Journal of Election and Leadership (JOELS)
ISSN 2723-5149

Understanding Indonesia's Cyber Security Policies: Opportunities and Challenges In The Digitalization Transformation Era

Dimas Febriawan[1]*, Hizra Marisa[2]
[1] Universitas Muhammadiyah Prof DR Hamka, Indonesia
[2] Universitas Paramadina, Indonesia
*Correspondence Author: hizra.marisa@paramadina.ac.id

Abstract
This paper will discuss the understanding of Indonesia's policies in Cyber Security, in terms of technical aspects and social effects. Where the era of digital transformation raises new risks and threats, namely Cyber Security. It is important for the government, as executor and supervisor, to identify potential risks and threats to ensure cyber security and efforts to build community digital literacy during the digital transformation era. The efficiency of the measures developed and implemented to minimize risks and eliminate threats to national cybersecurity depend on the quality and appropriateness of the implemented policies. From the research results found that a comprehensive approach to analyzing the risks and threats posed by cyber threats in the era of digital transformation is needed and must cover all related processes, both technical and non-technical, in particular the relations between the actors involved. This creates significant opportunities and challenges for Indonesia's future, especially in matters of national defense security from hacking threats and other cyber problems.
Keywords: *Cyber Security; Digital Transformation Era; Opportunies and Challenges; Policy*

1. Introduction

Nowadays, there are so many activities that can be done online or in a network. Currently the internet is transformed into something that can provide benefits and convenience for everyone. However, it is also undeniable that on the internet there is still a crime. Behind the world that relies on communication and information, it can actually trigger cybercrime.

Cyber crime can threaten and even attack individuals or groups with digital attacks, such as accessing personal data information or destroying important data (Abidin, C. 2018). To undestand about Cyber Security, we need to elaborate it conceptually and terminology.

Cyber security includes security tools, policies and concepts that can be used to protect organizational and user assets. Cyber security can minimize the entry of threat risks into computer systems. These safeguards apply to computing devices, applications, services, and information that is transmitted and stored in cyber environments (Anderson, R., & Moore, 2019).

Cybersecurity refers to practices that ensure three important points called the CIA Triad.The three points are confidentiality, integrity, and availability.CIA Triad is a security mode developed to help people understand various information technology security and become the main concept of cyber security (Warkentin & Orgeron, 2020).

Cyber Security Type

Here some of the type of Ciber Security based on some literature from Sari, N. W. 2018:

1. Could Security

This type of cybersecurity refers to efforts to protect data stored in the cloud. Some of the things involved in this protection are technology, control policies, and services that support cloud security.Cloud security is an important aspect in ensuring data security. Some of the threats to cloud security include

Received (2023-08-09); Accepted (2023-11-28); Published (2024-01-24)

data theft, data abuse, and service traffic hijacking.

2. Network Security

Network security or network security is an effort to protect the internal network by increasing network security. Network security is very important for companies that use network systems for every activity. This protective measure can protect company assets from cybercrime threats and can also manage network traffic to make it more efficient.One example of network security is the use of antivirus and firewalls to detect threats originating from malware.

3. Application Security

Application security is a type of cyber security that is used to enhance application security from various threats. Applications can be accessed from various networks that allow cyber attacks. This makes the application vulnerable to cyberthreats, so it is necessary to implement application security. Several ways to ensure that the security process works properly are authentication, authorization, encryption, logging, and application security testing procedures.

Meanwhile, we need to understand the threats and problems that exist in cybers, it is necessary to understand the structure of that space. The structure of cyber is formed based on the interaction of stakeholders and the type of technology contained therein. There are 3 stakeholders who interact with each other in cyberspace where each stakeholder has their own goals in using cybers. The three stakeholders are the State, citizens on the internet or netizens, and the international community (Yeli, 2017).

The state uses cyberspace with the perspective that cyberis the 5th space besides land, sea, air and outer space. Thus, the use of cyber space uses the perspective of traditional sovereignty and security. Sovereignty applied in cyber space is exclusive. What is meant by exclusive is the desire to have full or independent authority over cyber space.

If the state wants full control, netizens expect the opposite, namely complete freedom. This makes the relationship between the state and netizens in cybers very close. A consensus is needed that can regulate cyber sovereignty for the state and freedom for netizens. This consensus is usually regulated in cyber law which regulates the extent to which freedom is given to netizens to access and publish information in cyber space (Yeli, 2017).

For this reason, the term “Data is the New Gold” is a popular metaphor used to highlight the increasing value and importance of data in the modern world. Information is meaningful output derived from data.

But how about data using in Indonesia and the awareness of its security or cyberspace rank? According to National Cyber Security Index (NCSI, 2022), Indonesia's cybersecurity ranks 6th in Southeast Asia. Meanwhile, globally,
Indonesia is ranked 83rd out of 160 countries.

The NCSI makes this assessment based on a number of indicators, such as state laws relating to cyber security, whether or not there is a government institution in the field of cyber security, government cooperation regarding cyber security, as well as public evidence such as official government websites or other related programs.

With these indicators, NCSI considers Indonesia to have a score of 38.96 out of 100 in terms of cybersecurity. This figure is far below the scores of neighboring countries.

Malaysia is recorded as having the best cyber security in Southeast Asia with a score of 79.22. The cyber security of this neighboring country is rated at 18th globally.

Then Singapore is in second place in Southeast Asia with a cybersecurity score of 71.43. Followed by Thailand, the Philippines and Brunei Darussalam with successive scores of 64.9, 42.86 and 41.56.

While a number of other Southeast Asian countries were below Indonesia's ranking,

such as Vietnam with a score of 36.36, Laos 18.18, Cambodia 15.58 and Myanmar 10.39(NCSI, 2022). This research will focus on looking at how Indonesia's cybersecurity is and its opportunities and challenges.

2. Theoritical Perspective

In the international aspect, cyber warfare is one of the factors for countries in making decisions or making policies to protect their country's sovereignty. Norms or rules are also prepared to improve cyber security, protect global community connectivity, reduce risk, encourage better predictions, and limit problematic potentials, including preparing for war (Hizra, 2023).

The theory called Information Operations or IO sees that information can be used as a weapon to threaten the enemy. Gathering information about enemies, as well as spreading propaganda to gain diplomatic, economic, and political superiority are things that are done in IO (Kuehl D., 2017).

IO can be applied in all spectrums, both military and non-military (Department of the Army, 2003). Network attacks or CNAs, deception or deception, destruction (physical cyberattacks) or cyber attacks using electronic warfare, security operations, and psychological operations (Kuehl D., 2017).

Another example of IO is Deception or Fraud. Deception is the activity of sending false information with the aim of deceiving opponents and influencing psychological aspects. Deception, which is also known as Disinformation, is a type of threat that is difficult to detect but has a huge impact in the real world. This is because Deception aims to influence the target's behavior according to the wishes of the actor who commits fraud. Deception is a type of threat that can damage political stability in a country.

Figure 1. Cyber Threats Sources

The Figure above shows us that cyber threats can originate from a variety of sources, from hostile nation states, and terrorist groups, to individual hackers, to trusted individuals like employees or contractors, who abuse their privileges to perform malicious acts.

Next theory is Psychological Operation PSYOP is an information dissemination operation with the aim of influencing society from the emotional and behavioral aspects. If Deception has false information in it, PSYOP may contain factual information. However, this information is packaged in such a way as to create the emotions and behaviors desired by PSYOP actors (Andress, 2011).

1. Referring to the explanation of the types of IO above, there are similarities in context that can be concluded. The concept of security in cyberspace can be divided into two parts. The first part is the security context by ensuring that there is no damage to the information management system. Information is a strategic asset, so it must be stored safely in cyberspace belonging to a particular entity. Security Information management in this case is a computer network that must be protected from CAN operations and data centers that are safe from Physical Cyber-Attack. Based on the Real Perspective theory of Cyber Security, the context of information

management security must be regulated at the infrastructure level (Yeli, 2017).

3. Method

The research method is a scientific method used to obtain data with the aim and use of something (Sugiyono, 2013). In this research, the research method used in this research isqualitative research approach with descriptive methods, analizing the secondary data that found on books, journals, news and many reference. The data collection technique used is secondary data such as the use of documents through literature reviews obtained from journal articles, books, and online information as well as government website sources.

4. Result and Discussion

The era of digitalization requires every human being to move forward, changing all lines of life towards the use of technology. Digitalization itself is interpreted as a transformation that is based on a concept of using information and communication technology to increase efficiency in all fields, especially in terms of management, documentation, dissemination of information and knowledge (Furauki & Sukmana Ena, 2018).

Digital Transformation Era

Defining Digital Transformation (DT), we can see from several aspects of understanding, the first according to KBBI, the meaning of "Transformation" is about a change of form (shape, nature, function, etc.), while the word "Digital" means more related to numbers-numbers for a particular counting system. While the term TD fromexperts can be interpreted as changes related to the application of digital technology in all aspects of life in society. Digital technology: digital competence, digital use, digitaltransformation (Collin, 2015).

The use of the internet which is a major part of TD has been discussed by Mansbachin his article entitled International Relations and Information Technology (2016), he said that the internet, together with other innovations in technology has reduced the position of sovereign territory. the state and by doing so, weakens the state and contributes to the emergence of new thoughts in defining 'politics', as well as in determining a new political strategy as well. Mansbach further said that information technology has changed the territory into a post-territory, a conception that currently state boundaries are no longer determined by physical boundaries.

The emergence of DT started from Digitation which then developed into Digitalization and then came the term Digital Transformation. So that a flow can be drawn from the development phase: Digitization → Digitalization → Digital transformation (Kahne, 2011).

Digitization is defined as the conversion of analog information into digital form. Digitization is a process made possible by IoT (Internet of Thing), Big Data, Blockchain, Cryptocurrencies, etc. Meanwhile, Digital Transformation is interpreted as the total effect of digitalization in society (Hadiono & Santi, 2020). Simply put, DT is an extraordinary process where the process involves the resources that are owned, including utilizing digital technology that existed at that time to produce outputs to provide new experiences. This new experience can be in the form of a new value that is obtained by the community, such as the ease of transactions, shopping, communication, and so on.

According to Osmundsen (2018) there are 4 factors driving TD, namely (a) regulatory changes; (b) changes in the competitive landscape; (c) shift/change to the digital form of the industry; (d) changes in

consumer behavior and expectations. Tracing the current world conditions which are still in the era of the COVID-19 pandemic, judging from the driving factors for the occurrence of DT, of course, it is mainly due to regulatory changes. Like it or not, this has caused the government to issue new regulations that during the pandemic, everything is done online and digitally (Hizra, 2023). Another important theme concerns digital growth strategies is discussed by another expertise, they found that gaining a deeper understanding of what makes different platform growth strategies successful involves answering several important questions are necessary to do, such as: What is the optimal growth path in a platform environment. Should platforms first expand horizontally and then vertically, vice versa, or simultaneously? And if the platform is a market leader, should it diversify to other markets in search of greater network (Peter C. Verhoefa, Thijs Broekhuizen, 2021).

Indonesia and Cyber Crime

Unfortunately, Digital Transformation in Indonesia has not been accompanied by strong cybersecurity.This is indicated by the losses experienced by Indonesia in terms of cyber crime (Hizra, 2023).

	Global	Indonesia
GDP:*	USD 71,620 bn	USD 895 bn
Percent of global GDP*:		1,20 %
Cost of:**		
Genuine cyber crime:	USD 3,457 m	USD 43 m
Transitional Cyber crime:	USD 46,600 m	USD 582 m
Cyber criminal infrastructure:	USD 24,840 m	USD 310 m
Traditional crimes becoming cyber	USD 150,200 m	USD 2,748 m

Figure 2. Cyber Threats Sources

It can be seen that the large number estimated by Indonesia is due to cyber crime. The Indonesian government must be able to elaborate on issues related to building strong cyber-security in order to reduce and minimize losses in the following ways:

1. Weak understanding of state administrators or security related to the cyber world which requires restrictions on the use of server services are abroad it is necessary to use a secured system.
2. The legality of handling attacks in the cyber world.
3. The pattern of cybercrime incidents is very fast so it is difficult to handle.
4. Governance of national cyber-security institutions.
5. Low awareness of the threat of international cyber attacks that can paralyze a country's vital infrastructure.
6. Our industry is still weak in producing and developing hardware or hardware related to information technology which is a gap that can strengthen or weaken defensein cyber (Hasyim Gautama, 2023).

Opportunities and Challenges

Indonesia is included in the five largest countries in the use of social media, which has positive potential (strengths) and negative potential (vulnerabilities/ weaknesses) related to cyber warfare. Public use of social media can be a threat to state sovereignty. However, social media can be a source of knowledge about information, communication and digital technology, which enables people to become skilled in the digital world. The activity of using digital technology in Indonesia is a potential in cyber warfare. The use of information technology can be easily infiltrated by hackers or crackers from various countries, which results in information vulnerability, especially in terms of transmitting intelligence information through cyberspace (Luiijf & Nieuwenhuis, 2019).

Indonesia has a significant position in the use of social media, which has positive

implications in increasing public understanding of the digital world. However, this also carries vulnerabilities to cyber attacks that can threaten state sovereignty and the security of information sent via digital platforms.

The potential threat of cybercrime can have an impact on cyber warfare. The following are some of the potential threats of cybercrime in Indonesia (Luiijf & Nieuwenhuis, 2019):

Hacking

One of the causes of cyber attacks, ranging from the whim to test security to the rejection of the government. An example of a case during the 2014 presidential election was the spread of news that the KPU (General Election Commission) website had been hacked by hackers. The indication is that the KPU website is experiencing access problems which causes it to be temporarily inaccessible.

Cracking

In Indonesia, there have been cases of hacking carried out by individuals known as "carders". They use this method to steal credit card information, namely peeking at customers' credit card data. After gaining access to this information, the hackers then try to access sensitive data and customer deposits at the bank for the perpetrator's benefit.

Cyber sabotage

Cyber sabotage is an intentional act to disrupt, damage, or destroy data or computer network systems that are connected to the internet. This action is the most feared method of many large companies around the world.

Spyware

The program refers to software that records secretly online use, namely recording cookies or registry data. The successfully recorded data can then be sent or sold to certain companies or individuals, who can then use the information to send unwanted advertisements or spread harmful viruses. Unfortunately, in Indonesia there have been 24 cases of malware infection related to the use of online banking by the public.

It is better to carry out cyber crime risk identification regularly to identify trigger factors for cyber crime. In the process various aspects that have the potential to trigger cyber crimes need to be evaluated. The rapid advancement of wiretapping technology in hacking social media has become a significant threat in the era of cyber war.

There are two main types of cyber crimes (Wahid and Labib, 2005), first, crimes that use information technology (IT) as a facility: This refers to crimes in which perpetrators use IT as a tool or means to carry out criminal acts. Examples include cyberattacks, online fraud, identity theft, distribution of malware, or other illegal activities that utilize information technology as an implementation tool.

The two crimes that target information technology (IT) systems and facilities: This refers to crimes that are aimed directly at the IT systems and facilities themselves. Examples include cyberattacks against IT infrastructure, data theft, sabotage of computer networks, or exploitation of weaknesses in IT security systems. With various cybercrime cases in Indonesia, national security and order stability is facing a significant threat.

Cybercrime escalation has reached quite a high level. Handling unlawful acts in cyberspace is not easy only with conventional positive law. This is due to the complex relationship between the five related factors, namely the perpetrators of crime, victims of crime, social reactions to crime, and law.

Although law has an important role for crime prevention and control, creating legal regulations that are responsive to various fields of law change with fast as information technology is not easy task. In facing the challenge of cybercrime, cooperation is

needed across sectors, including government, law enforcement adencies, the private secote, and society as a whole. In addition, the development of adaptive legal frameworks and the use of advanced cybersecurity technologies are essesntial in combating ever-evolving cybercrimes (Suhariyanto, 2023).

There are several stages of the risk management process in dealing with the threat of cybercrime that can be applied, which are explained as follows (Rahmawati, 2017):

Identification

Periodically identify the risks of cybercrime to identify the causes of cybercrime. In this process, all aspects that have the potential to cause harm must be identified carefully. After the identification is carried out, all identified risks are then measured. The measurement of risk in cybercrime threats refers to two main measures, namely probability and impact.

Assess

Risk assessment or Assess basically aims to evaluate the level of risk arising from cyber crime and its impact on various aspects of life, including national defense. Cybercrime risk assessment cannot be carried out directly, but can use matrix tables for risk measurement. In cybercrime risk assessment, matrix tables describe the level of probability and impact of identified cybercrime threats.

Treats

Deciding on actions and responses to cybercrime risks involves determining whether those risks will be accepted, transferred, minimized, or avoided. In cases where information and data theft occurs between individuals and institutions, efforts to minimize risk are important.

Controls

In order to evaluate the success of risk management, it is important to continuously monitor and adjust. In the monitoring process, it is suggested that an early warning mechanism be in place for those responsible for security, such as the Ministry of Defense of the Republic of Indonesia, so that they are able to take the necessary actions in anticipating cybercrime threats.

To anticipate cyber crime, it is important to involve technology experts who have the ability to support the development of a sophisticated and modern national defense system. The need for an Indonesian defense industry cooperation is needed to create an information and communication system program that is competitive with other countries. The development of a cyber defense system in Indonesia is influenced by two factors, namely regulation and the existence of a cyber command center. The government needs to make good and appropriate regulations to regulate the development of national cyber security (Schneier, 2015).

One of the other important things is to build a cyber defense security command center. The Indonesian government plans to carry out a cyber operation command which aims to become a cyber defense command center in Indonesia. With the operation of the command center, it is hoped that the Indonesian people will be better prepared in anticipating non-traditional threats, namely cybercrimes which are increasingly having an increasing impact on the sovereignty of the Republic of Indonesia. This is a big step that needs to be continuously strengthened in order to function optimally. Appropriate regulations and capabilities are needed in terms of national defense systems, networks, applications, and policies related to cyber security.

In a global persepctive, Indonesia already take part in global act due cyberspace things. Indonesia is part of the ASEAN Network Security Action Council, a member of the International Telecommunication Union (ITU), a steering committee for the Asia Pacific Computer Emergency Response Team (APCERT), a member of the Forum of

Incident Response and Security (FIRST), carries out bilateral cooperation in the cyber field- security with Japan, England, and several other countries.

Indonesian government can take advantage of this opportunity as a formof national defense against the dangersof cyber crime.

5. Conclusions

The Indonesian government is currently accelerating Digital Transformation nationally with the principle of inclusivity in it. There are five steps that are the President's direction for accelerating TD, including accelerating access expansion and improving digital infrastructure and providing internet services, in 12,500 villages or sub-districts, as well as at public service points; preparing a digital transformation roadmap in strategic sectors; accelerating the integration of the National Data Center; prepare regulations, funding schemes and digital transformation financing as soon as possible; preparing for digital talent HR needs (Permadi, 2021).

Of course infrastructure development must be balanced with the readiness of human resources. Indonesia, in this case the Ministry of Communication and Information has drawn up three steps to improve digital human resources in Indonesia, including Basic Digitak Skills-Digital Literacy targeting the general public; Intermediate Digital Skills targeting technician and professional level workers; Advanced Digital Skills with a target of leadership-level practitioners in the public and private sectors (Social Development Talk, 2021).

There are several steps that taken and still continuing actions by the government to overcome cybercrime: 1. Mapping threats, 2. Create strong policies, 3. Establish good collaboration between instituions, 4. Improve skills, 5. Establish a national data centre.

6. Daftar Pustaka

Anderson R&T Moore. (2019). *TWhy Crypto Tokens Matter: How to Ensure Security in the Internet of Things. Harvard Business Review.* Retrieved from https:// hbr.org/2019/01/why- crypto-tokens-matter

Abdul Wahid& Mohammad Labib.(2005) *Kejahatan mayantara (cyber crime). Retrieved at* https://lib.ui.ac.id/detail.jsp?id=20232423

Hasyim Gautama, (2023).*A Probabilistic Approach to the Analysis of Program Execution Time Hasyim Gautama. Retrieved at* https:// www.researchgate.net/publication /2900706_A_Probabilistic_Approach_to _the_Analysis_of_Program_Execution_ Ti me_Hasyim_Gautama

Kahne, Joseph (2021). *Participatory Politics: New Media and Youth Political Action.* Retrieved at https://www.Researchgate.net/publication/2557027744_Participatory_Politics_New_Media_and_Youth_Political_Action

Kuehl, D. (2017). *Information Operations.* Retrieved from www.rand.org:http:// www.rand.org

Kuehl, D. T. (2009). From Cyberspace to Cyberpower: De ning the Problem. In F. Kramer, S. Starr, & K. Wentz, *Cyberpower and National Security.* Washington DC: National Defense University Press.

Luiijf, E., & Nieuwenhuis, L. J. M. (2019). Cyber Security as Competitive Advantage. *Journal of Cyber Policy*, 4(2), 161-178.

Marisa, H. (2023). *Memahami Literasi Digital (Digital* Literacy) dan Keterampilan Digital (Digital Talent) Masyarakat Indonesia Dalam Era Transformasi Digital. Retrieved from https://penerbitlitnus.co.id/portfolio/refl

eksi- politik-internasional-kontemporer-gatot- subroto-kav-97/

Verhoefa, Peter C, Broekhuizena, Thijs and Bartb, Yakov (2021) , Digital transformation: A multidisciplinary reflection and research agenda, Journal of Business Research Volume 122, January,, 889-901

Rahmawati, Ineu. (2017). Analisis Manajemen Risiko Ancaman Kejahatan Siber (Cyber Crime) dalam Peningkatan Cyber Defense. *Jurnal Pertahanan dan Bela Negara,* vol. 7, no. 2, 2017, pp. 35-50.

Sari, N. W. (2018). Kejahatan cyber dalam perkembangan teknologi informasi berbasis komputer. *Jurnal Surya Kencana Data Dinamika Masalah Hukum dan Keadilan*. 5(2): 577-592

Schneier, B. (2015). Data and Goliath: The Hidden Battles to Collect Your Data and Control Your World. W. W. Norton & Company.

Suhariyanto, B. (2023), Tindak Pidana Teknologi Informasi (Cybercrime): Urgensi Pengaturan dan Celah Hukumnya, Rajawalu Pers, Jakarta.

Warkentin & Orgeron. (2020). *Digital Technology-Based Teav¥ching 2020.* Retrieved from https://www.sciencedirect.com/science/article/abs/pii/S026840121930060X

Yeli, H. (2017). A ree-Prespective Teory. *PRISM,* 109-115.