

# CYBER SECURITY SHARING PLATFORM: INDONESIA'S APPROACH IN LAW ENFORCEMENT OF FINANCIAL TRANSACTION CRIMES

**Deni Kamaludin Yusup, UIN Sunan Gunung Djati Bandung**

## ABSTRACT

*The aim of the paper is to analyze the Indonesian government efforts in overcoming various criminal acts of financial transactions that have become increasingly prevalent in the last decade. On the one hand, information technology systems have provided various benefits for the community, especially business people to develop their businesses. On the other hand, it has also been misused by certain parties to share criminal acts, such as fraud, bank and credit card break-ins, selling personal data, and even money laundering. By using juridical-normative methods and qualitative approaches, this research concludes that the cyber security sharing platform is an effort made by the Indonesian government to regulate, supervise, prevent, prosecute, and protect all forms of financial transactions. It was created as the implementation of several government regulations on the cyber security system and has proven successful in suppressing and reducing the occurrence of digital based financial transactions crimes in Indonesia.*

**Keywords:** Cyber Security, Regulation, Law Enforcement, Financial Transaction, Crime.

## INTRODUCTION

In recent decades, Indonesia has a high potential for digital transactions when compared to other ASEAN countries (Pangestu & Dewi, 2017). The results of a study from Google, Temasec, and Bain & Company in 2020 show that Indonesia is the country with the highest digital economic transaction value in the region, reaching US\$ 44 billion and is predicted to reach US\$ 124 billion in 2025 (Sitanggang & Winarto, 2020). Therefore, of course there must be a central financial institution that monitors digital transactions, which has a role and duty as a regulator to oversee digital-based financial transactions in Indonesia. The purpose of the establishment of the institution is to monitor and detect potential risks that can arise, so that they can be immediately addressed when problems occur (Rasyida, 2020).

The existence of a regulator can be present to oversee all digital-based financial transactions, from detecting the number of digital transactions in circulation to recording in financial reports, so that transaction traffic and its value can be truly known and reported in detail by all financial institutions in Indonesia (Prawirasasra, 2018). Through this mechanism, the government can take a role in overseeing every digital financial transaction, preventing and overcoming cyber crimes that occur in the financial system in Indonesia. The main goal of this policy, of course, is to protect consumers and local businesses from various cyber crimes that may occur in digital-based financial transactions from the background to law enforcement process (Hidayat, 2020).

For instance, President Joko Widodo recently emphasized that eradicating money laundering is very important to maintain the integrity and stability of the economic system and financial system stability during the handling of the Covid-19 pandemic and national economic recovery (Rahman, 2020). He urged that all stakeholders of the anti-money launderings and prevention of terrorism financing regimes have to continue to anticipate developments and conditions that could disrupt the integrity and stability of the economic system and financial system in Indonesia (Vishnum, 2020). He also says that this is related to the government's efforts to fix the shadow economy, including dealing with various economic crimes more effectively, especially cybercrimes that exploit technology. At least there are several government institutions in Indonesia that have the authority and duty to oversee criminal acts of digital-based financial transactions, such as the Supervisory and Regulatory Agency (LPP), Law Enforcement Institutions, and the Center for Financial Transaction Reports and Analysis (PPATK) as financial intelligence institution (Suwiknyo, 2021).

The most interesting example of the implementation of cyber security system in Indonesia at this time is the handling of cases of money laundering which aims to find and prosecute individuals or corporations as perpetrators, also focused on finding and taking action against assets related to the crime of money laundering (Adiwijaya, 2020). Therefore, the regulation in Law Number 8 of 2010 on the Crime of Money Laundering has an instrument of delaying transactions and blocking related to assets suspected of being related to the crime of money laundering (Atikah, 2020). In addition, the Law Number 8 of 2010 also does not require prior proof of a predicate crime or a mechanism for reversing the burden of proof. This difference needs to be understood by the law enforcers when they are processing and adjudicating money laundering cases in Indonesian law (Nugroho et al., 2020).

In the anti-money laundering regime in Indonesia, there is a shift in the way in which the law is enforced, namely if in the criminal justice process the focus is generally on "*suspects*" as individuals or corporations, in the anti-money laundering regime the focus is on "*money*" or "*assets*". This shift is often termed as "*from follow the suspect to follow the money*". The object of the Crime of Money Laundering is not only "*Persons*" but also "*Assets*" (Husein, 2003). This is something that has not been fully accommodated by the Criminal Code, the Law Number 8 of 1981 on Criminal Procedure Law defined investigation is a series of actions of investigators in terms of and according to the method regulated in this Law to seek and collect evidence which with that evidence makes clear about criminal acts that occurred and in order to find the suspect (Nuryanto, 2019).

It should be underlined here that the orientation of investigations in Indonesia is also still focused on searching for "*people*" who are suspected of committing criminal acts. This is influenced by the understanding of the purpose of punishment in the Indonesian legal system, which in this context the Criminal Code which still adheres to a retributive understanding, where the purpose of imposing a sentence is retaliation for mistakes made through corporal punishment (Harahap, 2020). Based on this understanding, it will certainly be difficult to take action against assets that are known to be related to crimes, but in order to be processed, which they must first find and be found guilty of the "*owner*" of the asset. Therefore, in giving legal sanctions to perpetrators of money laundering crimes, the concept should be changed from "*follow the suspect*" to "*follow the money*" (Kurniawan, 2012).

In order to support the change in the concept, the use of sequestration and confiscation mechanisms in handling money laundering offenses is an important part of efforts to reduce crime rates (Girsang, 2014). However, this is one of the many different concepts in terms of handling money laundering offences. In addition, to cover these deficiencies, Law Number 8 of 2010 on the Prevention and Eradication of the Crime of Money Laundering, the Regulation of the Indonesian Supreme Court Number 1 of 2013 on Procedures for Settlement of Applications for Handling Assets in the Crime of Money Laundering or Other Crimes, and other provisions to regulate and facilitate the handling of money laundering crimes (Akbar, 2019).

Referring to the above background, the purpose of this paper is to explain the role of the Indonesian government to focus on developing a cybercrimes security system in the national economic and financial system through the Cyber Security Sharing Platform as Indonesia's approach in supervision of financial transaction crimes, which is in line with the national roadmap related to the development of the Indonesian financial market. This research can be categorized the normative or doctrinal legal research. The sources of the data were carried out from the number of literatures and documents that related to the research objective. Analysis of the data uses the combination of bibliographical and empirical through deductive and inductive approaches, including case, historical, comparative, and conceptual, until the formulation of the conclusion.

### **Understanding Cyber Security System**

Cyber security is the protection of systems connected to the internet, including hardware, software, and data from cyber attacks. In the context of computing, security consists of cyber security and physical security which are both used by companies to protect their data centers and computer systems against illegal access. Information security, which is designed to maintain the confidentiality, integrity and availability of data, is part of cyber security (Von Solms & Van Niekerk, 2013). Cyber security is a process or practice carried out by individuals, organizations, or companies to protect their devices, networks, programs, and data from malicious digital attacks. In practice, this sense includes various efforts such as installing firewalls, applying multifactor authentication, using secure wifi networks, making data backups, and other things that can prevent cyber criminals from accessing computers, networks, or sensitive information on a person or an institution (Stevens, 2016).

Cyber security system is also a field that continues to change and develop from time to time. This is much influenced by the rapid advancement of technology, in this system the introduction of various new devices, as well as the increasing quality and quantity of anti-cybercrimes. In other words, the success of the cyber security approach will be greatly influenced by your success in creating a strong defense system (Craig et al., 2014). Well, the best way is to set up a layered layer of protection to ensure that you will stay safe while surfing the internet. Especially in the digital era like today, everyone is very dependent on technology. Starting from the individual level to government institutions, all of them use the internet to transfer data then store their valuable information on various devices. However, both systems and networks often have security holes that can be exploited by hackers (Shafqat & Masood, 2016).

In many cases, the attackers continue to innovate and develop many types of applications to carry out digital attacks that are more massive and very difficult to detect. Based on this reasons, the concept of cyber security is not a simple concept and because the attacks tend to evolve every day as attackers become more inventive, it is imperative for Internet users to properly define the concept of cyber security and identify what good cyber security looks like (Ziccardi, 2020). Thus, the implementation of an effective cyber security system is now a must to increase the level of system or network security, so as to reduce the risk of cyber attack threats. Although the main challenge today is quite a lot of information technology companies offering programs to anticipate malware as a publicly available commodity that can make it easier for anyone to become a cyber attacker or anti cyber attacker, and maybe even more companies that offer fake security solutions and does little to defend against cyber attacks.

### **Cyber Security System Function**

Today, many IT experts and CEOs are aware that cyber security systems are very important to be protected more strongly against hacker attacks. They have seen the statistical data such as a company that went bankrupt due to a ransomware attacks in just 14 seconds. They are also all increasingly aware that a single attack can cause a business to stagnate, and even worse, bankruptcy. If a company only sees a cyber security system as an additional budget for IT infrastructure, of course, it will be worth the impact and benefits (McIntosh, 2015).

In fact, cyber security systems have proven to play a very vital role in the growth of a company's business. For example, according to survey in 2014, 84% of consumers are apathetic when their data is taken when they are buying something on the internet. But now the situation is very different, which according to research conducted by Vodafone recently showed 89% of company stakeholders agree that increasing cyber security system based on the consumers feel more loyal and trust the company (Benzie et al., 2014). The important thing here is business partners and potential investors also want to ensure a company has a high level of security before building or sharing data (Kouttis, 2016).

There are at least three reasons why a business company needs a strong cyber security system will have an advantage over competitors who have the opposite view, such as: first, cyber security system is very important to develop company strategy. A strong cyber security system will create a foundation for the company for other strategies such as migrating data and applications to the cloud and to expand its business wings more broadly; second, cyber security system is very important for individual data access. In this case, any personal data that has been inputted into the database and stored in the data bank becomes a reference source of information that can be used to conduct business contracts with other individuals, or between individuals and companies; third, the cyber security system is very important for exchanging information between institutions. Interconnection through the internet network is currently very easily accessible, and of course, it is very vulnerable to hacker attacks. Thus, some institutions require the sharing of information related to user data (Baldassarre et al., 2019).

In addition, the function of the cyber security system is commonly used by every business institution today to protect all user data safely. The use of a cyber security system is needed for several reasons, such as: first, for individuals, cybersecurity means that their personal data will not be accessible to anyone except themselves or other people who have access. This is

necessary to keep their computer devices working properly and free of malware; second, for small business owners, cyber security to ensure credit card data is properly protected and consumer data security is protected; third, for online business owners, cyber security will protect their servers from unknown accesses from the outside; fourth, for shared service providers, cyber security will protect many of their data centers that house servers, and in turn accommodate many virtual servers that belong to different users or companies; and fifth, for the government, cyber security will build different data classifications that have their own laws, policies, procedures, and technologies (Kaplan et al., 2015).

Then in terms of its objectives, the computer experts explained several purposes of using a cyber security system as a database consist of several points: first, confidentiality, which refers to the term to ensure that information is not confidential, or freely available unauthorized entities (people, organizations, computer process etc.). Do not worry about confidentiality and privacy because confidentiality is a subset of privacy, which specifically protects data from unauthorized entities, while privacy is a broader term for lag; second, integrity is a term for accurate and complete data. Integrity also includes ensuring non-repudiation, which means that data created cannot be disputed for authenticity or accuracy. Cyber attacks that alter data will damage integrity; and third, availability, which is to ensure all informations protected and the system used to store or process it can function properly to achieve specific benchmarks. In this regards, for people who are not very familiar with cybersecurity systems will consider availability as a secondary aspect, but in fact, ensuring availability is an important part of cybersecurity, so maintaining an availability is more difficult than confidentiality or integrity (Boiko et al., 2019).

In the context of legal protection for consumers, providing personal data to companies – even if the company already has a cyber security system that is considered very well – does not seem to be safe from hacker attacks. There are several risks that need to be considered by companies when implementing a cybersecurity system (Mat et al., 2019), such as: first, the risk of individuals potentially being misused, leaked, sold, or shared by unscrupulous users of the company's database to other parties in need; second, the financial risk of potential losses due to hacking. Direct financial losses can include the loss of money from an account by a hacker, of course these financial losses will cause a loss of consumer confidence in companies whose security systems are weak; third, professional risk in the form of dismissal has the potential to be experienced by C-Level stakeholders because they are careless in maintaining the company's system security tools that are too easy to break into by a hacker; fourth, the business risk in the form of material loss has the potential to be experienced by the company because the cyber security system is too easy to break into by hackers, thereby reducing the level of trust of investors or business partners to the company; and fifth, personal risk in the form of confidential data belonging to someone, ranging from explicit photos and other activities that are very vulnerable to being broken into and misused, sometimes even having implications for damaging personal relationship with other people.

Besides that, there are several benefits of using a cybersecurity system both in terms of business and security (Cloud, 2020), such as: first, it remains flexible. It must be remembered that cybersecurity is not a one-time thing and then done. IT threats and business ecosystems must continue to evolve, so that a cyber security strategy where everyone will follow suit; second, adapting best practices to meet needs. There are many resources that can help one build cybersecurity, including best practice guides and existing frameworks. However, he can

immediately implement it with a standard cyber security strategy because it doesn't necessarily match the company. Therefore we must understand the requirements and infrastructure, then adapt accordingly; third, involve stakeholders. To build a program requires collaboration between IT and C-Level stakeholders. These stakeholders have a broad and clear understanding of the company's priorities and goals, so they can provide additional ideas for building cybersecurity. The company leaders also need their sponsorship in the form of budget support and other resources to ensure cybersecurity is running properly; and fourth, comprehensive: A comprehensive cybersecurity system strategy will cover many aspects such as data management, business process management, enterprise risk planning, user authorization, data sharing and protection, including to prevention if the problems arise. Shortly, there are many benefits and uses of cyber security systems to protect all data, information, networks, and very important assets belonging to individuals, groups, or companies.

### Cyber Security System Threats Types

Cyber security system is the process of protecting systems, data, networks, and programs from digital threats or attacks (Cisco, 2020). These attacks are generally carried out by irresponsible parties for various purposes. Some examples are accessing sensitive information, making content changes, or even changing and destroying important data. The motive may be to disrupt a business or it may be to extort large sums of money (Aliya, 2020). Most information technology experts consider cybersecurity the same as information security or commonly called InfoSec. Yet they are two different things. InfoSec is more understood as an important element of a cyber security system that has a specific function to handle data security, while cyber security system is more understood as a big umbrella of InfoSec and other elements. In this regards, internet observers in TechTarget explained a lot about the various threats that may be faced in cyber security systems (Shea et al., 2020), such as follows:

#### Malware

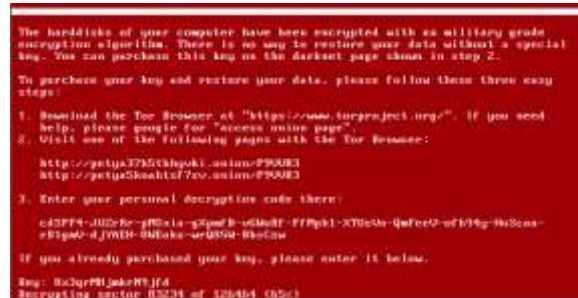
Malware is the first type of threat that most disrupts cyber security systems. This threat is usually in the form of malicious software that can annoy and harm computer users (Figure 1). Malware can harm system applications on computers and their users through the spread of computer viruses, spyware, worms, and many more (Idika & Mathur, 2007).



**FIGURE 1  
MALWARE**

## Ransomware

Ransomware is the second type of threat that can interfere with cyber security systems. Ransomware is generally a form of malicious software, but it is more extreme than just spreading viruses (O'Gorman & McDonald, 2012). Hackers will usually block access to someone (the account owner) to open a computer or important document. The only way to get him back into the computer is to pay the ransom demanded by the hacker (Figure 2). Even so, paying this amount of money also does not ensure that the files or computer systems that were taken over can return to normal (Richardson & North, 2017).



**FIGURE 2**  
**RANSOMWARE**

## Social Engineering

Social Engineering is the third type of threat that can disrupt cyber security systems. This term is used to describe attacks based on human interaction. In computer sciences, social engineering is understood as an important branch of information security, which the discipline is not well defined, because there are a number of different definitions appear in the literature (Salahdine & Kaabouch, 2019). Social engineering is commonly used by hackers to manipulate user data by providing sensitive information, such as passwords, answers to security questions, and more (Figure 3). This type of threat usually takes advantage of human curiosity and provokes it to do things that may feel normal, but are actually dangerous (Aldawood & Skinner, 2018).



**FIGURE 3**  
**SOCIAL ENGINEERING**

## Phishing

Phishing is the fourth most common type of threat to disrupt cyber security systems. Phishing is a form of fraud that is usually present via email in the form of Spam, where a fraudster will send an email using an address that is similar to a trusted source. Even so, there are one or two different letters that are usually invisible to the naked eye. This scam aims to steal sensitive data such as credit card security numbers, passwords, and other important information (Baykara & Gürel, 2018). Shortly, if you get the desired email, the email sender will require someone to enter sensitive data (Figure 4). Therefore, every person who receives an email message in the form of spam, he must always ensure the credibility of the sender of the email (Buber et al., 2017).



**FIGURE 4  
PHISHING**

## Cyber Security Sharing Platform in Indonesia

Currently, the Indonesian government has owned and implemented a financial cyber security system in the form of a Cyber Security Sharing Platform. This system was created as a tool to protect the financial sector payment system from various threats of cyber attacks. According to the Deputy Governor of Bank Indonesia (BI), Doni Primanto Joewono who explained in online discussion broadcasted on the Bank Indonesia YouTube Channel that the cyber security sharing platform is used as a means to share information about cyber threats and cyber incident mitigation, between organizations and institutions that are included in the financial ecosystem and payment system in Indonesia (Joewono, 2021). For example, he explained that currently, Bank Indonesia already has a Cyber Security Sharing Platform and Bank Indonesia has asked every financial institution for all payment systems to share information.

Every bank that detects a cyber threat or experiences a cyber incident is required to report it via email at CSPP-SP@bi.gp.id. Each incoming report will be analyzed and shared with other organizations via the Cyber Security Sharing Platform as material to improve cyber security and



prevent attacks. This platform is processed by Bank Indonesia itself, which includes filtering, formatting, and any attack analysis will be shared by other banks. In addition, any information provided by the organization through sharing platforms, especially those that are vulnerabilities, threats, incidents, and others, are equipped with sharing traffic protocol rules. This rule regulates all informations that can be shared with the public, among related organizations, between Bank of Indonesia and the sender of information only, or between CSSP members only. The main hope to be achieved from using this cyber security sharing platform is that every organization that is included in the digital economy ecosystem can improve its cyber security (Ulya & Jatmiko, 2021).

Furthermore, in recent years, fintech has continued to grow rapidly in Indonesia. The pattern of financial transactions does not only rely on conventional patterns but is now increasingly shifting to fintech. With the increasingly connected between banks and also fintech in financial transactions, it will certainly be very vulnerable to cyber threats. Based on data held by Bank Indonesia, recently there has been a significant increase in cyber attacks on the financial sector, reaching almost 70 percent. The consequence of this integration and collaboration between banks and fintech is that sensitive and responsive policies and actions are needed to ward off these cyber attacks. Therefore, Bank Indonesia as the regulator of the banking system in Indonesia is very concerned about strengthening the cyber security sharing platform in order to build a secure digital financial ecosystem (Suud & Sandy, 2021).

In addition, although in general the financial industry players have governance and capabilities in cyber risk management, it is still necessary to strengthen standard certification, adequacy of human resource capabilities, fraud risk management, the role of third parties, and the establishment of a cyber security operation center for the financial sector. To support this security, Bank Indonesia also cooperates with the National Cyber Encryption Agency (BSSN) and related industries to synergize together in developing security in the financial transaction system in Indonesia.

### **Constraints of Cyber Security Sharing Platform in Indonesia**

Among the most decisive problems faced by Indonesia in implementing the cyber security sharing platform is the shortage of talented personnel who have expertise in the field of cyber security systems. This raises very real problems in the strategic industry, defense, national unity and business. An illustration describes the possibility that if Indonesia faces a cyber war, the number and tactical capabilities of the Cyber Army in Indonesia may still be very limited to be able to defend and strengthen the nation's defense system (Yunita, 2020).

In this regard, the Indonesian government must increase the strength and capabilities of human resources in proportion to the progress and strength of technology itself. Moreover, in the industrial world, such as banking, telecommunications, and government agencies, it is a very vital need, where all countries in the world today have used information technology as a basis of strength and at the same time economic progress. It should be realized that information technology will continue to grow rapidly every year in the future without limits. In various kinds of information technology problems, the element of human resources plays a major role. Therefore, every country needs to prepare to prevent various inequalities that may arise as a result of the rapid development and advancement of information technology.

Referring to the results of previous surveys, according to Eva Noor, CEO of PT Xynexis International, she explained that the world currently needs at least 15 million experts for cyber security systems. Indonesia now needs around 1000 cyber security experts outside of officers for various needs of government agencies, industry, banking, telecommunications, and so on. To address and overcome this, it is necessary to make a breakthrough so that there is no gap between the advancement of information technology and human resources or special supervisory personnel in the IT field, PT Xynexis gave birth to a new innovation with the idea of the Born To Control program in collaboration with The Indonesian Ministry of Communication, Information and Telecommunications (Kominfo) in applying and running the program for the wider community (Noor, 2017).

For example, in the last three years, PT. Xynexis has partnered with Kominfo to search for talent among young people interested in the Born to Control program. It is possible, in the future, to collaborate with various government agencies in Indonesia, such as the Ministry of Defense, Ministry of Maritime Affairs, Ministry of Nasional Education, Bank Indonesia, Financial Institutions, and other government-owned agencies, including private parties such as automotive, telecommunications, banking, insurance, and industry players who are seen to be able to partner in this program.

Born to control is a cyber security talent search program in Indonesia, with the aim of attracting a minimum of 2000 human resource talents in the field of cyber security systems for 2017 in information technology today. In addition, the need for cyber security system supervisors is also still needed to provide supervision and guidance to cyber security system operators. This program ideally has a junior or senior secondary education background to higher education that has qualifications and competencies in the IT field, especially a Bachelor of Information Technology where informatics engineering is the main subject at the university (Yovita, 2017).

In the talent search process, PT. Xynexis together with Kominfo in 2017 carried out awareness-raising in five cities in disseminating the program that was initiated with the hope that it would continue in other cities in the following year. Awareness referred to here aims to invite all levels of society at large, especially the younger generation who are interested in cyber security programs. Especially for the talent search program in this cyber security system, you don't have to understand IT, because just having an interest is enough which will then be gathered and given special training at the bootcamp which will be held for 2 weeks in the second stage in recruiting candidates. From the 2000 participants, it is hoped that the 100 best people in each region will be selected and given character building and special training with international standards. The coaching aims to create good personnel are not only their IT skills, but also to produce a good mindset from a candidate who is elected in the future. This character building is very necessary because many people are smart and have excellent IT skills, but there are a lot of people who find these skills used in things that are not good or negative. In other words, building the mindset of human resources in the IT field can at least defend themselves while also being a retainer and defender of the state in the face of various cyber attacks or other serious threats in the future.

In the talent search program, the targeted targets for the Born to Control recruitment process are all Indonesian citizens, aged 16 years and over, and those with high school education up to college. Everything starts from the initial/basic, intermediate, and advanced test processes.

Although the candidates who participate have a high school education background and do not continue to college, they are considered very talented and have strong motivation, of course there is a very high possibility that they will be selected and selected as the main candidate Those who are selected will be re-selected to be the best candidates, and will receive appreciation in the form of educational scholarships. In addition, they will also be given access and the opportunity to work for various companies or agencies in need.

The limited human resources and skills in Indonesia are still the toughest challenges with a share of 36%, surpassing limited investment funding (31%), low access to a robust technology ecosystem (20%), government policies or regulations (17%), and security issues cyber (15%). Of course, In terms of its benefits, the Born to Control Program is clearly very important to continue to be held so that there is no imbalance between advances in information technology and the availability of human resources. This program will also provide many benefits for the government to no longer import or bring in experts from abroad to handle various cyber security system problems in Indonesia. If the policy is not populist way, it will be very detrimental, and endanger the defense and security of the country (Abdillah, 2019).

This is a dilemma that arises in Indonesia today, where on the one hand Indonesia needs the development of information technology in the field of business industry and governance, but on the other hand, its human resources are still very limited. In short, the Cyber Security Sharing Platform with all its derivative programs can be said as a concrete effort by the Indonesian government to no longer depend on foreign experts, but to prioritize the development of the quality of domestic resources with the general aim of maintaining the confidentiality of data, information, sovereignty, defense, and national security. The most basic thing from the government's efforts is to build and grow the mindset of cyber security system retainers in Indonesia to take part in counteracting all forms of attacks (cyber wars) that may occur at any time.

### **Strategy and Policy on Cyber Security Sharing Platform in Indonesia**

As explained at the beginning of this paper, Indonesia is the country with the highest digital economic transaction value in the ASEAN region, reaching US\$ 44 billion and is predicted to continue to rise in 2025 to reach US\$ 124 billion. With the largest population and internet users in the ASEAN region, Indonesia is committed to increasing economic recovery efforts from the impact of the COVID-19 pandemic and promoting long-term economic growth through digitalization support and a more sustainable approach. This was raised at the 7th Annual Meeting of the Ministers of Finance and Governors of the ASEAN Central Banks which was held virtually on March 30, 2021.

According to Haryono, Head of the Communications Department of Bank Indonesia, explained that as a form of Indonesia's commitment to strengthening future economic resilience, the Indonesian government has agreed on several commitments to strengthen support for the digitalization of the national economic and financial system together with other ASEAN countries (Haryono, 2021), such as follows:

1. Welcoming the various policy steps that have been implemented quickly and on a large scale by ASEAN member countries, including fiscal and monetary policies, to restore the economy and maintain financial stability from the impact of the Covid-19 pandemic;
2. Completing the transition work plan from the ASEAN Framework Agreement on Services (AFAS) to the ASEAN Trade in Services Agreement (ATISA) and ensure a commitment to open market access in the financial services sector that is more substantive and meaningful in the 9th AFAS Protocol. The 9th AFAS protocol is the last protocol before the transition to ATISA and is planned for co-signing;
3. Preparing the strategic steps towards banking integration in the ASEAN region in the digital era through the refinement of the ASEAN Banking Integration Framework (ABIF) Guidelines;
4. Continuing the commitment to facilitate the flow of capital traffic in the ASEAN region through the gradual elimination of restrictions, monitoring and regular policy discussions, as well as increasing the capacity of human resources;
5. Promoting the linkage of payment systems in the ASEAN region to facilitate trade, business, and financial inclusion;
6. Developing the ASEAN Taxonomy for Sustainable Finance which will be a guide and common language for all member countries in developing an environment-based financial and financing system;
7. Supporting the ASEAN Sustainable Banking Principles initiative which will serve as a guide for central banks in ASEAN in developing environmentally-based banking practices that are in accordance with the conditions in each country;
8. Continuing the efforts to develop financial inclusion in ASEAN, including through monitoring and evaluation activities as well as developing guidelines on digital financial literacy policies;
9. Appreciating and supporting the operation of the ASEAN Cybersecurity Resilience and Information Sharing Platform (CRISP) as a means of exchanging information among ASEAN central banks in dealing with cybersecurity threats and developing joint mitigation measures.

The main role of the Indonesian government in strengthening digital-based financial transaction policies also received appreciation and support from several international institutions that were present at the meeting, including: Asian Development Bank (ADB), Asian Infrastructure Investment Bank (AIIB), ASEAN+3 Macroeconomic Research Office (AMRO), the World Bank (WB), and the International Monetary Fund (IMF), as well as from several business organizations, namely the ASEAN Business Advisory Council, the EU-ASEAN Business Council, and the US-ASEAN Business Council.

During its development, the Indonesian government took several concrete steps related to strengthening regulations in the field of cyber security systems. For example, the legal basis for regulating cybersecurity system in Indonesia is the Electronic Information and Transactions Law Number 11 of 2008 and its revised with the Law Number 19 of 2016 (EIT Law). The EIT Law covers several offenses, such as distributing illegal content, breach of data protection, unauthorized access to another computer system to gain information, and an illegal and unauthorized interception or wiretapping of other computer systems or electronic systems. The EIT Law provides legal protection for content of electronic systems and electronic transactions. However, the EIT Law does not cover important aspects of cybersecurity, such as information and network infrastructure, and human resources with expertise in cybersecurity (Anjani, 2020).

Based on the EIT Law from 2016, the government of Indonesia issued technical regulations in Government Regulation Number 71 of 2019 on the Implementation of Electronic Systems and Transactions (GR 71 of 2019). This regulation contains updates related to the implementation of cybersecurity in electronic systems and transactions. Apart from several articles related to the offences regulated by the EIT Law, It also contains stronger provisions regarding the protection of personal data and information and website authentication to avoid

fake, fraudulent or scam websites. Besides that, it also emphasizes the need for the government to prevent any harm to public interests through the misuse of electronic information and electronic transactions and the need to develop a national cybersecurity strategy. However, it covers only cybercrimes that are related to electronic transactions, such as the misuse of data, unauthorized electronic signatures, and the spread of malicious viruses and codes. The limited coverage of the EIT Law and GR 71 of 2019 provide an inadequate response to everchanging cyberthreats, particularly those to the government's critical infrastructure.

To deal with cyberthreats to the national security, the Ministry of Defence Regulation Number 82 of 2014 provides cyber defence guidelines. It is the only regulation that provides a definition of cybersecurity: National cybersecurity comprises all efforts to secure the information and the supporting infrastructure at the national level from cyberattacks. Any words or actions done by any party that threaten national security, national sovereignty, and territorial integrity are considered cyberattacks. Unlike the EIT Law, the regulation covers critical infrastructure of, for example, the financial and transportation systems as objects of cybersecurity. However, the regulation only serves to develop military cyber defence capacities, developed and implemented by the Ministry of Defence for the National Armed Forces. For non-military cyberthreats, it refers to other regulations, such as the EIT Law.

Furhermore, in subsequent developments, especially after discussions of the Bill were initiated in May 2019, the academic research for the Bill was uploaded for public viewing by the DPR in June 2019<sup>5</sup>. While the academic paper was made available to the public, the Cybersecurity Bill itself was never uploaded to the internet. This led to an online petition<sup>6</sup> criticizing the closed policy-making process. The petition called for postponing the Cybersecurity Bill and requested involving the private sector and the academia in the deliberations. Thus, the Bill had also not involved relevant government institutions, such as MOCI and National Development Planning Agency (Aprilianti & Dina, 2021).

The closed policy-making process and the exclusion of the private sector resulted in articles that potentially hinder innovation and the development of cybersecurity services and products. Articles of the Bill stipulated certification requirements for businesses that plan to develop cybersecurity services and products for the government procurement process. However, these requirements might have duplicated requirements already stated in other laws and regulations. Article 17 of the Bill required businesses to get BSSN certifications for the products they want to offer for cybersecurity. Articles 19 and 21 required that human cybersecurity resources need to meet BSSN standards and acquire certifications from organizations accredited by BSSN. It remained unclear whether these certifications were the same as those stipulated by the ITE Law under the mandate of MOCI. If they had not been identical, the Bill would have added compliance costs for the private sector and created redundancies of these certifications. This would have disproportionately affected small and medium-sized enterprises with less institutional compliance capacities (Anjani, 2020).

Smaller companies will also be affected by BSSN Regulation Number 8 of 2020 on Security Systems in the Implementation of Electronic Systems, which was issued in December 2020. It is a technical regulation requested by Article 24 of GR 71 of 2019. BSSN Regulation Number 8 of 2020 lays out the need for operators of electronic systems (public and private) to ensure the safety of their information management. The regulations require electronic system operators to employ an individual security expert (local or foreign) or a consulting agency to

oversee the implementation of their electronic systems. However, there is no explanation of what qualifications these experts or agencies need according to BSSN standards. The draft of the Cybersecurity Bill followed the same requirement and did not elaborate on the required expertise.

Besides those product certifications, Article 48 of the Cybersecurity Bill mandated BSSN to issue permits for conducting research on, or testing cybersecurity applications. This added further confusion as the article did not determine which activities in research or testing of cybersecurity require a permit from BSSN. Thus, article 66 of the Cybersecurity Bill required businesses to meet local content requirements, more specifically, a domestic component level (TKDN) of 50%. Since most businesses use foreign hardware and software in their products and services, the required 50% TKDN would have affected the development of cybersecurity products and services in Indonesia. All mentioned articles appeared to contradict the aim of increasing cyber competitiveness and innovation through cyber utilization that is free, open, and responsible as stated in Article 3 (b) of Cybersecurity Bill. This aim can only be achieved in a meaningful dialogue with all relevant stakeholders from the corporate sector, the academia and the civil society (Anjani, 2020).

Referring to the description above, transparency is one of the principles established by Law Number 12 of 2011 on the Formulation of Law and Regulations in Indonesia. It is being manifested by disseminating the draft law to inform the public and to get input from the public and relevant stakeholders. Besides, the public has the right to provide input orally and in writing in the legislative process. The law also lays out several ways for the public to give input, including public hearing meetings, work visits, socialization, seminars, workshops, and discussions. The closed policy-making process of the Cybersecurity Bill was criticized for not complying with this law.

### **Law Enforcement on Financial Transaction Crimes in Indonesia**

The investigators from the Criminal Investigation Unit of the Indonesian National Police noted that the number of financial transaction crimes caused by cyber security attacks was still quite high. During the 2019-2020 periods, it reached 159,937,542 cases. This number experienced a very significant increase when compared to 2019 which reached 39,330,231 cases. Until now, the police of the Republic of Indonesia are still investigating various cyber crimes, which generally occur in the form of breaking into customer accounts at a number of large banks in Indonesia by using internet banking software. The main perpetrators are usually carried out by national and international syndicates who are very familiar with the cyber security system in Indonesia so that they use the crime mode of breaking into bank customer accounts which results in financial losses (Djumena, 2020).

Based on the results of the analysis and findings of investigators at the Indonesian National Police Criminal and Investigation Agency, it is known that the perpetrators of criminal acts of digital-based financial transactions are generally international syndicates that use several modes as follows: first, the case began when the perpetrator offered an antivirus application device through a service message. on the internet to victims of e-banking users to download them; second, the perpetrator then uses malware to manipulate the menu display and steal bank customer data that is implanted through the internet network; third, the perpetrator hijacks the

internet banking account of the bank customer so that when the customer is about to deposit money into his account, the flow of money will be diverted to the perpetrator's account; fourth, the perpetrator can easily control the customer's e-banking account after knowing the victim's password; and fifth, the perpetrators are generally not Indonesian citizens, but instead use the courier service of a Non-Indonesian Citizen, then the perpetrator of the Non-Indonesian Citizen transfers the stolen money back to the account of the perpetrator who was recruited from among Indonesian Citizens Figure 5 (Simanjuntak, 2020).



**FIGURE 5**  
**CYBER ATTACKS IN INDONESIA**

Indonesia is recognized as one of the countries with the largest number of internet users in the world and will become an easy target for digital-based (online) crimes, especially many people who still use fake software, so they are very vulnerable to being hacked by hackers. According to Irwan Lubis, Deputy Commissioner for Banking Supervision of the Financial Services Authority (OJK), he admitted that his party had not received reports from the bank, the Criminal Investigation Unit of the Indonesian National Police, and other institutions regarding on the cases of burglary customer funds at a number of banks in Indonesia. He also emphasized that OJK had asked all banks in Indonesia to increase the level of cyber security system security in all forms of digital-based bank services (Figure 6). The reason is the high number of crimes against cyber security systems in financial institutions generally seems to be directly proportional to the number of internet users in Indonesia, which reaches 63 million users (Lubis, 2021).



**FIGURE 6**

## INTERNET USSERS IN INDONESIA

From 2019 to present, the Indonesian National Cyber and Crypto Agency reported 290 million cases of cyberattacks. That was 25% more than the previous year, when cybercrimes had caused losses of USD 34.2 billion for Indonesia. The Covid-19 pandemic in 2020 triggered a significant increase in phishing attacks, malspams and ransomware attacks, adding to the urgency of establishing a well-functioning infrastructure for cybersecurity in Indonesia. Therefore, Indonesian cyber security laws and regulations have to create the fragmented responsibilities across different ministries and they remain ineffective in preventing cyberthreats and cybercrime through a comprehensive regulation and law enforcement efforts. In this regards, there are at least several institutions that are directly related to law enforcement efforts in eradicating criminal acts of digital-based financial transactions in Indonesia, including: Bank Indonesia, Financial Services Authority, Police, Attorney General's Office, Supreme Court, Ministry of Communication and Information, Ministry of Finance, Ministry of Defense, the State Intelligence Agency, and the National Cyber Encryption Agency (Ramli & Movanita, 2020).

The first example of law enforcement for money laundering cases is the Kuala Simpang District Court Decision Number: 212/Pid.Sus/2020/PN.Ksp dated January 28, 2021. This case begins with a report based on an analysis or examination of reports and information on Financial Transactions containing indications of criminal acts of money laundering and/or other criminal acts as referred to in Article 2 paragraph (1) page 144 of 219 in the Court Decision Number: 212/Pid.Sus/2020/PN.Ksp, which is strengthened by statements from PPAATK officials who have provided assistance law, including providing expert information, especially in the field of prevention and eradication of money laundering crimes for the purpose of examination. The main points of the case that were proven in the trial showed that there was a criminal element of money laundering with the aim of hiding or disguising the origin of assets. In accordance with the opinion of Expert Hardi Setiyo, SH from the Center for Financial Transaction Reports and Analysis (PPAATK) gave the opinion that in the perspective of money laundering, the act of a criminal act of borrowing or using another person's account to accommodate, place, and/or transfer the assets resulting from the crime. Crime is seen as an attempt to hide or disguise the origin of wealth.

In the consideration, the Panel of Judges refers to Article 39 of the Law Number 8 of 2010 on Prevention of the Eradication of the Crime of Money Laundering, which the Article 40 of this law provides the firm and clear evidence. Finally, the panel of judges had decided that the Defendant (Kamal alias Kmel) was declared legally and convincingly guilty of committing the crime of money laundering. The Perpetrator was also given a prison sentence of 7 (seven) years and a fine of IDR 1.000.000.000,- (One billion rupiah) with the provision that if the fine is not paid, it will be replaced with imprisonment for 6 (six) months. In addition, all assets obtained from the proceeds of money laundering are confiscated into the property of the State.

The second example is committing a crime of false recording in financial statements as shown in the South Jakarta District Court Decision Number: 322/Pid.Sus/2019/PN JKT.SEL dated July 24, 2019. This case began when the Defendant (Mamnua) had made a false record by asking an employee of Bank Mandiri Micro Unit Mandiri Bintaro, South Jakarta who has a password, namely witness Santi Arini, S.E., as a Credit Analyst to change the due date of credit installments for borrowers in the financial recording system, so that the installments of debtors in



the Mandiri Micro Portfolio look smooth and good, even though in fact the loan installments managed by the Defendant were in default.

In the consideration, the panel of judges succeeded in finding the facts revealed in the trial that the defendant was proven knowingly and intentionally to have made or caused false records in the books or in the reporting process and in documents or reports on business activities, as stated on page 46 of 55 in the Court Decision Number: 322/Pid.Sus/2019/PN JKT.SEL has fully complied with all elements of the crime of financial transaction crime as regulated in Article 49 paragraph (1) letter (a) of Law Number 8 of 2010 concerning Prevention and Eradication of the Crime of Laundering Money. Finally, the panel of judges decided that the Defendant (Mamnua) was declared legally and convincingly guilty of committing a criminal act, and the bank employee (Santi Arini, S.E.) was found guilty of intentionally making or causing false records in the books or in the reporting process, and in documents or business activity reports, transaction reports or bank accounts, and money laundering. Finally, both were given a prison sentence of 5 (five) years and a fine of IDR 10.000.000.000,- (ten billion rupiah) with the provision that if the fine was not paid, it was replaced with imprisonment for 2 (two) months. In addition, the panel of judges also stipulates that the period of arrest and detention that has been served by the Defendant is deducted entirely from the sentence imposed with a clause stipulating that the Defendant remains in custody, and stipulates all the evidence mentioned in the verdict.

The two examples of court decisions above have at least provided a concrete picture that the Indonesian government has carried out very serious law enforcement efforts in eradicating every criminal act of financial transaction crime, whose main purpose is as an effort to preventive effect and at the same time provide a deterrent effect for each Perpetrator. Shortly, the strategies and policies of the Indonesian government through strengthening regulations, law enforcement, and implementing the Born to Control Program through the implementation of the Cyber Security Sharing Platform have proven positive implications in dealing with various cyber-based threats and attacks.

## CONCLUSION

At the end of this paper, the following conclusions can be formulated: first, with all its advantages and disadvantages, cyber security systems are an absolute necessity that must be owned by the State and companies to protect data and various important informations in order to avoid all forms of digital-based attacks (cyber. crimes); second, several threats that may be faced in the cyber security system, namely malware, Ransomware, social engineering, and phishing; third, Indonesia already has a cyber security sharing platform that is used to share information about cyber threats and cyber incident mitigation, between organizations and institutions that are included in the financial ecosystem and payment system; fourth, the most decisive problem faced by the Indonesian government in implementing the Cyber Security Sharing Platform is the shortage of talented personnel who have expertise in the field of cyber security systems; fifth, strengthening regulations, law enforcement, and implementing the Born To Control Program is a strategy and concrete policy of the Indonesian government in overcoming any potential criminal acts of digital-based financial transactions and at the same time providing the need for skilled human resources in managing the Cyber Security Sharing Platform; Sixth, there are several institutions that are directly related to law enforcement efforts

in eradicating criminal acts of digital-based financial transactions in Indonesia, including: Bank of Indonesia, Financial Services Authority, Police, Attorney General's Office, Supreme Court, Ministry of Communication and Information, Ministry of Finance, Ministry of Defense, the State Intelligence Agency, and the National Cyber Encryption Agency; and seventh, the main objective of law enforcement is to preventive effect and provide a deterrence effect to every Perpetrator of criminal acts of financial transaction crimes in Indonesia.

## ACKNOWLEDGMENT

This paper is the result of competitive research that has been systematically and comprehensively compiled in accordance with academic norms and a rule, free from conflict of interest, and has been presented at the national workshop on law enforcement preventing criminal acts of financial transactions at UIN Sunan Gunung Djati Bandung, West Java, Indonesia, on 10 July 2021.

## REFERENCES

- [Abdillah, A. F. \(2019\). \*The challenges of running cyber security in Indonesia\*. Retrieved from https://www.indotelko.com/read/1561689578/cybersecurity-di-indonesia](https://www.indotelko.com/read/1561689578/cybersecurity-di-indonesia)
- [Adiwijaya, S. \(2020\). \*BI encourages digitalization of Islamic economy and finance\*. Retrieved from https://www.tagar.id/bi-dorong-digitalisasi-ekonomi-dan-keuangan-syariah](https://www.tagar.id/bi-dorong-digitalisasi-ekonomi-dan-keuangan-syariah)
- [Akbar, D. L. \(2019\). Criminal law policy in handling digital asset-based money laundering in Indonesia. \*Journal of Law and Legal Reform\*, 1\(1\), 129-176.](#)
- [Aldawood, H., & Skinner, G. \(2018\). Educating and raising awareness on cyber security social engineering: A literature review. In \*2018 IEEE International Conference on Teaching, Assessment, and Learning for Engineering \(TALE\)\* \(pp. 62-68\). IEEE.](#)
- [Aliya, H. \(2020\). \*Completely peel cyber security and the ins and outs\*. Retrived from https://glints.com/id/lowongan/cybersecurity-adalah/#.YN1v\\_aoxXIU](https://glints.com/id/lowongan/cybersecurity-adalah/#.YN1v_aoxXIU)
- [Anjani, N.H. \(2020\). \*Policy brief: Cybersecurity protection in Indonesia\*. Retrieved from https://www.cips-indonesia.org/post/policy-brief-cybersecurity-protection-in-indonesia](https://www.cips-indonesia.org/post/policy-brief-cybersecurity-protection-in-indonesia)
- Aprilianti, I., & Dina, S. (2021). Co-regulating the Indonesian digital economy. *Center for Indonesian Policy Studies*. Retrieved from https://repository.cips-indonesia.org/publications/332998/co-regulating-the-indonesian-digital-economy
- [Atikah, I. \(2020\). Consumer protection and fintech companies in Indonesia: Innovations and challenges of the financial services authority. \*Jurnal Hukum dan Peradilan\*, 9\(1\), 132-153.](#)
- [Baldassarre, M. T., Santa Barletta, V., Caivano, D., Raguseo, D., & Scalera, M. \(2019\). Teaching cyber security: The hack-space integrated model. In \*ITASEC\*.](#)
- Baykara, M., & Gürel, Z. Z. (2018). Detection of phishing attacks. In *2018 6th International Symposium on Digital Forensic and Security (ISDFS)* (pp. 1-5). IEEE.
- Benzie, J., McCarter, D., & Ko, R. (2014). *Cyber security NZ SME landscape: Report prepared for vodafone NZ Ltd*.
- Boiko, A., Shendryk, V., & Boiko, O. (2019). Information systems for supply chain management: Uncertainties, risks and cyber security. *Procedia computer science*, 149(2), 65-70.
- Buber, E., Dirri, B., & Sahingoz, O. K. (2017). Detecting phishing attacks from URL by using NLP techniques. In *2017 International conference on computer science and Engineering (UBMK)* (pp. 337-342). IEEE.
- [Cisco. \(2020\). \*What is cyber security system\*. Retrieved from https://www.cisco.com/c/en/us/products/security/what-is-cybersecurity.html](https://www.cisco.com/c/en/us/products/security/what-is-cybersecurity.html)
- [Cloud, I. \(2020\). \*How cyber security helps your business grow\*. Retrived from https://indonesiancloud.com/bagaimana-cybersecurity-membantu-pertumbuhan-bisnis-anda/](https://indonesiancloud.com/bagaimana-cybersecurity-membantu-pertumbuhan-bisnis-anda/)

- Craigien, D., Diakun-Thibault, N., & Purse, R. (2014). Defining cyber security. *Technology Innovation Management Review*, 4(10), 1-9.
- [Djumen, E. \(2020\). \*The mode of breaking into customer accounts through e-banking\*. Retrieved from https://money.kompas.com/read/2015/04/15/113500326/Ini.Modus](https://money.kompas.com/read/2015/04/15/113500326/Ini.Modus)
- Girsang, H. (2014). Eradication of the crime of trafficking in persons through the law on the prevention and eradication of the crime of money laundering. *Jurnal Ilmu Hukum Jambi*, 5(1), 432-487.
- Harahap, H. H. (2020). Prevention and eradication of the crime of money laundering. *Amaliah: Journal of Community Service*, 4(2), 186-190.
- [Haryono, E. \(2021\). \*Press release: Indonesia commitment to ASEAN economic recovery, digitization and sustainability\*. Retrieved from https://www.bi.go.id/id/publikasi/ruang-media/news-release/Pages/sp\\_238221.aspx](https://www.bi.go.id/id/publikasi/ruang-media/news-release/Pages/sp_238221.aspx)
- Hidayat, A. (2020). New regulation on payment system no. 22/23/PBI/2020 by central bank of Indonesia. *eCo-Bussiness*, 3(1), 1-6.
- Husein, Y. (2003). Money Laundering in International Law Perspective. *Indonesian Journal of International Law*, 1(1), 342-374.
- Idika, N., & Mathur, A. P. (2007). A survey of malware detection techniques. *Purdue University*, 48(2), 1-9.
- Joewono, D. P. (2021). *Leaders insight: Utilization of digital ID, cyber security*. Presented paper in online discussion, which was broadcast on the Bank Indonesia YouTube Channel.
- Kaplan, J. M., Bailey, T., O'Halloran, D., Marcus, A., & Rezek, C. (2015). *Beyond cyber security: Protecting your digital business*. John Wiley & Sons.
- Kouttis, S. (2016). Improving security knowledge, skills and safety. *Computer Fraud & Security*, 16(4), 12-14.
- Kurniawan, I. (2012). The development of the crime of money laundering and its impact on the economic and business sector. *Journal of Legal Studies*, 4(1), 1-9.
- [Lubis, I. \(2021\). \*The mode of breaking into customer accounts through e-banking\*. Retrieved from https://money.kompas.com/read/2015/04/15/113500326/Ini.Modus.Pembobolan.Rekening.Nasabah.Melalui.e-Banking.?page=all](https://money.kompas.com/read/2015/04/15/113500326/Ini.Modus.Pembobolan.Rekening.Nasabah.Melalui.e-Banking.?page=all)
- Mat, B., Pero, S., Wahid, R., & Sule, B. (2019). Cybersecurity and digital economy in Malaysia: Trusted law for customer and enterprise protection. *International Journal of Innovative Technology and Exploring Engineering*, 8(S3), 214-220.
- McIntosh, C. (2015). Cyber-security: Who will Provide Protection? *Computer Fraud & Security*, 15(12), 19-20.
- [Noor, E. \(2017\). \*Indonesia lacks cyber security talent\*. Retrieved from https://kominform.go.id/content/detail/8574/indonesia-kekurangan-bakat-cyber-security/0/sorotan\\_media](https://kominform.go.id/content/detail/8574/indonesia-kekurangan-bakat-cyber-security/0/sorotan_media)
- Nugroho, N., Sunarmi, S., Siregar, M., & Munthe, R. (2020). Analysis of the prevention of money laundering by bank negara Indonesia. *Arbiter: Master of Law Scientific Journal*, 2(1), 100-110.
- Nuryanto, A. D. (2019). The problem of investigating the crime of money laundering originating from the banking predicate crime. *Bestuur*, 7(1), 54-65.
- O'Gorman, G., & McDonald, G. (2012). *Ransomware: A growing menace*. Arizona, AZ, USA: Symantec Corporation.
- Pangestu, M., & Dewi, G. (2017). Indonesia and the digital economy: Creative destruction, opportunities and challenges. In *Digital Indonesia* (pp. 227-255). ISEAS Publishing.
- Prawirasasra, K. P. (2018). Financial technology in Indonesia: Disruptive or collaborative. *Reports on Economics and Finance*, 4(2), 83-90.
- [Rahman, R. \(2020\). \*Jokowi calls on fintechs to adopt good governance for enhanced cybersecurity, services\*. Retrieved from https://www.thejakartapost.com/news/2020/11/15/jokowi-calls-on-fintechs-to-adopt-good-governance-for-enhanced-cybersecurity-services.html](https://www.thejakartapost.com/news/2020/11/15/jokowi-calls-on-fintechs-to-adopt-good-governance-for-enhanced-cybersecurity-services.html)
- Ramli, R. R., & Movanita, A. N. K.. (2020). How bank Indonesia Faces cyber crime in the national economic and financial ecosystem. Retrieved from <https://money.kompas.com/read/2021/04/09/065726826/cara-bi-hadapi-kejahatan-siber-di-eksosistem-ekonomi-dan-keuangan-nasional>
- Rasyida, A. J. (2020). *Case study of financial services authority: The role of digital financial innovation in supporting financial inclusion in Indonesia an internship report*.
- Richardson, R., & North, M. M. (2017). Ransomware: Evolution, mitigation and prevention. *International Management Review*, 13(1), 10-25.

- Salahdine, F., & Kaabouch, N. (2019). Social engineering attacks: A survey. *Future Internet*, 11(4), 89-96.
- Shafqat, N., & Masood, A. (2016). Comparative analysis of various national cyber security strategies. *International Journal of Computer Science and Information Security*, 14(1), 129-134.
- [Shea, S., Gillis, A.S., & Clark, C. \(2020\). \*Cyber security system\*. Retrieved from https://searchsecurity.techtarget.com/definition/cybersecurity](https://searchsecurity.techtarget.com/definition/cybersecurity)
- [Simanjuntak, V. \(2020\). \*The mode of breaking into customer accounts through e-banking\*. Retrieved from https://money.kompas.com/read/2015/04/15/113500326/Ini.Modus.Pembobolan.Rekening.Nasabah.Melalui.e-Banking.?page=all](https://money.kompas.com/read/2015/04/15/113500326/Ini.Modus.Pembobolan.Rekening.Nasabah.Melalui.e-Banking.?page=all)
- [Sitanggang, & Winarto. \(2020\). \*Digital transaction increase, supervision is more important\*. Retrieved from https://keuangan.kontan.co.id/news/transaksi-digital-meningkat-peran-pengawasan-makin-penting](https://keuangan.kontan.co.id/news/transaksi-digital-meningkat-peran-pengawasan-makin-penting)
- Stevens, T. (2016). *Cyber security and the politics of time*. Cambridge University Press.
- [Suud, Y. A., & Sandy, O. P. \(2021\). \*Bank Indonesia says it already has a cyber security sharing platform\*. Retrieved from https://cyberthreat.id/read/11174/BI-Bilang-Sudah-Punya-Cyber-Security-Sharing-Platform](https://cyberthreat.id/read/11174/BI-Bilang-Sudah-Punya-Cyber-Security-Sharing-Platform)
- [Suwiknyo, E. \(2021\). \*Top! the perpetrators of economic and financial crimes will be impoverished\*. Retrieved from https://kabar24.bisnis.com/read/20210114/16/1342952/top-pelaku-kejahatan-ekonomi-dan-keuangan-bakal-dimiskinkan](https://kabar24.bisnis.com/read/20210114/16/1342952/top-pelaku-kejahatan-ekonomi-dan-keuangan-bakal-dimiskinkan)
- [Ulya, F. N., & Jatmiko, B.P. \(2021\). \*6 steps by BI to overcome fraud in the financial sector\*. Retrieved from https://money.kompas.com/read/2021/02/04/163000226/ini-6-langkah-bi-atasi-fraud-di-sektor-keuangan](https://money.kompas.com/read/2021/02/04/163000226/ini-6-langkah-bi-atasi-fraud-di-sektor-keuangan)
- [Vishnum. \(2020\). \*Cybersecurity threats cause US\\$34.2 Billion in economic losses to organizations in Indonesia\*. Retrieved from https://news.microsoft.com/id-id/2018/05/24/ancaman-keamanan-siber-menyebabkan-kerugian-ekonomi-bagi-organisasi-di-indonesia-sebesar-us34-2-miliar/](https://news.microsoft.com/id-id/2018/05/24/ancaman-keamanan-siber-menyebabkan-kerugian-ekonomi-bagi-organisasi-di-indonesia-sebesar-us34-2-miliar/)
- Von Solms, R., & Van Niekerk, J. (2013). From information security to cyber security. *Computers & Security*, 38(2), 97-102.
- [Yovita. \(2017\). \*It takes 1.5 million 'cyber soldiers' to secure Indonesia\*. Retrieved from https://kominfo.go.id/content/detail/9098/butuh-15-juta-tentara-siber-amankan-indonesia/0/sorotan\\_media](https://kominfo.go.id/content/detail/9098/butuh-15-juta-tentara-siber-amankan-indonesia/0/sorotan_media)
- Yunita, (2020). *Indonesia lacks cyber security talent*. Retrieved from https://kominfo.go.id/content/detail/8574/indonesia-kekurangan-bakat-cyber-security/0/sorotan\_media
- Ziccardi, G. (2020). Wearable technologies and smart clothes in the fashion business: Some issues concerning cybersecurity and data protection. *Laws*, 9(2), 12-26.