Journal of Progressive Law and Legal Studies
E-ISSN 2986-9145 E-ISSN 3031-9242
Volume 3 Issue 01, January 2025, Pp. 69-85
DOI: https://doi.org/10.59653/jplls.v3i01.1365

Cyber Law Policy Development: Indonesia's Response to International Cybercrime Threats

Muhammad Taufik Rusydi
Universitas Surakarta, Indonesia
Corresponding Email: mtaufikrusydi@gmail.com

Received: 17-12-2024 *Reviewed: 03-01-2025* *Accepted: 19-01-2025*

Abstract

The rapid development of information technology has driven the growth of the digital economy and increased the threat of cross-border cybercrime. In Indonesia, cyber law regulation still faces challenges in terms of legal substance, institutions, and implementation of law enforcement. This article explores strengthening cyber law policy in Indonesia to face global challenges in cybercrime. This article identifies various weaknesses in existing policies using a juridical-normative research method and a descriptive-analytical approach. It recommends strengthening regulatory harmonization, increasing law enforcement capacity, and international collaboration. The study results indicate that Indonesia's cyber law framework needs to be updated to be more adaptive to technological developments and global threats. In addition, integrating national law and international policy is a major highlight in increasing the effectiveness of controlling cybercrime. This article makes an important contribution to developing responsive and relevant cyber law in facing the challenges of the digital era.

Keywords: Cyber Law, Cyber Crime, Legal Policy

Introduction

Information technology has become a major pillar of modern life, from communication economy to government. The digital revolution triggered by technological developments has provided many benefits, such as increased efficiency, ease of access to information, and new economic opportunities (Ashibly & Jimmy, 2023). However, this progress also brings major challenges, especially in the form of cybercrime threats. These cybercrimes are local and cross-border, creating an urgent need for legal policies to deal with these threats' complexity. Indonesia, one of the countries with rapid digital growth, faces an increasing threat of cybercrime. Based on a report from the National Cyber and Crypto Agency (BSSN), in 2023 there were more than 1.2 million cyber incidents involving various forms of crime, such as phishing, ransomware, and Distributed Denial of Service (DDoS) attacks. This report reflects the vulnerability of digital systems in Indonesia, which harm individuals and threaten economic

stability and national security. Cybercrime can disrupt government systems, steal personal data, and even damage the country's financial system. This makes the need for policies responsive to technological dynamics very important.

Cybersecurity is a global issue that Indonesia cannot address with isolated policies. According to research by Kusuma (2020), cybercrime often involves perpetrators operating beyond national borders, making it difficult to track and prosecute in national courts. Therefore, cyber law regulations in Indonesia require integration with international standards (Mantovani, 2023), such as the Budapest Convention on Cybercrime issued by the Council of Europe. Member states participating in this convention have a more integrated legal framework to address transnational cybercrime. However, Indonesia is not yet a party to the convention, which limits international collaboration in addressing transnational cybercrime.

Although Indonesia has the Electronic Information and Transactions Law (UU ITE) as the main legal basis, the effectiveness of the law is often questioned. The ITE Law, which was first passed in 2008, covers many aspects related to electronic transactions and digital information (Ramlan & Riza, 2024). However, along with the rapid development of technology, the ITE Law is considered not yet adaptive enough to the challenges that arise. A number of groups have criticized the articles in the ITE Law, which cannot accommodate changes and new developments in the digital world, such as crimes that utilize the latest technology, such as artificial intelligence (AI) and the Internet of Things (IoT). This creates legal loopholes that cybercriminals can exploit to avoid punishment. One of the main challenges in regulating cyber law in Indonesia is the weak implementation and enforcement of the law. Many parties complain about the lack of human resources who have technical expertise in solving cybercrime cases (Casotti, 2023). Law enforcement in Indonesia often faces difficulties in identifying perpetrators who are hidden behind the globally distributed internet network. In addition, many law enforcement officers are not equipped with adequate training to handle highly technical cybercrimes. According to Santoso (2019), this deficiency leads to a high number of cybercrime cases that are not revealed or even not handled seriously by the relevant authorities. This is also exacerbated by the lack of adequate technical facilities, such as digital forensic tools needed to trace the perpetrators in cyberspace.

The importance of international collaboration in combating cybercrime cannot be ignored. This collaboration includes cooperation between countries in terms of information exchange, strengthening joint regulations, and legal action against cross-border cybercriminals. According to Pratama (2021), international cooperation is essential, considering that cybercrime often involves perpetrators and victims in different countries. Strengthening Indonesia's cyber law policy also needs cooperation with other countries in dealing with global cybercrime to face the increasingly complex challenges of cybercrime, and regulatory updates are very important. These updates are limited to the ITE Law and include implementing laws that can accommodate the latest technological developments (Palito et al., 2023). For example, Indonesian cyber law needs to pay attention to more detailed regulations on crimes that occur in cyberspace related to AI and IoT. This is also important in order to protect users' personal data, which is increasingly vulnerable to theft and misuse by irresponsible parties. Indonesia can create a safe and accountable digital ecosystem by strengthening cyber law policies (Palito

et al., 2023). This strengthening is not only related to laws that are reactive to cyber threats but must also be proactive in creating policies that can anticipate potential cyber threats in the future. With a more holistic and integrated approach, Indonesia can be better prepared to face the challenges of global cybercrime that continue to grow. (Rahmat et al., 2023)

Literature Review

In addition to weaknesses in legal substance, institutions in Indonesia also face major challenges in dealing with cybercrime. Several institutions, such as BSSN, Polri, and the Attorney General's Office, have been given the responsibility to address cybercrime. However, each institution often operates in a separate space without effective coordination. According to research conducted by Setyawan (2018), the lack of coordination between these institutions causes ineffectiveness in handling cybercrime cases as a whole. In this case, collaboration between domestic and international institutions is crucial to strengthen cyber law enforcement (Abdurrahman, 2024). Strengthening policies and institutions that strengthen cyber law policies also includes the importance of increasing the capacity of law enforcement and public education. Law enforcers in Indonesia need to be given further training on identifying, investigating, and handling more complex cybercrime cases. Setyawan (2018) also emphasized the importance of empowering educational institutions to produce experts in the field of cyber law. In addition, education and digital literacy for the public are also very important as preventive measures. According to Sugiarto (2020), increasing digital literacy can help people better understand the risks in cyberspace and help them avoid various types of cybercrime, such as phishing and identity theft. (Syukur et al., 2023)

Research Method

This study uses a juridical-normative method with a descriptive-analytical approach. The data used are secondary data derived from laws and regulations, scientific journals, reference books, and official reports from related agencies. The analysis was conducted to identify weaknesses in Indonesia's cyber law regulations and offer solutions to strengthen national cyber law policies (Pinto et al., 2023). The normative approach is used to examine the applicable legal framework, including the ITE Law and other regulations. Meanwhile, the descriptive-analytical approach is used to link the findings to the global challenges faced in cybercrime. The results of this study also refer to relevant case studies and compare cyber regulations in several countries to produce contextual recommendations for Indonesia.

Result and Discussion

Overview of Cyber Law in Indonesia

Cyber law refers to laws regulating cyberspace activities, including the use of information and communication technology (ICT), electronic transactions, and crimes committed online. In Indonesia, cyber law has developed along with the rapid use of the

internet and digital technology, which affects various aspects of people's lives (Irawan, 2024). Cyberlaw regulations in Indonesia focus on protecting personal data and electronic transactions and combating cybercrime. Indonesia, as a country with a large number of internet users, has begun to develop a legal framework to regulate various activities in cyberspace. This regulation is important to create a safe and orderly climate, both for individual internet users and for the interests of the state and the business world. The existence of this regulation also aims to protect the public from potential losses due to crimes related to information technology.

Some of the legal bases that regulate the scope of cyber law in Indonesia include:

1. Law Number 11 of 2008 concerning Electronic Information and Transactions (UU ITE)
   The ITE Law is the main basis for cyber law in Indonesia. Introduced in 2008 and updated by Law Number 19 of 2016, the ITE Law regulates electronic transactions, electronic contracts, and criminal acts that occur in cyberspace. This law also provides provisions related to the use of information for legitimate electronic transactions and overcoming crimes such as the spread of negative content and defamation.
2. Law Number 14 of 2008 concerning Openness of Public Information
   This law regulates the public's right to obtain transparent information, which also includes electronic data managed by public bodies. This law also plays a role in encouraging government accountability and clarifying the boundaries of information that the public can access.
3. Law Number 27 of 2014 concerning Amendments to Law Number 19 of 2002 concerning Copyright
   This law is important in the context of copyright protection for works published and distributed in electronic form. This protection applies to creative works distributed through digital media, such as software, music, and other digital content.
4. Law Number 36 of 1999 concerning Telecommunications
   Although this law focuses more on the telecommunications industry as a whole, it provides important regulations regarding Internet services and the control of the flow of information.

In addition to these laws, several other regulations, such as Government Regulation 82 of 2012 concerning Electronic System Service Providers, have also been issued to clarify provisions regarding electronic system organizers and their obligations in protecting user data. The implementation of cyber law in Indonesia is not without challenges. Some of the challenges faced include:

1. Inconsistency of Regulations with Technological Developments
   One of the main challenges is the inability of regulations to keep up with the rapid development of technology. Existing regulations do not yet cover many new innovations in information technology. This has led to legal loopholes that cybercriminals exploit to carry out illegal acts. For example, there is the use of blockchain technology and cryptocurrency, which do not yet have specific regulations that can regulate them firmly.
2. Public Lack of Understanding of Cyber Law
   The level of cyber law literacy in Indonesia is still low, especially among the general public. This causes many individuals to be unaware of the potential risks they face when carrying out activities in cyberspace, such as the spread of personal information or cyber-attacks. Low legal awareness also worsens efforts to prevent and deal with cybercrime.

3. Limited Human Resources (HR)
   Strengthening cyber law policies requires experts who have high competence in the fields of law and technology. Limited human resources who understand the relationship between law and technology are obstacles to effective law enforcement in cyberspace.
4. Weak Coordination Between Institutions
   Handling cybercrime cases involves various institutions, such as the police, the Ministry of Communication and Information, and personal data protection institutions. Unfortunately, coordination between these institutions is often hampered, so law enforcement in the cyber field is not optimal. In addition, the existence of jurisdictional limitations in cyberspace is also a challenge in prosecuting cybercriminals who can operate across countries.

In facing these challenges, the Indonesian government has made several efforts to strengthen cyber law policies. Several initiatives that have been implemented include:

1. Drafting of the Personal Data Protection Law
   The Indonesian government has begun drafting the Personal Data Protection Law, which is expected to provide stronger protection for internet users' personal data. This law also aims to align Indonesian policies with international standards, such as those implemented by the European Union with the General Data Protection Regulation (GDPR).
2. Improving Digital Literacy
   Along with the increasing Internet use in Indonesia, various digital literacy improvement programs have begun to be introduced. This aims to increase public understanding of potential risks in cyberspace and how to protect their personal data. Kominfo is also actively conducting campaigns and outreach related to cybersecurity and cybercrime prevention.
3. International Cooperation in Combating Cybercrime
   Cybercrime is often cross-border, so international cooperation is needed to handle it. Indonesia is actively involved in various international forums, such as Interpol and ASEAN, to strengthen its capacity to combat the threat of global cybercrime.
4. Establishment of the National Cyber Agency (BSSN)
   The Indonesian government has also established the National Cyber and Crypto Agency (BSSN), which coordinates national cyber policies, monitors and handles cyber attacks, and educates the public on cyber security. BSSN also plays a role in formulating more effective national information security policies and strategies.

More comprehensive reforms are still needed to strengthen Indonesia's cyber legal system. This includes revising the ITE Law to be more responsive to the latest technological developments and increasing the capacity of law enforcement and related state institutions. Thus, Indonesia can reduce legal loopholes exploited by cybercriminals and create a safer digital environment.

Cybercrime Challenges in a Global Context

Cybercrime is a growing threat worldwide, with implications that can threaten national security, economic stability, and individual privacy. As ICT advances, cybercrime has become more sophisticated, global, and difficult to combat. The challenges of cybercrime in a global context are not limited to attacks on computer systems or digital devices but also include attacks

on personal data, the spread of false information, and threats to critical infrastructure that is vital to a country's survival. In this section, we will discuss the main challenges faced by countries around the world in dealing with cybercrime. Cybersecurity is facing increasingly complex threats. Cybercrime is no longer simple, such as data theft or system destruction, but now involves sophisticated techniques that are difficult to detect.

Cyberattacks, known as Advanced Persistent Threats (APT), refer to a type of attack that lasts for a long time and is carried out by perpetrators with high technical skills. APTs are usually used by hacker groups supported by a particular country or organization to damage or steal essential data from countries or large companies. These attacks are carried out in a very stealthy manner and often collaborate with other techniques such as phishing and malware to gain access to sensitive systems or data. Another type of attack that is increasingly popular is ransomware, where perpetrators attack critical systems or data by encrypting the information, and then demanding a ransom to return it. Ransomware has threatened many organizations around the world, including the healthcare, financial, and critical infrastructure sectors. One well-known example of a ransomware attack is the attack on hospitals and healthcare systems in various countries, which resulted in huge losses for the public and government.

Cybercrime is often transnational, meaning that perpetrators can operate from one country and attack targets in another. Transnational cybercrime poses significant challenges for law enforcement because laws in different countries often differ in substance and application. The country where the attack takes place may have a different legal system than the country where the perpetrator operates, making investigation and prosecution difficult. Many countries lack clear laws regarding cybercrime or have weak policies to combat it. This provides opportunities for perpetrators to escape legal responsibility by changing the location of the attack and hiding their tracks. Transnational cybercrime requires stronger international cooperation between countries to combat the threat. A country's critical infrastructure, such as its power grid, transportation, and communications systems, are prime targets for cyberattacks. Attacks on critical infrastructure can cause significant damage, disrupting people's lives and impacting a country's economy. One of the most notorious attacks targeting critical infrastructure was the Stuxnet attack, a computer worm designed to attack industrial control systems at Iranian nuclear facilities. These attacks cause physical damage and threaten national and international stability. Attacks on critical infrastructure are increasingly common and can have far-reaching impacts. Cybercrimes targeting the energy, clean water, health, and transportation sectors can destabilize a country, even causing enormous economic and social security damage. Therefore, countries around the world need to strengthen the protection of this critical infrastructure by implementing appropriate policies to reduce the risk of cyberattacks.

In addition to attacks on physical infrastructure and data, one of the major challenges in the context of global cybercrime is the spread of false information or hoaxes, as well as propaganda that can damage social and political integrity. Social media and other digital platforms are often used to spread misinformation, manipulate public opinion, incite hatred, or change election results. Although not always involving hardware or software, these attacks can have a much greater social and political impact and undermine democracy. The spread of

disinformation or hoaxes is very dangerous because it can create distrust among citizens, exacerbate political polarization, and trigger social tensions. In recent years, countries such as the United States, Russia, and China have used disinformation campaigns through social media to influence elections or create political instability in other countries.

Personal data security has become a major issue in global cyber law. The increasing use of digital technology has resulted in the threat of personal data theft becoming more prevalent. Personal data, such as personal identification numbers, credit card information, and medical data, are often the targets of cyber attacks. Crimes involving identity theft, online fraud, and theft of financial information are increasingly being discovered. Various personal data leaks involving large companies, such as the data leak cases experienced by Facebook or Google, reveal the extent to which privacy and personal data threats can damage public trust in digital platforms. Countries worldwide are starting to adopt policies to protect personal data more strictly, one of which is by implementing regulations such as the General Data Protection Regulation (GDPR) in the European Union. However, even though regulations such as GDPR have been implemented, there are still many challenges in implementing them in various countries that do not have equivalent privacy policies.

Comparison of Cyber Law Policies with Other Countries

Comparing cyber law policies between countries is one way to understand the differences and similarities in approaches to combating cybercrime and finding the best solutions to address existing challenges. Each country has different characteristics and legal needs, so policies and regulations related to cyber law can vary. In this discussion, we will compare Indonesia's cyber law policies with those of several other countries, such as the United States, the European Union, and Singapore, to illustrate the various global approaches to cyber threats.

1. ***Indonesian Cyber Law Policy***

   In Indonesia, cyber law policy is still developing. The Indonesian government has taken significant steps in formulating policies to deal with cybercrime, from drafting laws and regulations to establishing institutions that handle this issue. One of the main steps is the implementation of the ITE Law, which is the legal basis for cybercrime in Indonesia.

   The ITE Law regulates various matters related to electronic transactions and information in cyberspace, including protecting personal data, distributing illegal content, and threats to information and computer systems. Although there are clear regulations, their implementation still often faces challenges, especially related to the ambiguous definition of hate speech and defamation in cyberspace. Some parties consider that the ITE Law is often misused to silence criticism and freedom of expression in Indonesia. In addition to the ITE Law, Indonesia also has the BSSN, which functions as an institution responsible for improving national cybersecurity, including protecting critical infrastructure and strengthening the capacity of human resources in the cyber field. However, despite progress, Indonesia's cyber law policy still has shortcomings, especially in terms of coordination between institutions and effective law enforcement at the regional level.

2. United States Cyber Law Policy

The United States is one of the countries with a highly developed cyber law policy. One of the main regulations implemented in the US is the Computer Fraud and Abuse Act (CFAA), which regulates hacking and misuse of computer access. In addition, the Federal Information Security Management Act (FISMA) regulates government information security, while the National Cybersecurity Protection Act (NCPA) provides a legal basis for regulating cyber protection in the public and private sectors.

The United States also implements the Cybersecurity Information Sharing Act (CISA), which facilitates the exchange of information related to cyber threats between the public and private sectors. In terms of law enforcement, the US has agencies such as the Federal Bureau of Investigation (FBI), which plays an active role in handling transnational cybercrime. The FBI works with international agencies like Interpol and Europol to handle global cybercrime. The United States' approach to cyber policy focuses heavily on public-private cooperation and information exchange to improve the response to cyber threats. This policy is considered effective, although challenges remain, such as privacy issues and misuse of data collected by private companies. Overall, US cyber law policy is more open to technology and innovation, albeit with stricter controls on potential abuse.

3. EU Cyber Law Policy

The European Union has been a leader in cyber law policy, with the General Data Protection Regulation (GDPR) being a particularly influential regulation. The GDPR is a regulation that provides stronger protection for its citizens' personal data by regulating individuals' rights to control their personal data. In addition, the GDPR also imposes obligations on companies to ensure that the data collected and processed is safe from cyber threats. The EU also has a Cybersecurity Act, which sets out a framework for improving cybersecurity across Europe. The Cybersecurity Act establishes the European Union Agency for Cybersecurity (ENISA), which works to strengthen the capacity and coordination of member states in dealing with cyber threats. In addition, the EU has drafted the Network and Information Systems Directive (NIS Directive), which regulates the protection of critical infrastructure and increases the resilience of information systems across sectors, including energy, transport, and healthcare. The EU focuses heavily on the protection of personal data and the rights of individuals in cyberspace. This policy provides very strict protection for the privacy of its citizens but is often considered too bureaucratic by some, as many companies struggle to meet the requirements set by the GDPR. Despite this, the European Union remains the global benchmark for privacy regulations and personal data protection.

4. Singapore Cyber Law Policy

Singapore is known for its proactive and modern legal policy in cybercrime. The country has a Cybersecurity Act that regulates cybersecurity in various sectors, including critical infrastructure, digital services, and the business sector. The Cybersecurity Act authorizes the Cyber Security Agency of Singapore (CSA) to oversee and regulate cybersecurity throughout the country. Singapore also implements the Personal Data Protection Act

(PDPA), which focuses on protecting personal data. The PDPA gives individuals the right to access and correct their personal data and ensures that company data is stored and processed securely. In addition, Singapore is also an active member of various international organizations that deal with cybercrime issues, such as the Asia-Pacific Economic Cooperation (APEC) and Interpol. Singapore's approach to cyber law policy is highly integrated between the public and private sectors, with a focus on the resilience of critical infrastructure and the protection of personal data. The country also has a clear and coordinated legal infrastructure, with institutions specifically dealing with cybercrime. Singapore's success in creating an effective cyber law policy is also thanks to the development of a safe and innovative digital ecosystem. The comparison of cyber law policies in Indonesia, the United States, the European Union, and Singapore shows several striking similarities and differences. Some similarities include a focus on personal data protection, strengthening policies for critical infrastructure, and implementing laws governing cyber attacks. However, there are significant differences in terms of implementation, coordination between institutions, and the level of public trust in these policies. Indonesia still faces challenges in terms of policy implementation and coordination between institutions, while the United States prioritizes public-private cooperation in combating cybercrime. The European Union has a stricter approach to personal data protection, while Singapore is the best example of creating an integrated policy between the public and private sectors with a focus on infrastructure resilience.

Analysis of Weaknesses of Cyber Law Policy in Indonesia

As a developing country with the largest population in Southeast Asia, Indonesia faces major challenges in dealing with increasingly sophisticated cyber threats. Although various policies and regulations have been implemented to address this issue, cyber law policy in Indonesia still faces a number of weaknesses that hinder the effectiveness of combating cybercrime. In this discussion, we will analyze the various weaknesses of cyber law policy in Indonesia, starting from legal aspects, institutions, and social and cultural issues affecting its implementation.

1. **Ambiguity in Legal Regulations**

One of the main weaknesses of cyber law policy in Indonesia lies in the lack of clarity and ambiguity in several existing legal regulations. One of them is the ITE Law, which is the main legal basis for dealing with cybercrime in Indonesia. Although the ITE Law has been amended several times, many provisions in the law are still being debated, especially regarding the definition of various forms of cybercrime, such as the spread of fake news (hoaxes) and hate speech.

For example, articles regulating content that violates moral norms or fake news are often widely understood, which can confuse the application of the law. Many parties argue that these provisions have the potential to be misused to limit freedom of expression and the right to information. This shows that the lack of clarity in legal regulations can lead to indecisiveness in law enforcement and uncertainty for people involved in digital activities. Regulations on personal data protection contained in the ITE Law are also often not fully effective. Several sectors, such as the health and banking sectors, have not yet fully

complied with the obligation to protect their citizens' personal data. This is due to the absence of a clear and firm comprehensive law on personal data protection.

2. A mismatch between National Law and International Law

The success of combating cybercrime depends on domestic law and the country's ability to cooperate with other countries at the international level. Cybercrime is often transnational, which makes law enforcement more complex. Although Indonesia has a fairly strong legal framework at the national level, it still has limitations in terms of international cooperation in dealing with cybercrime.

Several developed countries, such as the United States and European Union countries, have formulated more coordinated cyber law policies and have strong international agreements to deal with cybercrime. Indonesia, on the other hand, has not been fully integrated into the international agreement system related to cyber law, such as the Budapest Convention on Cybercrime. This makes it difficult for Indonesia to cooperate with other countries to handle increasingly complex cases of transnational cybercrime.

Although Indonesia has signed international agreements such as the ASEAN Cybersecurity Cooperation Strategy, its implementation in the field is often hampered by political and administrative constraints. Without a clear international agreement, Indonesia will have difficulty dealing with cybercrime involving international actors.

3. Fragmented Institutions

One of Indonesia's main weaknesses in cyber law policy is institutional fragmentation, which causes ineffective coordination between various institutions that have a role in combating cybercrime. Indonesia has several institutions related to cybersecurity, such as BSSN, Polri, and Kominfo. However, the lack of good coordination between these institutions often hinders a quick and effective response to cyber threats.

For example, BSSN is responsible for supervising and protecting critical infrastructure, while Kominfo focuses more on supervising and regulating internet service providers. Meanwhile, Polri is responsible for enforcing the law against cyber criminals. This fragmentation creates unclear duties and authorities between institutions, which can slow down efforts to mitigate and combat cybercrime. In addition, fragmented institutions also reduce Indonesia's ability to implement comprehensive and coordinated policies in dealing with cyber threats.

4. Lack of Trained Human Resources (HR)

Cybersecurity depends not only on policies and regulations but also on the quality of the HR personnel who handle this issue. In Indonesia, there is still a shortage of experts in the field of cybersecurity, both in the public and private sectors. Although there have been efforts to train professionals in this field, the need for trained and competent experts in the cyber sector is very high. Several government agencies, including the National Police and BSSN, have conducted training to improve human resources' ability to handle cybercrime. However, the number of experts available is still limited, especially in areas far from the

center of government. In addition, existing training does not fully cover the entire spectrum of knowledge needed, from an understanding of hacking techniques to policies and strategies in dealing with global cyber threats. Increasing the capacity of human resources in the cyber field must be a priority for Indonesia, especially considering the ever-growing cyber threats. One way to achieve this is by increasing cooperation with international universities and training institutions to produce experts ready to face cyberspace's challenges.

5. **Social and Cultural Issues**

   In addition to technical and institutional weaknesses, social and cultural issues also affect the effectiveness of cyber law policies in Indonesia. One of the influencing factors is the level of public awareness of the importance of cyber law. Many Indonesians, especially in rural areas, do not understand cyber threats and how to protect themselves in cyberspace. This challenge is also influenced by the still limited level of education in some areas, which makes it difficult for people to understand issues related to the security and privacy of personal data. A broader and more structured educational campaign on the importance of cybersecurity and the need to comply with legal regulations is urgently needed to raise public awareness of the importance of keeping their data and information secure.

Strategy for Strengthening Cyber Law Policy in Indonesia

Cybersecurity has become one of the main issues in the development of information technology in Indonesia. Along with the increasing dependence on technology and the internet, the threat of cybercrime is increasingly complex and disturbing various sectors of life. Therefore, strengthening cyber law policies is very important to protect personal data, critical infrastructure, and the integrity of information systems. In this discussion, strategies that can be applied to strengthen cyber law policies in Indonesia will be outlined, including:

1. **More Comprehensive Regulation Improvement**

   One of the first steps that must be taken to strengthen cyber law policy is to update and improve existing regulations. The ITE Law, which has been in place since 2008, is indeed an important legal basis for regulating cyber activities in Indonesia. However, the ITE Law needs to be updated to better suit technological developments and the challenges that arise along with changing times. The revision of the ITE Law must prioritize clarity and openness, especially in defining types of cybercrime, such as the spread of hoaxes, hate speech, hacking, and online fraud. Ambiguity in regulating cybercrime often leads to inconsistent law enforcement and raises various problems in practice. For example, articles related to hate speech and defamation are often misused to silence freedom of expression. Therefore, the revision of the ITE Law must create clear boundaries about what is meant by cybercrime and ensure that freedom of expression remains guaranteed.

   Indonesia also needs to develop new regulations that focus more on protecting personal data, given the importance of information security in the digital world. The Personal Data Protection Law (UU PDP) that has begun to be discussed by the government must be passed immediately to provide a clear legal basis regarding the protection of personal data

and citizens' rights in cyberspace. This regulation must also include obligations for companies or third parties that manage personal data to ensure that they do not misuse their users' personal information. This is important so that citizens can feel safe in using digital services.

2. Improving Inter-Agency Coordination

As a country facing cross-border cyber threats, Indonesia needs a more coordinated approach between various institutions that have a role in cybersecurity. In this case, strengthening coordination between institutions such as the National Cyber and Crypto Agency (BSSN), the Indonesian National Police (Polri), the Ministry of Communication and Informatics (Kominfo), and other institutions is very important. Cybercrime often involves more than one institution to identify, prevent, and handle violations that occur. Establishing the National Cyber Security Coordination System (SKKSN) could be a solution. SKKSN aims to integrate all institutions that play a role in cybersecurity, from monitoring critical infrastructure and monitoring cyber activities to law enforcement. Good coordination between these institutions will accelerate the response to cyber threats and prevent greater losses due to cybercrime. Existing institutions must also strengthen the mechanism for exchanging information effectively and efficiently. For example, BSSN can be more active in providing information about threats and vulnerabilities to the Ministry of Communication and Information and the National Police so that follow-up actions to handle cybercrime can be carried out more quickly and precisely.

3. Improving the Quality of Human Resources (HR)

Success in dealing with cybercrime is highly dependent on the abilities and skills of cyber professionals. Therefore, improving the quality of HR in the legal and information technology sectors must be one of the main strategies for strengthening cyber law policies in Indonesia. Indonesia must ensure that professionals in law, information technology, and cybersecurity have adequate expertise to handle the ever-growing challenges in cyberspace. To that end, the government and private sector need to work together to provide better education and training for cybersecurity experts. One important step is to organize more frequent training programs and involve international experts in cybersecurity to provide a better understanding of the latest developments in cybercrime and the technology used by criminals (Nuarsa et al., 2023). In addition, universities and educational institutions in Indonesia must also strengthen the curriculum in the field of technology law and cybersecurity so that the younger generation involved in the world of law and technology has relevant skills.

This improvement in the quality of human resources applies not only to the government sector but also to the private sector. The private sector, especially large companies, also store users' personal data, which needs to be properly protected. Therefore, education on privacy policies and data security must be integrated into every aspect of company management, and competent professionals must be involved in this field.

4. **Improving International Cooperation**

   Cybersecurity is cross-border, so countries need to establish international cooperation to deal with increasingly complex cybercrime threats. Indonesia must increase its participation in international agreements and forums discussing cybersecurity, such as the Budapest Convention on Cybercrime, the first international agreement to regulate cybercrime. By joining this international agreement, Indonesia can increase its capacity to address cyber threats involving perpetrators from various countries. In addition, Indonesia needs to strengthen cooperative relations with other countries in exchanging information on cyber threats and attacks. One step that can be taken is to strengthen the ASEAN Cybersecurity Cooperation Strategy, which prioritizes cybersecurity in the Southeast Asia region. Indonesia will be better prepared to handle transnational cyber threats by working together at the regional level.

5. **Education and Socialization to the Community**

   In addition to stricter legal policies and more coordinated institutions, public awareness also plays a very important role in strengthening cyber law policies. Communities that are aware of the importance of protecting personal data and the potential for cybercrime will be more careful in using technology and the internet. Therefore, education about cybersecurity must be part of government policy. The government must launch a more intensive socialization campaign regarding the importance of personal data protection and information security. One effective way is to hold seminars, training, and workshops targeting all levels of society, both in urban and rural areas. This socialization must involve the private sector, civil society organizations, and educational institutions to achieve maximum results.

6. **Development of Cybersecurity Infrastructure**

   The security of critical infrastructure, such as energy, transportation, banking, and government systems, must be a priority in Indonesia's cyber law policy. Therefore, it is necessary to develop and improve a more modern cybersecurity infrastructure that is resistant to cyber threats. This can be done by updating the technology and systems used to protect critical infrastructure and conducting tighter monitoring of potential threats. One example of an effort that can be made is to build centers for monitoring and early detection of cyber threats, such as those carried out by BSSN. This monitoring center can monitor, detect, and respond to cyber threats that can endanger critical infrastructure and provide real-time information to the authorities to take immediate action.

Conclusion

Strengthening cyber law policies in Indonesia is a strategic step that must be taken to face the increasingly complex and diverse challenges of cybercrime. Cybercrime has grown rapidly along with advances in information and communication technology, which threatens privacy, data security, and the integrity of information systems in various sectors. Therefore, regulatory updates such as the revision of the ITE Law and the implementation of the Personal

Data Protection Law (UU PDP) are very important to ensure clarity of regulations in dealing with cyber threats.

Strengthening coordination between institutions, such as BSSN, Polri, and Kominfo, is necessary to handle cyber threats effectively and efficiently. Cooperation between institutions will accelerate the response to cross-border cyber attacks. The importance of improving the quality of human resources in the legal and information technology sectors also cannot be ignored. Through adequate training and education, Indonesia can produce competent experts to handle cyber crimes professionally. In addition, international cooperation in terms of agreements and exchange of information regarding cyber threats will help Indonesia in dealing with global cyber threats. By strengthening cyber law policies, improving coordination between institutions, improving the quality of human resources, and strengthening international cooperation, Indonesia will be better prepared to face the challenges of cybercrime and ensure the protection of personal data and the country's critical infrastructure. Strengthening this policy will be a solid foundation for creating a safe, secure, and trustworthy digital ecosystem for all levels of society

References

Abdurrahman, U. (2024). Correlation of Cyber Law with Civil Law: Theoretical and Practical Studies. *International Journal of Sustainability in Research*, *2*(1). https://doi.org/10.59890/ijsr.v2i1.1146

Arifin, J. (2019). Tantangan dan solusi dalam hukum siber. Jurnal Hukum dan Teknologi, 7(4), 120–130.

Ashibly, A., & Jimmy, F. (2023). Tiki Taka's Strategy as an Effort to Prevent Copyright Infringement in Indonesia: E-Commerce Platforms on Digital Era. *Journal of Progressive Law and Legal Studies*, *2*(01), 13–22. https://doi.org/10.59653/jplls.v2i01.448

Badan Siber dan Sandi Negara. (2020). Strategi keamanan siber nasional.

Badan Siber dan Sandi Negara. (2021). Laporan tahunan keamanan siber nasional 2021.

Badan Siber dan Sandi Negara. (2023). Laporan statistik insiden siber Indonesia tahun 2023. Jakarta: BSSN.

Budi, S. (2022). Koordinasi antar lembaga dalam penanganan kejahatan siber. Jurnal Kejahatan Siber, 6(2), 110–118.

Cyber Security Agency of Singapore. (2021). Cybersecurity Act 2021.

Casotti, F. (2023). About Borders, Horses and Gatekeepers: The Evolution of Interoperability and Networks Access Debate in Cyberlaw. *Revista de Direito, Estado e Telecomunicacoes*, *15*(2). https://doi.org/10.26512/lstr.v15i2.45341

European Commission. (2018). General Data Protection Regulation.

European Council. (2001). Budapest Convention on Cybercrime. Strasbourg: European Council.

Federal Communications Commission (FCC). (2021). Cybersecurity in the United States.

Harahap, M. (2020). Perkembangan teknologi dan implikasi hukum di Indonesia. Jurnal Hukum Teknologi, 5(3), 45–58.

Harrison, L. (2022). Protecting critical infrastructure in the age of cyber attacks. Journal of National Security, 13(2), 59–71.

Irawan, B. (2024). Juridical Reviewcyber Law On Developmentfintech In Indonesia. *Journal of Law and Sustainable Development*, *12*(1). https://doi.org/10.55908/sdgs.v12i1.2466

Interpol. (2020). Kerja sama internasional dalam menanggulangi kejahatan siber.

Kelly, P. (2020). The rise of data breaches and their consequences. Journal of Privacy Law, 22(2), 78–90.

Kementerian Komunikasi dan Informatika. (2020). Perlindungan data pribadi: Status dan tantangannya.

Kementerian Komunikasi dan Informatika. (2021). Peningkatan literasi digital di Indonesia.

Kementerian Komunikasi dan Informatika. (2020). Rancangan undang-undang perlindungan data pribadi.

Kusuma, D. (2020). Kelemahan kebijakan siber di Indonesia dan solusinya. Jurnal Hukum dan Teknologi, 10(2), 123–140.

Mantovani, R. (2023). DAMPAK BERITA HOAX TERHADAP KEAMANAN NEGARA DALAM PERSPEKTIF CYBERLAW BELA NEGARA. *Jurnal Magister Ilmu Hukum*, *8*(2). https://doi.org/10.36722/jmih.v8i2.2305

Nuarsa, I. K. G., Paraniti, A. A. S. P., & Pidada, I. B. A. (2023). Effectiveness of Law Number 2 of 2002 Concerning Police Members Who Commit Alleged Violations or Criminal Acts in the Case of Ferdy Sambo. *Journal of Progressive Law and Legal Studies*, *1*(03), 181–186. https://doi.org/10.59653/jplls.v1i03.251

O'Neill, J. (2021). Disinformation campaigns: A global threat to democracy. Journal of Political Cybersecurity, 10(1), 145–158.

Palito, J., Raila, T. A., Safiranita, T., & Permata, R. R. (2023). The spread of hoax through digital platforms in the perspective of Indonesian cyberlaw. *International Journal of Public Law and Policy*, *9*(2). https://doi.org/10.1504/ijplap.2023.10053504

Pemerintah Indonesia. (1999). Undang-Undang Nomor 36 Tahun 1999 tentang Telekomunikasi. Sekretariat Negara. Jakarta.

Pemerintah Indonesia. (2008). Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik. Sekretariat Negara. Jakarta.

Pemerintah Indonesia. (2008). Undang-Undang Nomor 14 Tahun 2008 tentang Keterbukaan Informasi Publik. Sekretariat Negara. Jakarta.

Pemerintah Indonesia. (2016). Undang-Undang Nomor 19 Tahun 2016 tentang Perubahan Atas Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik. Sekretariat Negara. Jakarta.

Pinto, F. C. de S., Garcia, L. R., & Rosa, A. M. da. (2023). RIGHTS FOR ROBOTIZED HUMANS OR RIGHTS OF HUMANIZED ROBOTS? *Novos Estudos Juridicos*, *28*(3). https://doi.org/10.14210/nej.v28n3.p536-553

Pratama, A. (2021). Kolaborasi internasional untuk penegakan hukum siber di Indonesia. Jurnal Hukum Internasional, 7(1), 78–95.

Purnama, D. (2023). Masyarakat dan keamanan siber: Menanggulangi krisis di era digital. Jurnal Sosial dan Budaya, 12(1), 33–47.

Rahmat, R. F., Aziira, A. H., Purnamawati, S., Pane, Y. M., Faza, S., Al-Khowarizmi, & Nadi, F. (2023). Classifying Indonesian Cyber Crime Cases under ITE Law Using a Hybrid of Mutual Information and Support Vector Machine. *International Journal of Safety and Security Engineering*, *13*(5). https://doi.org/10.18280/ijsse.130507

Ramlan, R., & Riza, F. (2024). Supervision of Fishery Resources through Integrated Technology. *Journal of Progressive Law and Legal Studies*, *2*(02), 82–92. https://doi.org/10.59653/jplls.v2i02.646

Richards, M. (2021). Ransomware and the growing threat to global cybersecurity. International Cyber Law Review, 5(1), 67–81.

Santoso, A. (2019). Analisis keamanan siber di era digital: Tantangan dan kebijakan. Jurnal Teknologi Informasi, 8(3), 45–59.

Setiawan, J. (2022). Tantangan implementasi UU ITE dalam penanggulangan kejahatan siber. Jurnal Hukum dan Teknologi, 7(3), 89–101.

Setiawati, L. (2021). Keamanan siber dalam perspektif hukum internasional. Jurnal Hukum Internasional, 8(2), 45–60.

Setyawan, R. (2018). Hukum siber di Indonesia: Perspektif dan tantangan. Yogyakarta: Deepublish.

Silverman, R. (2019). The Stuxnet attack and its global implications. Journal of Cyber Warfare, 12(4), 112–126.

Simmons, J. (2020). Cyber crime and international cooperation. Global Cybersecurity Journal, 7(3), 93–104.

Sugiarto, D. (2020). Peningkatan literasi digital sebagai upaya pencegahan kejahatan siber. Jurnal Literasi Digital, 5(1), 1–15.

Suharto, A. (2023). Perlunya reformasi dalam hukum siber Indonesia. Jurnal Hukum Siber, 9(1), 45–65.

Supriyanto, H. (2021). Sumber daya manusia dalam penegakan hukum siber. Jurnal Penegakan Hukum, 8(1), 85–95.

Syukur, G. F., Amirulloh, M., & Haffas, M. (2023). USAGE OF COPYRIGHTED SONGS

AND/OR MUSIC FROM YOUTUBE BY DISCORD MUSIC BOT ACCORDING TO INDONESIAN COPYRIGHT AND CYBER LAW. *Jurnal Poros Hukum Padjadjaran*, *5*(1). https://doi.org/10.23920/jphp.v5i1.1316

Thomas, S. (2020). Advanced persistent threats: A new era of cybersecurity. Journal of Cyber Security, 18(2), 34–45.