain integration, the potential consequences are larger. Cyber resilience requires conscious planning and relentless action from both the security provider and the multinational corporation (Lees et al., 2018). Lees introduces four key areas that warrant particular attention: 1) Infrastructure design: the development of architectures that are inherently more resilient and easier to protect; 2) Change management: minimizing the operational risks of cyber infrastructure; 3) Backups: the ability to recover; and 4) Resourcing: senior support for the 'total cost' of protection. For the example, on the first case in the study Visegrad Group Countries (Czechs Republic, Hungary, Poland, and Slovak) built mutual contacts at all levels, from the highest political summits to experts and diplomatic meetings, to activities of NGOs in the region, think-tanks and research bodies, cultural institutions, and numerous work of individuals apparently performing better due to their developed national strategies: 1) Sharing best practice and lessons learned within the organizational units to deal with crisis management, risk assessment, and physical infrastructure security to increase cyber resilience; 2) Education and training in cyber issues either private or public sector; and 3) International cooperation is a cross-cutting issue. There is no place for competition, when security is concerned (Tonhauser & Ristvej, 2019). Then, the second case is Norway's digitalization development needs to be emulated because it is able to create digital value chains that cross national jurisdictions, including Europe, Asia, the US, even space (GPS). The technology of 'smart grid' and 'smart city' with the operation of electric power grid enables service improvements in the aspects of safety, surveillance, energy management, and security (Hagen, 2017).

Third, how is international law supposed to apply? The absence of a special international legal system for cyberspace does not mean that there are no legal rules that would apply to cyber activities. If international law is intended to build efficient governance, it is necessary to adapt to new phenomena without the need to reinvent the entire regulatory framework at each event. i.e: the

finalization of the UN charter related to power suppression in the Nuclear Weapon Advisory Opinion, the international court issued a statement "apply to any use of force, regardless of the weapons employed", thus following the same logic cyber operation must both comply with legal regulations about the use of force (Maľák, 2016). These include the 1992 Constitution of the International Telecommunication Union, the 2001 Budapest Convention on Cybercrime, and its 2006 Protocol on Xenophobia and Racism, the 2009 Shanghai Cooperation Organization's Information Security Agreement, and the 2014 African Union's Cyber Security Convention. However, this international agreement only regulates a small part of activities related to cyberspace, such as: criminal offenses committed by means of a computer system or operations interfering with existing telecommunication networks, or the Shanghai Cooperation Agreement and African's Union Convention have a very limited membership. Microsoft's proposal, entitled International Cybersecurity Norms: Reducing Conflict in an Internet-Dependent World, was published in 2014, urging states to revise their 'country-centric laws' and adopting instead 'international standards' regulating important aspects of online behavior including security, privacy, and taxation and make it appear legally binding (Maľák, 2016). Therefore, doubts in the development and application of international law have generated a power vacuum and allowed the emergence of the creation of non-state norms. Particularly in the 21st century where the pluralization of norm-making processes involves multiple states and non-state actors to identify overlaps with their strategic interests.

When observing the world scenarios, complex cyber incidents covering transnational issues, such as money laundering, corruption and organized crime require cooperation between countries to mitigate threats. Initiatives in fighting cybercrime are still fragmented and lack alignment to build mutual trust, therefore cooperation between nations aiming at the conclusion of international agreements capable of establishing mutual assistance to guarantee digital inclusion (Bechara & Schuch, 2020). Furthermore, increasing cybersecurity in the policy agenda requires a Rapid Action Cybersecurity Framework to harmonize cyber resilience in the region and internationally. The existence of a collaborative framework is expected to narrow the gaps in strategy, policies, laws and governance in cybersecurity. Adoption of a multilateral regime and directives from the national government could bring strategic and operational benefits, so that law enforcement cooperation would run quickly.

Conclusion

This study suggests that there has been no clear agreement either at the level of international and national about legal frameworks as well as an architectural models associated with cyber resilience. Legal frameworks that exist at the international level are still focused on the concept of cybersecurity. Meanwhile at the national level, for example, Indonesia still does not have a set of rules related to cyber security and resilience, where Singapore already has a Cyber Security Law. The need to encourage countries to become more involved in building one at the level of international agreements on legal frameworks and revisit the rules of existing laws which did not fully accommodate the cyber resilience in the era of digital economy.

Acknowledgement

This research is funded by DIPA Budget Fakultas Ilmu Sosial dan Ilmu Politik Universitas Diponegoro 2018.

References

Bradford, Anu. (2007). *Regime Theory.* Max Planck Encyclopedia of Public International Law.

Harrop, W., & Matteson, A. (n.d.). *Cyber Resilience: A Review of Critical National Infrastructure and Cyber-Security Protection Measures Applied in the UK and USA.* In Current and Emerging Trends in Cyber Operations (1st ed.). Palgrave Macmillan UK.

Reich, P. C., & Gelbstein, E. (2012). *Law, Policy and Technology: Cyberterrorism, Information Warfare and Internet Immobilisation*. Scopus.

Russel, A. L. (2014). *Cyber Blockades*. Georgetown University Press.

Srinivas, K., & Yasmeen, S. (2017). *A Study on Employee Engagement in Small and Medium Enterprises in Digital Economy*. Zenon Academic Publishing, 57–64(Millennial Workforce-A Contemplation).

Kott, A., and Linkov, I. (2019). *Cyber Resilience of Systems and Networks.* USA: Springer International Publishing AG.

Wall, David S. (2001). *Crime and the Internet.* New York: Routledge.

Ahmedov, I. (2020). *The Impact of Digital Economy on International Trade.*

European Journal of Business and Management Research, 5(4). https://doi.org/10.24018/ejbmr.2020.5.4.389

Annarelli, A., Nonino, F., & Palombi, G. (n.d.). *Understanding the management of cyber resilient systems*. Elsevier Ltd.

Bechara, F. R., & Schuch, S. B. (2020). *Cybersecurity and Global Regulatory Challenges*. Emerald Publishing Limited, 1359–0790. https://doi.org/10.1108/JFC-07-2020-0149

Causevic, A. (2017). *Facing an Unpredictable Threat: Is NATO Ideally Placed to Manage Climate Change as a Non Traditional Threat Multiplier?* Partnership for Peace Consortium of Defense Academies and Security Studies Institutes, 16(2), 59–80.

Chang, L. Y. C., & Coppel, N. (2020). *Building Cyber Security Awareness in a Developing Country: Lessons from Myanmar.* Elsevier Ltd., 0167–4048. https://doi.org/10.1016/j.cose.2020.101959

Crespigny, M. de. (2012). *Building Cyber-Resilience to Tackle Threats*. Information Security Forum.

Devine, M. S. (2011). *Sinister Trends in Cyber threats: European Guidelines for Resilience and Cybersecurity*. Elsevier Ltd., 3.

Dupont, B. (2019). *The cyber-resilience of financial institutions: Significance and applicability.* Journal of Cybersecurity, 5(1).

Eberle, Edward J. (2007). *Comparative Law.* Annual Survey of International & Comparative Law, 13(1).

Hagen, J. (2017). *Critical Infrastructure Protection*. International Journal of Critical Infrastructure Protection. https://doi.org/10.1016/j.ijcip.2017.11.003

Hanisch, M. (2016). *What is Resilience? Ambiguities of a Key Term*. Federal Academy for Security Policy.

Hanish, M. (2017). *Forward, Resilience! –: Ideas on how to Strengthen Resilience in Germany.* Federal Academy for Security Policy. http://www.jstor.com/stable/resrep22183

Hausken, K. (2020). *Cyber Resilience in Firms, Organisations, and Societies.* Elsevier Ltd., 2542–6605. https://doi.org/10.1016/j.iot.2020.100204

Heinl, C. (2014). *Regional Cybersecurity: Moving Toward a Resilient ASEAN Cybersecurity Regime.* Asia Policy, 18, 131–160. http://www.jstor.org/stable/24905282

Kramer, F. D. (2010). *An Integrated Governmental Strategy for Progress*. Atlantic

Council JSTOR. http://www.jstor.com/stable/resrep03332

Lees, M. J., Crawford, M., & Jansen, C. (2018). *Towards Industrial Cybersecurity Resilience of Multinational Corporations.* Elsevier Ltd., 2405–8963. https://doi.org/10.1016/j.ifacol.2018.11.201

Linkov, I., & Kott, A. (n.d.). *Fundamental Concepts of Cyber Resilience: Introduction and Overview.* In Cyber Resilience of Systems and Networks (pp. 1–25). Springer International Publishing.

Pauletto, C. (2020). *Information and Telecommunications Diplomacy in the Context of International Security at United Nations*. Emerald Publishing Limited, 30. https://doi.org/10.1108/TG-01-2020-0007

Putranti, I.R., (2015). *Developing of Cyber Resilience System of the International Trade Facilitations: Specific reference Indonesia UNCITRAL Congress 2015*, http://eprints.undip.ac.id/71123/1/UNCITRAL.pdf

Putranti, I.R. et.al (2020). *Cyber Resilience of Small and Medium Enterprises In Semarang City*. Jurnal Sosial dan Pembangunan MIMBAR, Vol 36 No. 2, pp. 288-297, https://ejournal.unisba.ac.id/index.php/mimbar/article/view/5856/pdf

Putranti, I.R. et.al (2020). *Smartcity : Model Ketahanan Siber Untuk Usaha Kecil Dan Menengah, Jurnal Ketahanan Nasional*, Vol 36 No. 2, pp.359-379, https://journal.ugm.ac.id/jkn/article/view/57322/30278

Riswanti, I. P. (2019). *Developing of Cyber Resilience System of the International Facilitations: Specific Reference Indonesia*. https://core.ac.uk/download/pdf/195785509.pdf

Roege, P. E., Collier, Z. A., Chevardin, V., Chouinard, P., Florin, M. V., Lambert, J. H., & Todorovic, B. (2017). *Bridging the gap from cyber security to resilience.* In Resilience and Risk (pp. 383–414). Springer

Rutkowski, A. (2011). *Public International Law of the International Telecommunication Instruments: Cyber Security Treaty Provisions Since 1850*. 13, 13–31. http://dx.doi.org/10.1108/14636691111101856

Schiff, David N. (1976). *Socio-Legal Theory: Social Structure and Law.* The Modern Law Review, 39(3), 287-310.

Shad, M. R. (2019). *Cyber Threat Landscape and Readiness Challenge of Pakistan*. Journal of Strategic Studis, 39(1), 1–19.

Siciliano, G. G., & Gaudenzi, B. (2018). *The Role of Supply Chain Resilience on IT and Cyber Disruptions*. Springer International Publishing. https://doi.

org/10.1007/978-3-319-62636-9_4

Sofaer, A. D. (n.d.). *Toward an International Convention on Cyber Security*. Hoover Press.

Soren, Chunuram. (2021). *Legal Research Methodology: An Overview.* Journal of Emerging Technologies and Innovative Research (JETIR), 8(10).

Tonhauser, M., & Ristvej, J. (2019). *Disruptive Acts in Cyberspace, Steps to Improve Cyber Resilience at National Level*. Elsevier Ltd. https://doi.org/10.1016/j.trpro.2019.07.220

Watanabe, K. (2019). *PPP (Public-Private Partnership) - Based Cyber Resilience Enhancement Efforts for National Critical Infrastructures Protection in Japan*. Springer Nature Switzerland AG 2019, LNCS 11260, 169–178.

Kahan, Jerome H., Allen, Andrew C., and George, Justin K. (2009). *An Operational Framework for Resilience.* Journal of Homeland Security and Emergency Management, page 10.

Bodeau, Deborah, and Graubart, R. (2011). *Cyber Resiliency Engineering Framework*. MITRE Report, page 37.

Cassleman, R. (2020). *Expanding Cyber Resilience Beyond Convention Resiliency and Nuclear Command, Control, and Communications*. Center for Strategic and International Studies (CSIS).

Kearney. (2021). *Cybersecurity in ASEAN: An Urgent Call to Action*. https://www.southeast-asia.kearney.com/web/southeast-asia/article?/a/cybersecurity-in-asean-an-urgent-call-to-action [Retrieved at January 20, 2021]

Maᷞlák, K. (2016). *Is the International Law of Cybersecurity in Crisis?* NATO CCD COE.

Onwubiko, C. (n.d.). *Focusing on the Recovery Aspects of Cyber Resilience.* Artificial Intelligence, Blockchain & Cyber Security.

ASEAN-EU Statement on Cybersecurity Cooperation. (2020). Accessed from https://asean.org/storage/2019/08/ASEAN-EU-Statement-on-Cybersecurity-Cooperation-FINAL.pdf [Retrieved at January 19, 2021]

Budapest: Convention on Cybercrime. (2021). European Treaty Series - No. 185.

Cyberattack: Ransomware cases reported in Asia. (2017). Accessed from http://www.straitstimes.com/asia/east-asia/cyber-attack-ransomware-cases-reported-in-asia [Retrieved at January 22, 2021]

Dalam Ministerial Conference on Cybersecurity BSSN Serukan Kesiapan Berkolaborasi dengan Negara ASEAN untuk Perkuat Keamanan Siber. (2020). Accessed

from https://bssn.go.id/dalam-ministerial-conference-on-cybersecurity-bssn-serukan-kesiapan-berkolaborasi-dengan-negara-asean-untuk-perkuat-keamanan-siber/ [Retrieved at January 21, 2021]

Data Pengguna Tokopedia Bocor Cek Apakah Akun Anda Terdampak. (2020). Accessed from https://tekno.kompas.com/read/2020/05/03/11580057/data-pengguna-tokopedia-bocor-cek-apakah-akun-anda-terdampak [Retrieved at January 16, 2021]

Digital ASEAN. (2021). Accessed from https://www.weforum.org/projects/digital-asean [Retrieved at January 18, 2021]

Digital Customs: The Opportunities of the Information Age. (2021). Accessed from https://mag.wcoomd.org/magazine/wco-news-79/digital-customs-the-opportunities-of-the-information-age/ [Retrieved at January 22, 2021]

Interpol: Kejahatan Siber Meningkat Selama Pandemi. (2020). Accessed from http://setnas-asean.id/news/read/interpol-kejahatan-siber-meningkat-selama-pandemi [Retrieved at January 17, 2021]

In challenging times, digital economy and e-commerce can chart a path toward recovery. (2020). Accessed from https://www.thejakartapost.com/academia/2020/04/21/in-challenging-times-digital-economy-and-e-commerce-can-chart-a-path-toward-recovery.html

Indonesian Cybersecurity Strategy. (2020). Accessed from https://bssn.go.id/strategi-keamanan-siber-nasional/

Impact Assessment Accompanying the Document Proposal for a Directive of the European Parliament and of the Council Concerning Measures to Ensure a High Level of Network and Information Security across the Union. (2013). Commission Staff Working Document.

Indonesia Act 2008 Concerning Information and Technology. (2008).

Keamanan Siber dan Smart City Jadi Fokus KTT ASEAN. (2018). Accessed from https://mediaindonesia.com/internasional/156273/keamanan-siber-dan-smart-city-jadi-fokus-ktt-asean [Retrieved at January 21, 2021]

OECD Digital Economy Outlook 2015. (2015). Accessed from https://www.oecd.org/sti/oecd-digital-economy-outlook-9789264232440.htm [Retrieved at January 20, 2021]

Potensi Indonesia Menjadi Kekuatan Ekonomi Global. (2015). Accessed from

https://nasional.sindonews.com/berita/1010858/18/potensi-indonesia-menjadi-kekuatan-ekonomi-global?showpage=all [Retrieved at January 21, 2021]

Peningkatan Keamanan Siber ASEAN Melalui Kerjasama Keamanan Siber dengan Australia. (2020). *Pusat Studi ASEAN*.

Pemerintah Berusaha Mempersempit Kesenjangan Digital. (2020). Accessed from https://www.kemenkeu.go.id/publikasi/berita/pemerintah-berusaha-mempersempit-kesenjangan-digital/ [Retrieved at January 17, 2021]

Stanford Draft. (2021). Accessed from http://www.iwar.org.uk/law/resources/cybercrime/stanford/cisac-draft.htm [Retrieved at January 18, 2021]

Tiga Stretagi Kominfo dalam Tangani Hoaks, dan Misinformasi. (2020). Accessed from https://aptika.kominfo.go.id/2020/09/tiga-strategi-kominfo-dalam-tangani-hoaks-dan-misinformasi/ [Retrieved at January 16, 2021]

What is Cyber Resilience? (2021). Accessed from https://www.itgovernance.co.uk/cyber-resilience. Accessed on January 5, 2021. [daring].

World Trade Report 2020: Government Policies to Promote Innovation in the Digital Age. (2020). Accessed from https://www.wto.org/english/res_e/publications_e/wtr20_e.htm [Retrieved at January 21, 2021]