Cyber Diplomacy And Protection Measures Against Threats Of Information Communication Technology In Indonesia

Muhammad Ridha Iswardhana

International Relations Department Universitas Teknologi Yogyakarta
Email: muhammad.ridha@staff.uty.ac.id

Abstract

This article attempts to explain the forms of Indonesian cyber diplomacy related to the protection of the use of information technology. In this case, Indonesia as the fourth largest country in the world often gets cyber threats and attacks. This was then followed up with efforts to protect it domestically, but was constrained by threats from abroad. The research method used in this study uses a qualitative descriptive analytical approach using the theoretical framework of cyber diplomacy and the concept of information and communication technology. The case analysis will explain the causes and effects of holding Indonesian cyber diplomacy based on secondary data. The author finds that the Indonesian government does not only use a legal approach through the ITE Law, but also culture, technological renewal, and diplomacy towards various countries. The Indonesian government has enacted the 2008 ITE Law and has encouraged the wise and positive use of the internet through various approaches. Furthermore, the Government of Indonesia also carries out cyber diplomacy efforts through several relevant ministries towards other countries, both bilaterally, regionally, multilaterally, and internationally. For example, Indonesia actively participates in cyber diplomacy at the TELMIN, ADMIN, PCC, OEWG forums and BSSN collaborating with various countries to overcome cyber threats. However, it all depends on every internet user to always be vigilant and careful in using cyberspace to avoid the threat of cybercrime.

Keywords: *Cyber Diplomacy, Indonesia, Information Communication Technology, Protection, Threats.*

Abstrak

Artikel ini berusaha menjelaskan bentuk diplomasi siber Indonesia terkait perlindungan penggunaan teknologi informasi. Dalam hal ini Indonesia sebagai negara terbesar keempat di dunia sering mendapatkan ancaman dan serangan siber. Hal ini kemudian ditindaklanjuti dengan upaya perlindungan secara domestik, namun terkendala terhadap ancaman dari luar negeri. Metode penelitian yang digunakan dalam penelitian ini menggunakan pendekatan kualitatif secara dekriptif analitis dengan menggunakan kerangka teori diplomasi siber dan konsep teknologi informasi komunikasi. Dalam analisa kasus akan menjelaskan sebab akibat diadakannya diplomasi siber Indonesia berdasarkan data sekunder. Penulis menemukan bahwa Pemerintah Indonesia tidak hanya menggunakan pendekatan hukum melalui UU ITE, melainkan juga budaya, pembaharuan teknologi, dan diplomasi terhadap berbagai negara. Pemerintah Indonesia telah memberlakukan UU ITE 2008 dan mendorong penggunaan internet secara bijak dan positif melalui berbagai pendekatan. Selain itu, Pemerintah Indonesia juga melakukan upaya cyber diplomacy melalui beberapa kementerian terkait terhadap negara lain, baik secara bilateral, regional, multilateral, maupun internasional. Misalnya, Indonesia berpartisipasi aktif dalam diplomasi siber di forum TELMIN, ADMIN, PCC, OEWG dan BSSN yang bekerjasama dengan berbagai negara untuk mengatasi ancaman siber. Namun, itu semua tergantung pada setiap pengguna internet untuk selalu waspada dan berhati-hati dalam menggunakan dunia maya agar terhindar dari ancaman kejahatan dunia maya.

Kata Kunci: *Diplomasi Siber, Indonesia, Teknologi Informasi Komunikasi, Perlindungan, Ancaman.*

INTRODUCTION

The development of information and communication technology (ICT) has become an inseparable part of Indonesian society. The Corona Virus Disease (COVID-19) pandemic has also increased the use of ICT, represented by the use of the internet by almost everyone. A total of 202 million of the 274 million population in Indonesia have been connected to the internet through various means (Republika, 2021). The development of smartphones, laptops, tablets, smart TVs, to smartwatches has made people more aware of information technology. Payment transactions, marketplaces, and various online services also encourage information technology to be widely used.

The internet has become one of the most important needs, but it was different in the late 2010s when the internet was only for entertainment and additional needs. Ease of access, speed of service, and a more affordable cost are considerations in using the internet. Especially when the world is faced with the phenomenon of the COVID-19 pandemic, which causes people to be advised to stay at home more, this is a factor that drives the internet to become more familiar in Indonesia (Kompas.com, 2020). There are some new habits after the COVID-19 pandemic, especially in terms of Work From Home (WFH), School From Home (SFH), and Virtual Meetings, have caused information technology to have shifted to become a significant need, these three things cause people to become addicted to the internet.

Then, almost all levels of society have become internet users, ranging from small children, teenagers to the elderly. In terms of facilities, as many as 195.3 million people, or the equivalent of 94.6% of the internet, are accessed via smartphones with average access of 8 hours 52 minutes every day. Meanwhile, the average internet speed in Indonesia reaches 23.32 Mbps for fiber optic network users and 17.2 Mbps for cellular networks (Kompas, 2021).

In Indonesia, internet users consist of various groups, ranging from business circles, students, students, employees to housewives. Meanwhile, the number of internet users is concentrated on the island of Java, followed by people on the islands of Sumatra, Sulawesi, Kalimantan, and other islands, as is the reality of the Indonesian population. These various realities can be seen as "two sides of a coin," namely opportunities and challenges. The efficiency and effectiveness in various ways are also followed by the threat of cybercrime (Danuri and Suharwi, 2017). Based on the various things above, this article seeks to dissect in-depth in the form of how is Indonesia's diplomacy to overcome various existing cyber problems and what are the Indonesian Government's domestic protection policies to overcome cyber threats from the perspective of Cyber Diplomacy Theory and The Information Communication Technology

Concept. Moreover, this topic tends to have not been studied in-depth, especially from the point of view of Indonesian researchers.

THEORETICAL FRAMEWORK

Cyber Diplomacy Theory

According to Hodzic, cyber diplomacy is increasingly used by major global political actors to describe transformations in diplomacy in the digital era. The evolution of diplomacy in cyberspace revolves around new social media, orientation to public actors, and cyber threats and cyber behaviour as new areas in international politics. In addition, cyber diplomacy can also be an evolution of public diplomacy and referred to as public diplomacy 2.0. The development of cyber diplomacy is a response to shifts in international relations (Hodzic, 2017).

In general, cyber diplomacy adopts a foreign agenda, including cybersecurity, cybercrime management, trust-building, international freedom, and internet governance. Cyber diplomacy is a form of diplomacy in the cyber area through the performance of diplomatic functions to secure the state's interests. This kind of diplomacy can be understood as an effort by referring to the foreign policy agenda to facilitate communication, negotiate agreements, gather information and intelligence from other countries to avoid friction in cyberspace. Cyber diplomacy in its implementation involves diplomacy, conflict resolution, agreements and policies related to the cyber world. This cyber diplomacy is a means of using diplomatic resources and functions to secure national interests related to cyberspace.

The Information Communication Technology Concept

The word technology comes from the Greek, 'techne', which means expertise and 'logia' which means knowledge. In a narrow sense, technology refers to objects used to facilitate human activities, such as machines, tools, or hardware (Rusman et al., 2013). Meanwhile, Rogers explained that technology is an instrumental step design to explain the causal relationship in achieving the expected results deeply. This technology generally has two components: hardware aspects in the form of equipment and software aspects in the form of information (Ishak and Dermawan, 2019).

Information and communication technology is a means and infrastructure (hardware, software, useware) systems and methods for obtaining, transmitting, processing, interpreting, storing, organizing and using data meaningfully. Information technology provides many conveniences in managing information in terms of storing, retrieving and updating information. Information technology is also a technology used to process, process, obtain, compile, store, manipulate data in various ways to produce quality information (Wardiana, 2002).

The development of global information and communication technology has succeeded in bringing together computing, television, radio and telephone capabilities in an integrated manner through the internet. This result is a combination of revolutions in personal computers, data transmission and compression, bandwidth, data storage technology and multimedia integration access, and computer networks. This development in internet has brought together various media, namely sound (voice and audio), video, graphic images, and text.

RESEARCH METHOD

This study uses a qualitative approach, an approach that places the researcher's view on something studied subjectively. Researchers appreciate and pay attention to the subjective views of each subject under study. The type of research used in this research is descriptive analysis. In this case, the researcher tries to provide a systematic and comprehensive picture of the problems faced regarding cyber attacks, types and actors, actions taken, and forms of cyber diplomacy cooperation.

Referring to the data in the form of qualitative data, analysing it used an interpretive approach (interpretive approach). The qualitative data process refers to the standards owned by Babbie (2008), namely: Coding, Memoing, and Concept mapping. The coding process is the process of classifying and categorising data. Memoing process is the process of writing memos or notes for researchers in research activities. Finally, Concept Mapping is the process of mapping relationships between various concepts.

RESULT AND DISCUSSION

Data Leaks in Indonesia

During the last three years, there have been several incidents of personal data leaks in Indonesia. The leak of private company data began in March 2019 when 13 million Bukalapak customers were sold illegally (Okezone, 2021); one year later, 91 million Tokopedia users were sold on dark sites in May 2020; 1.2 Bhinneka users' data continued in the last month. Similarly, as many as 890,000 Creditplus online loan customers were also suspected of leaking in August 2020; then the leak also happened to Shopback users in September 2020; then there were recorded leaks of 2.9 million Cermati users and 5.8 million RedDoorz users in November 2020. Meanwhile, government agencies also The 2014 General Election Permanent Voters List (DPT Election) leaked 2.3 million population data (Kompas.com, 2021), 279 million population data at BPJS Health leaked on May 21, 2020, and 230 thousand data on COVID-19 patients were also suspected experienced a leak (CNN Indonesia, 2021).

The data is intentionally sold on illegal forums for improper purposes. These various personal data are horrendous because they are large amounts and contain essential information, such as name, bank account, credit card, telephone number, email address, date of birth, income, and other information. The data leak does not only occur in government institutions but also in private companies. Most hackers try to steal user data which mostly happens on e-commerce and online lending.

Various data leaks in Indonesia can show the magnitude of the risks and dangers of irresponsible parties' misuse of technological advances. Service providers who receive and store data should have security and confidentiality that can be hacked, which leads to personal data being sold freely. This reality is one of the fundamental challenges to the development of information technology. Moreover, Indonesia, as a country with the fourth-largest internet user background in the world, Indonesia still faces many challenges that need to be resolved together. If we look at the geographical conditions and demographics of the population, then Indonesia tends to be very vulnerable to the threat of information technology.

Cyber Crime Threats in Indonesia

In addition, there are also the phenomena of hoaxes, hate speech, terrorism, online fraud, and cybercrime, which are the five most significant threats to the use of information technology (Infokomputer, 2021). The five threats are happened due to the people who have not been fully careful in using technology, causing the internet to become a means for criminal acts. The author attempts to explain these five phenomena as follows:

1. **Hoaxes** are the first harmful impact of the ease of information dissemination along with advances in information technology. The public misuses the existence of news disseminated using online means on the internet platform to spread false news. A hoax can be understood as a product of fake news and attempts to deceive readers into believing something to create public opinion in a particular community. The spread of fake news mainly occurs on social media, reaching 92.40%, which shows how communication interactions become vulnerable to be used as an effort to divide society. The low literacy and habit of people believing in myths is the leading cause of many hoaxes in Indonesia. Moreover, the 2014 and 2019 General Elections made social media considered a source of information for some people. When reading habits are still low while dealing with the development of news through online media, many residents quickly conclude without trying to find out further (Juditha, 2018).

   Moreover, hoaxes are used as economic income for certain groups to vilify certain groups or groups, making hoaxes widespread. However, many parties only use hoaxes for political gain and economic gain without considering the impact. As a result, riots occurred in Wamena, Papua, in 2019 caused by racism, which was responded to by demonstrations by students, which ended in chaos and caused 16 residents to die as victims (Jawa Pos, 2019). In general, society is now divided into two groups: groups that are considered to believe hoaxes as truth and communities that have studied whether it is merely fake news.

2. **Hate speech** followed as the second threat to the existence of internet technology in Indonesia. This hate speech occurs because they are not aware of the limitations in the use of social media and ignorant of the rules in social media (Febriansyah & Purwinatro,

2020). Although it is often considered a hoax because it is widely disseminated on social media and online news, hate speech has a fundamental difference. Hate speech can be understood as an attempt to intentionally abuse the freedom of the public sphere to attack and damage a particular person, group, institution, or institution because of specific differences. This hate speech is very contrary to the polite eastern culture and the Pancasila ideology adopted by the Indonesian people. Efforts to insult, defamation, and provoke the public have wrong meanings, and hate tendencies are some of the characteristics of hate speech (Ningrum et al., 2018).

The right to freedom of expression and the existence of public spaces is 'ridden' by certain groups who have the economic capital and the ability to spread wrong information. Sentiments of thought, political views, political interests, economic inequality, prejudice, hatred, resentment, and polarization in society cause hate speech to spread widely. Differences in backgrounds and groups with different interests cause efforts to shape people's way of thinking to hate groups that are considered opponents by using hate speech. These conditions not only threatens democracy in Indonesia but also harm the unity and integrity of society. As a result, riots occurred in Tolikara, Papua, due to the spread of hate speech on social media in 2017 (Kusumasari & Arfianto, 2020).

3. **Terrorism and radicalism** are the next dark side to the ease of information technology globally, especially in Indonesia. The existence of these two things has succeeded in threatening people's lives in the real world and has an impact on the virtual world. If initially, the terrorists succeeded in creating fear and fear through bombs, attacks, and various other violent attempts. Furthermore, social media is a new struggle that is being used to spread radicalism in line with the significance of the use of information technology. When mass media and social media use the internet, these terrorist groups try to "set the stage" for themselves. By creating

one-sided reporting that uses the emotional side and the similarity of specific religious backgrounds, the pro-violence groups make publicity efforts. This misleading propaganda targets teenagers and unstable young people, tend to be less knowledgeable about Islam, and is easily instigated with specific religious labels (Fahmi, 2018).

Terrorist groups seek to gain the trust and support of online readers to fight conventional news and ideologies that are perceived to be against them. The use of websites, showing videos, uploading photos, and short message facilities containing violence and radicalism is an attempt by terrorist groups to show their existence and spread their ideology (Junaedi, 2010). The most dangerous influence of the existence of terrorism in the use of the internet and social media is as an effort to recruit new members in order to carry out the next terror attack. The development of the Islamic State of Iraq and Syria (ISIS) in 2014, which later grew into a sizeable terrorist organization, can occur due to the use of Twitter media in their militia recruitment. Posting an invitation to join that is 'labeled' in the name of Jihad using various social media attracts thousands of members every year from all over the world. The existence of the internet allows ISIS to control the propaganda and recruitment of prospective members without having to meet in person. The Thamrin Bombings in Jakarta in 2016 and the Surabaya Police Attack in 2018 can show how dangerous the misuse of information technology by terrorism and radicalism groups is, that bomb attacks occurred in Indonesia while the leaders of the ISIS group were in Syria and Iraq (Nuruzzaman, 2018).

4. **Online fraud** is then a threat of misuse of information technology in terms of economic activities and transactions. Along with the convenience and efficiency of information technology, it encourages an increase in digital economic activities. Needs and markets that are no longer in physical form create a new lifestyle in electronic transactions. The goods to services trade can all

be made online just by using a finger on a smartphone. These developments are then also directly proportional to the increase in online fraud crimes. Data shows that 48% of consumers are victims of cyber fraud, with 6% of them have become victims and losing money. Meanwhile, the average loss is estimated at IDR 3.6 million, with 54% of them successfully getting their money back in full.

In committing the crime, online fraud can take several forms, including fraud with fake websites, fake emails, use of telephones, sending SMS, and credit card media. Some examples of forms of cyber fraud, including sending messages when winning a prize, asking for important information such as a secret password, and contacting to tell them if a relative has been robbed, all of which will lead to an attempt to trick potential victims into sending some money for various reasons (Samudra, 2019). Another form of fraud is to sell products at prices below the average price on the internet. Not infrequently, many victims of fraud are easily tempted by the low price but instead get goods that do not match or even do not get the product ordered at all. Many causes of online fraud are still often found in internet media, for example, economic factors, lack of experience, ignorance of the threat of fraud, low awareness of legal compliance, and digital transactions without protection (Sumenge, 2013). The public needs to access education before making digital transactions to avoid the threat of cyber fraud.

5. **Cybercrime** has multiple means. The threat of this crime can take the form of virus attacks, malware, cracking, hacking, and other efforts. For example, Indonesia was the second most frequent destination after China in Ransomware and Wannacry malware attacks in 2018. Indonesia was ahead of Australia, Hong Kong, and Singapore, which experienced these cybercrime attacks (Bisnis.com, 2019). Most of these attacks occur when people access websites and emails that intentionally contain viruses and malware, which increased 4 times bigger compared to the previous year (Liputan6,

2019). The various threats of cybercrime aim to be able to intercept financial transactions and obtain personal data. If a device has been infected with these viruses and malware, the perpetrators can quickly get private, confidential data that can be misused or become a victim of extortion. Not infrequently, it then leads to mastery of emails, social media, and even credit cards of victims, which leads to fraud and extortion.

The greatest threat from cybercrime is if it is aimed at public officials, military officials, or leaders of state institutions who can obtain vital data and state secrets. Another example is when South Korea experienced an attack allegedly carried out by North Korea, which succeeded in crippling some of the banking sectors in 2014 (Suara.com, 2014). Cybercrime can be dangerous for every country that can disrupt various vital objects such as the financial sector, electricity, navigation, transportation, and even the military.

Types of Cybercriminals

Based on the explanation above, it can be understood that information technology has made changes to human life. If previously everyone interacted more and did many activities in the real world, on the contrary now each individual is familiar with using the virtual world to fulfill many needs. Advances in technology encourage people to be able to access and disseminate various information freely through the internet. The internet has become a new space for communities to share data, express opinions, and follow a developing lifestyle. However, many conveniences will certainly pose various threats, considering that currently, the existence of the internet has blurred the boundaries and clarity of internet use (Chotimah; Iswardhana; Pratiwi, 2019).

Life in the era of globalization on the internet is different from activities in the real world because it can be accessed by anyone, anytime, and anywhere. There are potentials and risks of contact between one individual and another, both in terms of cooperation or conflict. Differences background of internet users can also increase the potential profit and risk of loss. An anonymity element in cyberspace makes a fundamental difference to the real world, which encourages many parties to carry out behaviors that harm others, either unknowingly or intentionally (Makarim, 2005). It can be understood how significant the potential cyber threat is in various crimes in cyberspace. Moreover, the risk of this threat can befall anyone, either when we are fully aware or careless. Some of the objectives of cyber threats that often occur, including (Magdalena, 2007):

1) Social media,
2) e-commerce,
3) e-learning,
4) Credit card,
5) Copyright, and
6) Trade secrets.

Based on various sources, the author summarizes several types of crimes in cyberspace, including (Iswardhana, 2021):

1) Fraud,
2) Data tampering,
3) Information breach,
4) Unauthorized access,
5) Piracy,
6) Wiretapping,
7) Theft of personal data,
8) Spreading fake news,
9) Broadcasting of hate speech,
10) Pornography,
11) Blackmail,
12) Banking and credit card crimes,
13) Hijacking of economic transactions, and
14) Cyber terrorism.

If we viewed from the side of cybercriminals, it could be divided into two actors (Sulaiman, 2002):

1) Internal actors, meaning that the perpetrator has direct access to the victim. This is indicated by manipulating, changing, and modifying software and hardware that connects the perpetrator and the victim. The forms of crimes committed are often related to online fraud and terrorism, radicalism. Usually, this is closely related to internet crimes with the same network by perpetrators who have knowledge and experience in specific fields.
2) External actors, meaning that the perpetrators can interfere and damage various activities on the internet even though they do not have the same network as the victim. Perpetrators tend to use the means of writing, sound, video, viruses, and malware. Most of the crimes committed are in the form of hoaxes, hate speech, and cybercrimes. Even though they do not have direct access,

perpetrators can take actions that are considered detrimental to their good name, from infiltration to burglary.

Cyber Law Approach and Rules

Responding to the various threats above, the Government of Indonesia cooperates with private service providers called the Indonesia Information Sharing and Analysis Center. The cooperation forum is a means of sharing information related to threats, vulnerabilities, risks, issues, assessments, and handling cyberattacks in information technology. Although it tends to be voluntary, this collaboration has many members from private and public companies. Based on Kominfo data (2019), several members of this forum, including:

1) Telekomunikasi Selular (Telkomsel),
2) Xynexis International,
3) Smart Telecom,
4) Telkom,
5) PANDI,
6) XL Axiata,
7) Indosat,
8) Aplikanusa Lintasarta,
9) Data Sinergitama Jaya (Elitery),
10) APJII,
11) PwC,
12) KPMG, and
13) PT Sampoerna Telematics.

Then, there are several ways to overcome various threats in information technology, namely: a cultural approach, technology renewal, and law enforcement.

First, the cultural approach can form healthy habits in internet use (Siagian et al., 2018). The public can use the virtual world for various positive benefits, for example, selling, promotion, service transactions, seeking journal literacy, and others. In addition, it is crucial to counteract harmful content in cyberspace by strengthening literacy for the community. Netizens are encouraged to read more and find out the truth of the information before trusting and spreading it. The public can also check websites owned by the government through the Ministry of Communication and Information to check the authenticity of the information. If the cyber community has been reduced and can distinguish between true and false information, it can slowly encourage internet users to fight harmful content. In the end, good habits in using the internet will make good use of the virtual world ecosystem to provide benefits for all parties.

Second, technology updates can be carried out by requiring every service provider on the internet to improve security regularly. It is important to protect networks, software, and hardware from being compromised, eavesdropped on, and accessed illegally. Service providers must periodically update and protect their information and communication technology infrastructure. The broader the scope of services, the greater the number of users, which leads to a higher risk of cyber threats to the providers of these products and services. If the system has strong defense and security capabilities, it can ward off various threats of sabotage, piracy, theft, and data destruction.

Third, it is necessary to have rules that provide certainty and explanations for various activities in cyberspace related to law enforcement. Referring to this urge, the term cyberlaw or cyberlaw has emerged in the context of efforts to protect, supervise, and enforce the law in cyberspace. This cyber law is needed to provide legal certainty, protection, and sanctions for allowed and prohibited things in using the internet. There is a tendency for internet users who feel they have the right to violate and harm the rights of others, both in ideas, words, actions, and other actions while using information technology. On the other hand, some specific individuals and parties deliberately create bad things to fulfill particular economic and political interests.

Cyber Protection by the Government of Indonesia

Following up on the many threats that occur on the internet, the Government of Indonesia has made efforts to recognize and protect cyber against the public by showing the existence of Law Number 11 of 2008 concerning Information and Economic Transactions (UU ITE). The ITE Law contains stipulations, mandates, limitations, protections, prohibitions, and sanctions for various activities related to the use of information and communication technology. The ITE Law also regulates electronic transactions, online commerce, and the recognition of digital content as legal evidence.

In the cyber law aspect, as stated in the ITE Law, it has protected and enforced the law for anyone who owns, stores, disseminates, and takes any action that harms other parties and violates the law. Suppose we look at the reality of Indonesia, which has the most significant number of internet users, which reaches 202 million people, the risk of cyberattacks increases. Reflecting on this in Article 27-34 of the ITE Law, Articles 36-40 have explained the forms of legal violations that are accompanied by criminal sanctions, including data confidentiality, cyber attacks, and access breaches.

The existence of the ITE Law is one of the legal bases for the protection and enforcement of the law for the Indonesian people who use the internet or commonly called Warganet (Economic Balance Daily, 2019). Moreover, if the netizen suffers losses due to the actions of others in cyberspace, then this law can be used as a means of defending rights. All activities carried out using the internet that causes loss, damage, and harm to citizens in Indonesia can use the ITE Law as a legal tool. Some parties consider the ITE Law to be a 'rubber article' misused based on defamation of anything on the internet.

Based on the release of the Directorate General of Legislation of the Ministry of Law and Human Rights (2019), the authors collect at least twenty things guaranteed in the ITE Law, such as:

1) Confidentiality
2) Data protection
3) Securing economic transactions
4) Electronic signature
5) Trade secret
6) Intellectual Property Rights
7) Online promotion
8) Electronic evidence
9) Legality of online services
10) Responsibilities of online services
11) Protection of financial transactions and investments
12) Protection against loss of information
13) Dispute resolution
14) Prohibition of spreading fake news
15) Prohibition of insults
16) Gambling ban
17) Prohibition of prostitution and immoral activities
18) Ban on blackmail
19) Prohibition of threats by force
20) Prohibition of online fraud

There is also a Criminal Code (Kitab Undang-Undang Hukum Pidana/KUHP) and a Civil Code (Kitab Undang-Undang Hukum Perdata/KUHPer). The two laws have explained orders, prohibitions, and punishments to every party and institution that harms other parties, primarily when it occurs in cyberspace. All actions that are considered disturbing, damaging, and harming others in any form can be imposed in the legal rules of the Criminal Code and the Criminal Code. Cyber law protection and enforcement are focused not only on the ITE Law but also on other legal rules, taking into account technological advances (Ersya, 2017).

Regarding cybercrime, Indonesia has an organisation that handles all complaints against cybercrime, namely ID-CERT (Computer Emergency Response Team) and ID-SIRTII (Indonesian Security Incident Response Team on Internet Infrastructure). ID-CERT and ID-SIRTII have the same duties and functions to record and respond to all public complaints regarding security disturbances on the internet (Setiadi et al., 2012). Meanwhile, the police established a Cyber Crime Investigation Center at the Criminal Investigation Unit at the National Police Headquarters and a Cyber Crime Investigation Satellite Office (CCISO) at several Provincial Police Headquarters (Polda) with the assistance of the Australian Federal Police (AFP) (Tekno.kompas.com, 2013).

However, there are obstacles when actors from abroad carry out cyberattacks because the perpetrators are outside the jurisdiction of Indonesia. It tends to be difficult to enforce the law while the perpetrator is not a citizen and is not domiciled in Indonesia. The rules of the ITE Law, the Criminal Code, and the Criminal Code require a long process and time to carry out the judicial process. Cooperation and standard rules are needed regarding the protection, supervision, and law enforcement across countries against actors who cause harm to Indonesian citizens. The Indonesian government can use diplomacy and law enforcement by collaborating with friendly countries or reporting to Interpol.

However, researchers have difficulty finding data on the number of foreign actors arrested for attacking Indonesian cyber-attacks from other countries. This is because apart from Interpol, Indonesia and the country of origin of the perpetrator must have an extradition treaty.

Indonesia's Cyber Diplomacy Towards Global

Regarding protection against cyber attacks, the international community has a global cooperation related to cybersecurity called the International Telecommunication Union (ITU). ITU was established in 2003 as a follow-up to the 2001 United Nations General Assembly to tackle cyber attacks together. ITU is at the forefront of promoting shared values and standards in cyberspace to be put to positive use. Despite being the world's highest cyber institution, ITU has drawbacks related to not having the authority to provide legal action for each country. As a result, each country tends to carry out more protection against cyber attacks and wars in accordance with their respective interests. In addition, each country then makes policies according to its national initiatives and needs. Regarding law enforcement, most countries prefer to cooperate with Interpol to catch the perpetrators of cyber-attacks in other countries. (Parestri, 2016). Indonesia has served as a member of the board and executive board at ITU in the period 2008-2013 (Kemenlu, 2013) Apart from ITU, there is international cooperation that is related to cyber threats, namely: International Multilateral Partnership Against Cyber Threats (IMPACT). IMPACT was established in 2011 in collaboration with ITU (Kittichaisaree, 2017). In relation to IMPACT as a United Nations (UN)-backed cyber security alliance, Indonesia as a member country of the UN also actively involved in diplomacy by encouraging cyber security.

Furthermore, there is standard rule called the Paris Call for Trust and Security in Cyberspace. This rule has been signed by 51 world countries, including developed countries in Europe. The international agreement aims to ward off attacks and cyber warfare. Through the agreement, it has been regulated that all internet infrastructure and facilities are not misused as a means of cyber attacks (CNN, 2019). In addition, this convention can prevent cyber wars from happening that lead to conflicts and wars in the real world. However, cyber issues do not yet fully have the same understanding because it tends to be controlled by the military for self-defense and retaliation for attacks (CNN Indonesia, 2019). Indonesia supports this agreement as demonstrated by the membership of the Indonesian Corporate Counsel Association (ICAA), Indonesia Cyber Security Forum (ICSF), and Special Olympics Indonesia (Paris Call, 2021).

Indonesia also succeeded in becoming one of the initiators in a joint declaration called the ASEAN Declaration to Prevent and Combat Cybercrime in 2017. This agreement can serve as a basis for reference and a form of shared understanding of cybersecurity threats. The Indonesian government is also actively promoting cross-border cooperation at the bilateral, multilateral, and international levels that support the wise use of the internet (Media Indonesia, 2019).

Following up on the declaration of cyber protection in the Southeast Asia region, there are Computer Emergency Response Teams (CERTs), Telecommunication Ministerial Meeting (TELMIN), and ASEAN Digital Ministerial Meeting (ADMIN). CERTSs are forums that discuss cyber issues and efforts to deal with the threat of cyber attacks (Kittichaisaree, 2017). Meanwhile, TELMIN is a negotiation forum in the region that later developed into ADMIN at the input of Indonesia to discuss cyber and digital issues since 2019. Through TELMIN and ADMIN, Indonesia has contributed to various meetings to further discuss digital protection into broader cyber. Meanwhile, several Indonesian government institutions that carry out cyber diplomacy include the Coordinating Ministry for Political, Legal and Security Affairs (Kemenko Polhukam), Ministry of Foreign Affairs (Kemlu), National Cyber and Crypto Agency (BSSN), Ministry of Communication and Information (Kemenkominfo), Ministry of Defense (Kemhan), and the Indonesian National Army (TNI) (Chotimah et al., 2019).

One form of diplomacy that BSSN has done is by partnering with various world countries, such as the United States, China, Russia, Britain, the Netherlands, and Australia (BSSN, 2019). The collaboration carried out by BSSN is related to cyber protection and terrorism. Diplomacy between BSSN and partners in the United States, China, and Russia can be a mapping effort and a means of mitigation considering that these three countries are the most prominent cyber attack destinations globally. Through these various collaborations and diplomacy, Indonesia can bridge the interests of Indonesia to protect and enforce cyber law in cyberspace.

Indonesia also actively holds and participates in various international meetings in global public discussions, such as: establishing a Policy Planning Consultation (PCC) in Geneva in 2017, participating in the 5th Annual Cyber Intelligence Asia in Malaysia in 2017, and being involved in the Open-Ended Working Group on International Information Security (OEWG on IIS) in 2019 (Kemlu, 2018).

It is understood that the development and utilization of information technology and cyberspace, including digital media and social media, also brings consequences of increasing threats to the security of the information exchanged. Real-world crime is now also shifting to cyberspace. It is undeniable that cybersecurity has embraced almost all aspects of public services, from infrastructure, aviation, finance, trade, to national security, due to the increasing dependence on digital technology. Reflecting on this issue, how important is the role of cyber diplomacy in guarding national policies, especially in the digital sector.

Moreover, there is also a difference in understanding of cybersecurity in each country in the international world due to global political developments and differences in national interests. Several factors cause these obstacles, including (Cahyadi, 2017):

a) Differences in norms and values that are understood by each country
b) Differences in interests between developed and developing countries
c) Different perspectives on cyber defense
d) There is no agreement that is fully binding on each country
e) Every country is trying to dominate the cyber world.

Various conditions above are the obstacle to creating a cybersecurity protection and governance regime. It is necessary to have a policy that can protect the interests of national cyber security and contribute to making a collective agreement in understanding how to deal with cyber threats. This can be resolved peacefully between countries through cyber diplomacy, which provides understanding for each country regarding cyber protection and cooperation. Cyber diplomacy is distinguished from digital diplomacy, which emphasizes using digital tools and techniques to conduct diplomacy. The similarity is that diplomats and non-state actors can carry out cyber diplomacy and digital diplomacy.

There are two things we can do to maintain security to maintain international cybersecurity, through cyber diplomacy:

The first is to build trust between countries through cybersecurity diplomacy and minimize conflict and an emergency response team from IT to avoid escalation of conflict from cyber to physical conflict.

The second is capacity building because not all countries have a capable cybersecurity infrastructure—international cooperation in building the capacity of world countries to maintain national and international security. Thus, mutual understanding can arise so as not to use cyber technology to disrupt the cyberinfrastructure of other countries because it is difficult to determine (attribution) the actors behind it, whether hackers or state-sponsored actors.

Based on the dynamics of reality in the international world above, it is necessary to have cyber diplomacy that the Government of Indonesia must be done. The widespread use of social media and financial transactions in cyberspace shows excellent potential and risks. The government needs to fight for cybersecurity protection for all activities on the internet to benefit the Indonesian people. The Indonesian government must also map out threats and immediately take protective measures based on in-depth analysis to obtain the right policies. The government can carry out diplomacy against other countries whose citizens are the perpetrators or origins of cyberattacks. Suppose the government is late in overcoming the protection and law enforcement in cyberspace. In that case, it will lead to enormous economic, social, and political losses because it impacts conflicts and casualties in the real world.

CONCLUSION

Based on the various explanations above, it can be understood that Indonesia's development of information and communication technology has given rise to various benefits and threats. Many Indonesian people do not fully understand the use of the internet. Meanwhile, service providers in cyberspace also do not have strong protection against various cybercrime threats. The Indonesian government has enacted the 2008 ITE Law and has encouraged the wise and positive use of the internet through various approaches. Furthermore, the Government of Indonesia also carries out cyber diplomacy efforts through several relevant ministries towards other countries, both bilaterally, regionally, multilaterally, and internationally. For example, Indonesia actively participates in cyber diplomacy at the TELMIN, ADMIN, PCC, OEWG forums and BSSN collaborating with various countries to overcome cyber threats.

However, it all depends on every internet user to always be vigilant and careful in using cyberspace to avoid the threat of cybercrime.

BIBLIOGRAPHY

Bisnis.com. *Ancaman Siber Indonesia Terbanyak Kelima Se-Asia Pasifik*. Retrived from https://teknologi.bisnis.com/read/20190306/84/896967/ancaman-siber-di-indonesia-terbanyak-kelima-se-asia-pasifik on 24 June 2021.

Badan Siber dan Sandi Negara. *Building a National Soft-Power on Cyber Space Through Cyber Diplomacy*. Retrieved from https://bssn.go.id/building-a-national-soft-power-on-cyber-space-through-cyber-diplomacy/ on 24 June 2021.

Babbie, E. (2008). *The Basics of Social Research*. Belmont: Thomson Wadsworth.

Cahyadi, Indra. (2016) Cyber Governance and Threat of National Sovereignty. *Politica*. No. 7, Vol. 2.

Chotimah, Hidayat Chusnul; Iswardhana, Muhammad Ridha; Pratiwi Tiffany Setyo. (2019). Penerapan Military Confidence Building Measures dalam Menjaga Ketahanan Nasional Indonesia di Ruang Siber. *Jurnal Ketahanan Nasional*. Vol. 25. No. 3.

CNN Indonesia. (2019). *51 Negara Dukung turan Keamanan Siber Global*. Retrieved from https://www.cnnindonesia.com/teknologi/20181113075756-185-346044/51-negara-dukung-aturan-keamanan-dunia-siber-global on 25 June 2021.

CNN Indonesia. (2021). *INFOGRAFIS: Rentetan Kebocoran Data di Indonesia Sejak 2020*. Retrieved from https://www.cnnindonesia.com/teknologi/20210523132216-188-645888/infografis-rentetan-kebocoran-data-di-indonesia-sejak-2020 on 25 June 2021.

Danuri, Muhammad dan Suharnawi. (2017). Tren Cyber Crime dan Teknologi Informasi di Indonesia. *Infokam*, No.2.

Direktorat Jenderal Peraturan Perundang-Undangan. *Hukum Teknologi Informasi*. Retrieved from http://ditjenpp.kemenkumham.go.id/hukum-teknologi/668-dinamika-konvergensi-hukum-telematika-dalam-sistem-hukum-nasional.html on 24 June 2021.

Ersya, Muhammad Prima. (2017). Permasalahan Hukum dalam Menanggulangi Cyber Crime di Indonesia. *Journal of Moral and Civic Education Edisi 2017*.

Fahmi, Novrizal. (2018). Melawan Aksi Terorisme di Media Sosial: Penggunaan Tagar #KamiTidakTakut di Twitter. *Jurnal Komunika*. Vo.1. No.1.

Febriansyah, Ferry Irawan & Purwinatro, Halda Septiana. (2020). Pertanggungjawaban Pidana bagi Pelaku Ujaran Kebencian di Media Sosial. *Jurnal Penelitian Hukum De Jure*. Vol.20. No.2.

Harian Ekonomi Neraca. (2019). *Menyikapi Positif Perkembangan Dunia Cyber*. Retrieved from http://www.neraca.co.id/article/87868/menyikapi-positif-perkembangan-dunia-cyber on 24 June 2021.

Hodzic, N. (2017). *Cyber-Diplomacy: Framing the Transformation*. Budapest: Central European University.

Infokomputer. (2021). *Pengguna Internet Indonesia Terbesar ke-4 di Dunia Ini Tantangannya*. Retrieved from https://infokomputer.grid.id/read/122756150/pengguna-internet-indonesia-terbesar-ke-4-di-dunia-ini-tantangannya on 24 June 2021.

Ishak dan Dermawan, Deni. (2019). *Teknologi Pendidikan*. Bandung: PT. Remaja Rosdakarya.

Iswardhana, Muhammad Ridha. (2021). *Diplomasi Siber dan Teknologi Mobile Pada Multidisiplin*. Padang: PACE.

Jawa Pos. (2019). *Kaleidoskop 2019: Karena Berita Hoax Kerusuhan Wamena Pecah*. Retrieved from https://www.jawapos.com/nasional/28/12/2019/kaleidoskop-2019-karena-berita-hoax-kerusuhan-wamena-pecah/ on 24 June 2021.

Juditha, Christiany. (2018). Interaksi Komunikasi Hoax di Media Sosial serta Antisipasinya Hoax Communication Interactivity in Social Media and Anticipation. *Jurnal Pekommas*. Vol. 3. No. 1.

Junaedi, Fajar. (2010). Relasi Terorisme dan Media. *Jurnal ASPIKOM*. Vo.1. No.1.

Kementerian Komunikasi dan Informasi. (2018). *Tingkatkan Koordinasi Proteksi Keamanan Siber di Indonesia*. Retrieved from https://kominfo.go.id/content/detail/14605/ciip-id-summit-2018-tingkatkankoordinasi-proteksi-keamanan-siberindonesia/0/sorotan_media on 25 June 2021.

Kementerian Luar Negeri Republik Indonesia. (2013). *Diplomasi Multilateral*. Vol. II. No.2. Jakarta: Direktorat Jenderal Multilateral Kementerian Luar Negeri RI.

Kementerian Luar Negeri Republik Indonesia. (2018). *LAKIP Kemenlu*.

Kittichaisaree, Kriangsak. (2017). *Public International Law of Cyberspace*. Switzerland: Springer International Publishing.

Kompas.com. (2020). *Akankah Work From Home Jadi Tren Setelah Pandemi Covid-19 Berakhir?*. Retrieved from https://www.kompas.com/tren/read/2020/04/21/070400465/akankah-work-from-home-jadi-tren-setelah-pandemi-covid-19-berakhir-?page=all on 25 June 2021.

Kompas.com. (2021). *7 Kasus Kebocoran Data yang Terjadi Sepanjang 2020*. Retrieved from https://tekno.kompas.com/read/2021/01/01/14260027/7-kasus-kebocoran-data-yang-terjadi-sepanjang-2020?page=all on 25 June 2021.

Kompas.com. (2021). *Jumlah Pengguna Internet Indonesia 2021 Tembus 202 Juta*. Retrieved from https://tekno.kompas.com/read/2021/02/23/16100057/jumlah-pengguna-internet-indonesia-2021-tembus-202-juta. on 25 June 2021.

Kusumasari, Dita & Arfianto, S. (2020). Makna Teks Ujaran Kebencian Pada Media Sosial. *Jurnal Komunikasi*. Vol. 12. No. 1.

Liputan6.com. (2019). *50 Juta Ancaman Siber Diblokir di Indonesia Sepanjang 2018*. Retrieved from https://www.liputan6.com/tekno/read/3947074/50-juta-ancaman-siber-diblokir-di-indonesia-sepanjang-2018?utm_expid=.9Z4i5ypGQeGiS7w9arwTvQ.0&utm_referrer=https%3A%2F%2Fwww.google.com%2F on 25 June 2021.

Magdalena, Merry dan Setyadi, Maswigrantoro R. (2007). *Cyberlaw, Tidak Perlu Takut*. Yogyakarta: Penerbit Andi.

Makarim, Edmon. (2005). *Pengantar Hukum Telematika – Suatu Kompilasi Kajian*. Yogyakarta: Badan Penerbit FH UII.

Media Indonesia. (2019). *Merajut Diplomasi Siber Indonesia*. Retrieved from https://mediaindonesia.com/read/detail/199360-merajut-diplomasi-siber-indonesia on 25 June 2021.

Ningrum, Dian Junita; Suryadi; Wardhana, Dian E.C. (2018). Kajian Ujaran Kebencian di Media. *Jurnal Ilmiah Korpus*. Vol.2. No.3.

Nuruzzaman, Muhammad. (2018). Terorisme Dan Media Sosialsisi Gelap Berkembangnya Teknologi Informasi Komunikasi. *Jurnal Ilmiah Indonesia Syntax Literate*. Vo. 3. No.9.

Okezone.com. (2021). *Bikin Geger! Berikut 3 Kasus Kebocoran Data Pribadi di Indonesia*. Retrieved from https://nasional.okezone.com/read/2021/05/31/337/2418242/bikin-geger-berikut-3-kasus-kebocoran-data-pribadi-di-indonesia?page=1 on 25 June 2021.

Parestri, Awinditya. (2016). Negara Liliput dalam Persoalan Digital: Upaya-upaya Swiss Menghadapi Ancaman Keamanan Siber. *Jurnal Analisis Hubungan Internasional*. Vol. 5. No. 2.

Paris Call (2021). *The Supporters*. Retrieved from https://pariscall.international/en/supporters on 15 November 2021.

Republika. (2021). *Kominfo: Pengguna Internet Indonesia Terbesar ke-4 di Dunia*. Retrieved from https://www.republika.co.id/berita/qv56gb335/kominfo-pengguna-internet-indonesia-terbesar-ke4-di-dunia on 25 June 2021.

Rusman; Kurniawan, Deni; Riyana, Cepi. (2013). *Pembelajaran Berbasis Teknologi Informasi dan Komunikasi; Mengembangkan Profesionalitas Guru*. Jakarta: PT. Raja Grafindo Persada.

Samudra, Anton Hendrik. (2019). Modus Operandi dan Problematika Penanggulangan Tindak Pidana Penipuan Daring. *Mimbar Hukum*. Vol. 31. No.1.

Setiadi, Sucahyo, and Hasibuan, Z. (2012). An Overview of the Development Indonesia National Cyber Security. *International Journal of Information Technology & Computer Science*. Vol. 6.

Siagian, Lauder; Budiarto, Arief, Simatupang. (2018). Peran Keamanan Siber Dalam Mengatasi Konten Negatif Guna Mewujudkan Ketahanan Informasi Nasional. *Jurnal Prodi Perang Asimetris*. Vol. 4. No. 3

Suara.com. (2014). *Membongkar Kecanggihan Pasukan Hacker Korea Utara.* Retrieved from https://www.suara.com/tekno/2014/12/24/073200/membongkar-kecanggihan-pasukan-hacker-korea-utara on 25 June 2021.

Sulaiman, Robintan. (2002). *Cyber Crimes: Perspektif E-Commerce Crime*. Tangerang: Pusat Bisnis Fakultas Hukum Universitas Pelita Harapan.

Sumenge, Melisa Monica.(2013). Penipuan Menggunakan Media Internet Berupa Jual Beli. *Lex Crimen*. Vol.II. No.4.

Tekno Kompas. (2012). *Indonesia Bangun Pusat Investigasi Kejahatan "Cyber.* Retrieved fromhttps://tekno.kompas.com/read/2013/04/30/15491539/indonesia.bangun.pusat.investigasi.kejahatan.quotcyberquot on 25 June 2021.

Wardiana, Wawan. (2002). *Perkembangan Teknologi Informasi di Indonesia, Makalah Seminar dan Pameran Teknologi Informasi 2002*. Bandung: Fakultas Teknik Unikom.