JURNAL HUKUM Khaira Ummah

E-ISSN: 2988-3334
ISSN: 1907-3319
Vol. 20 No. 1 March 2025

Master of Law, UNISSULA

Criminal Law Policy Based on Pancasila Values in the Framework of Strengthening Cyber Security

Doni Akbar Alfianda
Faculty of Law, Sultan Agung Islamic University, Semarang, Indonesia, E-mail: DoniAkbarAlfianda.std@unissula.ac.id

Abstract. *Today, threats to the sovereignty of the Indonesian nation are no longer military threats or colonialism over the seizure of a region conventionally, we are entering a digital era where crime enters virtual spaces that can even be said to be borderless. Crime in the digital era is commonly called cybercrime. Cybercrime not only has the potential to damage personal data and information, but can also destroy economic and business activities, infrastructure, and even the stability of a country's national security. Cybercrime is a crime committed by utilizing information and communication technology (ICT). This crime can be said to be an extraordinary crime, therefore in overcoming and preventing it, extraordinary measures are also needed. Prevention and overcoming should be carried out using a criminal law policy approach based on the values of Pancasila. Pancasila is the ideology of the Indonesian nation which is the basis of the state, legal views and legal ideals (rechtidee) of its people in living the life of the nation and state. In addition, Pancasila is also full of respect for humanitarian values and protection of human rights. In such conditions, the existence and relevance of Pancasila in the process of implementing and formulating criminal law policies are not automatically established, but require various efforts to enforce them. National criminal law policies in the context of strengthening and developing cyber security must lead to state goals and be guided by the values of Pancasila as the foundation of the state.*

Keywords: *Criminal; Cyber; Law.*

1. Introduction

Crime (mala per se) is a social phenomenon whose existence and development cannot be separated from various political, economic, social and cultural problems in society.[1]Multidimensional globalization factors supported by advances in modern communication, transportation and information technology also have a major influence on the development of crime.[2]The description certainly illustrates the threat to the sovereignty of a nation, which has now experienced rapid development and has various forms, both visible and invisible. Today, the threat to the sovereignty of the Indonesian nation is no longer a military threat or colonization of the seizure of a region conventionally, we are entering the digital era where crime enters virtual spaces that can even be said to be borderless. Crime in the digital era is commonly called cybercrime. Cybercrime not only has the potential to

[1]Muladi and Diah Sulistyani RS, Complexity of the Development of Criminal Acts and Criminal Policy, (Bandung: Alumni, 2016), p. 24
[2]Ibid, this is commonly known as the term globalization of crime.

E-ISSN: 2988-3334
ISSN: 1907-3319
Vol. 20 No. 1 March 2025

damage personal data and information, but can also destroy economic and business activities, infrastructure, and even the stability of a country's national security.[3]

In the past 2 (two) years, Indonesia has experienced various cyber attacks from irresponsible parties. The Bjorka case in 2022 shocked the Indonesian government. Bjorka claimed to have hacked documents belonging to President Joko Widodo in the period 2019 to 2021. In the case of alleged hacking of documents claimed to belong to President Jokowi in the period 2019 to 2021, the hacker with the identity Bjorka admitted to having uploaded 679,180 documents in a compressed condition.[4]Another case is the data breach of 337 (three hundred and thirty seven) million data managed by the Directorate General of Population and Civil Registration of the Ministry of Home Affairs, which according to cyber security expert Alfons Tanujaya, this incident is considered very serious.[5]This is because the leaked data contains the full name of the biological mother, which is usually used to verify banking security. In addition, there was also a case of a leak of Bank Syariah Indonesia (BSI) customer data in 2023, which triggered a response from member of Commission XI of the Indonesian House of Representatives Masinton Pasaribu who then asked the Financial Services Authority (OJK) to carry out monitoring and supervision functions for the acceleration of digitalization of all banks in Indonesia.[6]

One very important aspect of cybercrime is that this act can be carried out at a great distance, even outside the jurisdiction of the victim, which makes it difficult to deal with and prevent this crime. In addition, it is also necessary to state the factors that cause cybercrime, as follows:[7]

1. Unlimited internet access. The interconnectedness of one network to another makes it easier for criminals to carry out their actions;
2. Negligent use of a computer;
3. Easy to do with little security risk and no need for super modern equipment. Although computer crime is easy to do but it will be very difficult to track it, so this encourages criminals to do this;
4. The perpetrators are generally intelligent, curious, and fanatical about computer technology. The knowledge of computer criminals about how a computer works is far above that of computer operators;
5. Lack of public and law enforcement attention;
6. Weak network security system;
7. *Cybercrime*viewed as an economic product.

[3]See https://bpptik.kominfo.go.id/Publikasi/detail/jenis-jenis-serangan-siber-di-era-digital (accessed on May 22, 2024)
[4]See https://www.bbc.com/indonesia/indonesia-62870532 (accessed 22 May 2024)
[5]See https://www.bbc.com/indonesia/articles/c51v25916zlo (accessed 22 May 2024)
[6]See https://www.dpr.go.id/berita/detail/id/44937/t/BSI+Data+Leaks%2C+OJK+Requested+to+Run+the+Function+of+Digitalization+Acceleration+of+All+Banks (accessed on May 22, 2024)
[7]Amin Suhaimin and Muslih, Op.Cit, p. 22

E-ISSN: 2988-3334
ISSN: 1907-3319
Vol. 20 No. 1 March 2025

In 2023, BSSN determined the "Top 3 Cyber Incidents" in the 2023 Indonesian Cyber Security Landscape Report, which included:[8]

1. Web Defacement Incidents: Web defacement attacks are actions carried out by unauthorized parties to exploit a website by damaging, modifying, or deleting content on the website. In 2023, the most web defacement cases occurred in January with the largest sector being Government Administration. In relation to online gambling incidents, government websites are targeted by exploiting vulnerabilities that allow threat actors to insert scripts that can display online gambling displays so that they can affect the reputation of the agency and public trust in the services provided by the government. In addition, in more severe impacts, victim agencies can experience data theft and full takeover of access rights;

2. Ransomware Incidents: Ransomware incidents are cyber incidents triggered by malware that attacks a device, encrypts the data it contains, and steals the data with the aim of intimidating the victim into paying a ransom to regain access to the data. Currently, ransomware tactics have evolved into double extortion, where in addition to holding data hostage through encryption, the perpetrator also threatens to reveal sensitive data if the ransom is not handed over by the system owner;

3. Data Breach Incident: A data breach is a situation in cyberspace where confidential information or data owned by an organization is accessed and disclosed to the public by a threatening party, without the knowledge of the system owner. Data taken by the threat actor usually includes highly personal information, such as Personal Identifiable Information (PII), highly confidential data for individuals or organizations, and other information that should only be known by authorized parties.

Indirectly, this crime not only attacks the sovereignty of the state but also attacks the state ideology, namely Pancasila. Therefore, this crime can be categorized as an extraordinary crime, therefore in overcoming and preventing it, an extraordinary measure is also needed. Prevention and overcoming should be carried out using a criminal law policy approach based on the values of Pancasila. Pancasila is the ideology of the Indonesian nation which is the basis of the state, legal views and legal ideals (rechtidee) of its people in living the life of the nation and state. In addition, Pancasila is also full of respect for humanitarian values and protection of human rights.[9]In such conditions, the existence and relevance of Pancasila in the process of implementing and formulating criminal law policies are not automatically established, but require various efforts to enforce them. National criminal law policies in the context of strengthening and developing cyber security must lead to state goals and be guided by the values of Pancasila as the foundation of the state.[10]

2. Research methods

[8]National Cyber and Crypto Agency, Indonesian Cyber Security Landscape 2023, (BSSN: Jakarta, 2023), pp. 62-71
[9]Pujiono, Collection of Criminal Law Writings, (Bandung: Mandar Maju, 2007), p. 1
[10]Mahfud MD, "Legal Politics Towards the Development of a National Legal System" presented at the Seminar on the Direction of Legal Development According to the 1945 Constitution as a Result of the Amendment at the BPHN in 2006 at the National Legal Development Agency, Final Report of the Working Group on Legal Analysis and Evaluation related to Strengthening the Pancasila Ideology, (Jakarta; BPHN, 2019), p. 1

This writing uses a normative legal research approach, with a legislative and conceptual approach, which also examines document studies, namely using various secondary data such as laws and regulations, court decisions and legal theories.[11]

3. Resultsh and Discussion

3.1. Definition and Forms of Cybercrime in the Digital Era

In this digital era, forms of crime have evolved and become more complex. Before the internet spread globally as it is today, cybercrime was also known as computer crime. Barda Nawawi Arief quoted the opinion of the Organization for Economic Co-Operation and Development (OECD), that what is meant by computer crime is "any illegal, unethical or unauthorized behavior involving automatic data processing and/or transmitting of data".[12]

In today's digital and internet of things era, the concept of computer crime has developed into a broader and more complex concept, which is then known as cybercrime. According to Gregory, cybercrime is a form of virtual crime by utilizing computer media connected to the internet, and exploiting other computers connected to the internet as well. The existence of security holes in the operating system causes weaknesses and opens holes that can be used by hackers, crackers and script kiddies to infiltrate the computer.[13]In other literature it is also stated that cybercrime is "the use of a computer as an instrument to further illegal ends, such as committing fraud, trafficking in child pornography and intellectual property, stealing identities, or violating privacy".[14]UNODC (United Nations Office on Drugs and Crime) even said that cybercrime is an “evolving form of transnational crime”. This is considered reasonable, because of the complexity and nature of the crime which is in the “borderless realm of cyberspace” which is exacerbated by the increasing involvement of organized criminal groups in committing cybercrime.[15]

Based on the various definitions, it illustrates how complex the scope of cybercrime is. Most cybercrime attacks are aimed at information about an individual, corporation, or even a government. In general, cybercrime can occur in several forms, such as:[16]

1. *Unauthorized Access*: It is a crime that occurs when someone enters or infiltrates a computer network system illegally, without permission or without the knowledge of the owner of the computer network system they are entering;

2. *Illegal Contents*: This is a crime committed by entering data or information into the internet about something that is incorrect, unethical and can be considered to be against the law or disturbing public order, for example the distribution of pornography;

---

[11]Soerjono Soekanto, Normative Legal Research, (Jakarta: Raja Grafindo Persada, 2009), p. 56

[12]Barda Nawawi Arief and Muladi, Bunga Rampai Hukum Pidana, (Bandung: Alumni, 2010), p. 31 At that time, several phenomena arose in the context of computer crime, such as: 1. Fraud by computer manipulation (fraud caused by manipulation by computers); 2. Computer espionage, software piracy, high technology theft (espionage through computers, software piracy, theft of advanced technology); 3. *Computer sabotage* (sabotage using computers); 4. Theft of service (theft of services); 5. Unauthorized access to differential privacy system (illegal access to differential privacy system)

[13]Amin Suhaemin and Muslih, “Characteristics of Cybercrime in Indonesia”, EduLaw: Journal of Islamic Law and Jurisprudence, Vol. 5 No. 2 (2023): 18

[14]See https://www.britannica.com/topic/cybercrime (accessed 19 May 2024)

[15]See https://www.unodc.org/romena/en/cybercrime.html (accessed 19 May 2024)

[16]Amin Suhaimin and Muslih, Op.Cit, p. 20-22

E-ISSN: 2988-3334
ISSN: 1907-3319
Vol. 20 No. 1 March 2025

3. Intentional virus spreading: Virus spreading is generally done using email. Often people whose email systems are infected with viruses are not aware of this. The virus is then sent to other places via their email;

4. *Data Forgery*: This type of crime is committed with the aim of falsifying data on important documents on the internet. These documents are usually owned by agencies or institutions that have web-based database sites.

5. Cyber Espionage, Sabotage and Extortion: Cyber Espionage is a crime that utilizes the internet network to conduct spy activities against other parties, by entering the target party's computer network system. Sabotage and Extortion are types of crimes committed by creating interference, damage or destruction of data, computer programs or computer network systems connected to the internet;

6. Cyberstalking: This type of crime is committed to disturb or harass someone by utilizing a computer, for example by using email, and is done repeatedly. This crime resembles terror directed at someone by utilizing the internet media. This can happen because of the ease of creating an email with a certain address without having to include your real identity;

7. Carding: is a crime committed to steal other people's credit card numbers and use them in internet trading transactions;

8. Hacking and Cracker: The term hacker usually refers to someone who has a great interest in learning the system in detail and how to improve its capabilities. Those who often carry out destructive actions on the internet are usually called crackers. It can be said that this cracker is actually a hacker who uses his abilities for negative things. Cracking activities on the internet have a very wide scope, ranging from hijacking other people's accounts, hijacking websites, spreading viruses, to paralyzing targets. The last action is called DoS (Denial of Service). DoS attack is an attack that aims to paralyze the target (hang, crash) so that it cannot provide services;

9. *Cybersquatting and Typosquatting*: Cybersquatting is a crime committed by registering a domain name of another person's company and then trying to sell it to the company at a higher price. Typosquatting is a crime by creating a fake domain, namely a domain that is similar to someone else's domain name. The name is the name of a rival company's domain;

10. *Hijacking*: is a crime of pirating the work of others. The most common is software piracy;

11. Cyber Terrorism: A cybercrime action including cyber terrorism if it threatens the government or citizens, including cracking into government or military sites. Some examples of cyber terrorism cases include:

a. Ramzi Yousef, the mastermind behind the first attack on the WTC buildings, was known to have stored details of the attack in encrypted files on his laptop;

b. Osama bin Laden was known to use steganography for his network communications.

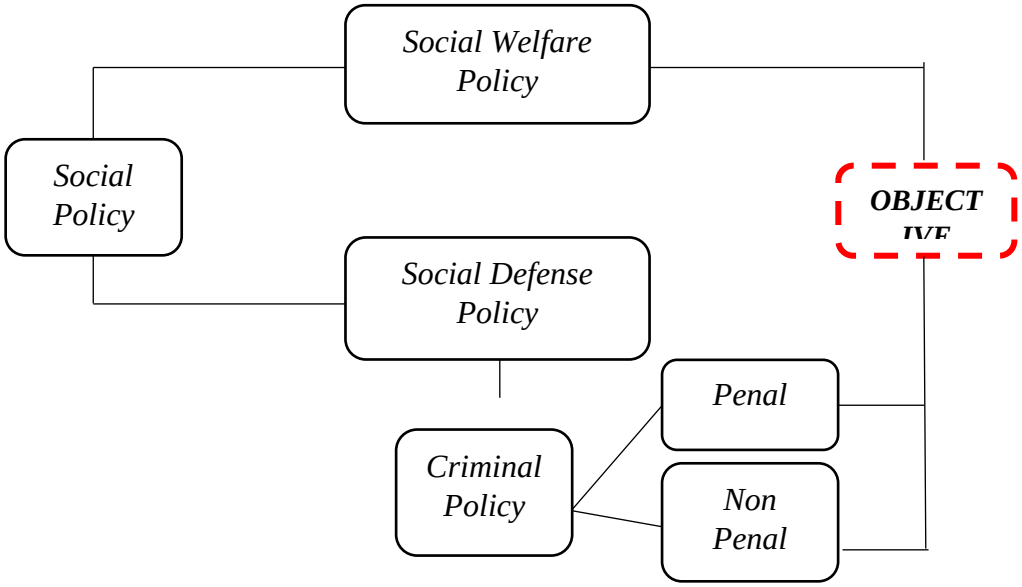
c. A website called the Muslim Hacker Club is known to list tips for hacking the Pentagon;

d. A hacker who calls himself Doctor Nuker is known to have been defacing or changing the contents of web pages with anti-American, anti-Israel and pro-bin Laden propaganda for approximately five years.

E-ISSN: 2988-3334
ISSN: 1907-3319
Vol. 20 No. 1 March 2025

3.2. Criminal Law Policy in the Framework of Strengthening Cyber Security Based on Pancasila

In order to overcome cybercrime with criminal law means, it cannot be separated from the discussion of criminal policy. According to Marc Ancel, the definition of criminal policy is a rational effort by society to overcome crime (the rational organization of the control of crime by society).[17]Criminal law policy and criminal policy essentially have a very close relationship, namely they are part of efforts to protect society (social defense), which if schematized would be as follows:[18]



Scheme 1: Criminal Policy

Based on the scheme, it can be said that criminal policy and criminal law policy cannot be separated, and are an integral part of social politics whose goals are both social welfare and social defense. According to Marc Ancel, modern criminal science consists of three components, namely criminology, criminal law, and penal policy.[19]Criminal law policy according to Marc Ancel is both a science and an art which ultimately has the practical aim of enabling positive legal regulations to be formulated better and to provide guidance not only to lawmakers, but also to courts that apply laws and also to organizers or implementers of court decisions.[20]

The definition of criminal law policy can basically be seen from the perspective of legal politics. According to Prof. Sudarto, what is meant by legal politics is:

1. Efforts to create good regulations in accordance with the circumstances and situations at a given time;

[17]Barda Nawawi Arief, Anthology – Criminal Law Policy, (Jakarta: Kencana Paramedia Group, 2014), p. 3
[18]Ibid, p. 5
[19]Ibid, p. 23
[20]Ibid

E-ISSN: 2988-3334
ISSN: 1907-3319
Vol. 20 No. 1 March 2025

2. The policy of the state through authorized bodies to establish the desired regulations which are thought to be able to be used to express what is contained in society and to achieve what is aspired to.[21]

So, starting from this idea, Sudarto then stated that implementing "criminal law policy" means holding elections to achieve the best criminal legislation results in the sense of fulfilling the requirements of justice and utility.[22]This crime certainly indirectly also hits the ideology of the Indonesian nation, namely Pancasila. For this reason, it is necessary to see how the correlation between criminal law policies or politics based on Pancasila in overcoming this problem. The embodiment of the values of Pancasila should be reflected in the various formulations in each regulation formed by the Government. This is also emphasized in Article 2 of Law No. 12 of 2011 as last amended by Law No. 13 of 2022 concerning the Formation of Legislation (UU PPP), that Pancasila is the source of all sources of state law. This also means that every material contained in state policy, including the 1945 Constitution, must not conflict with the values contained in Pancasila.[23]

The realization and implementation, especially in overcoming and preventing cybercrime, have resulted in the formation of several legal instruments for cybersecurity protection. According to Article 1 number 4 of Presidential Regulation No. 82 of 2022 concerning the Protection of Vital Information Infrastructure, Cybersecurity is "an adaptive and innovative effort to protect all layers of cyberspace, including the information assets contained therein, from cyber threats and attacks, both technical and social". In relation to the criminal law policy based on Pancasila, Indonesia itself has various related regulations which are a form of adaptive efforts by this country to protect its sovereignty against cybercrime. Several related laws and regulations, in order to strengthen cybersecurity, are:[24]

1. Law No. 44 of 2008 concerning Pornography (Pornography Law): In brief The regulation of pornography in this law includes (1) prohibition and restriction of the making, distribution, and use of pornography; (2) protection of children from the influence of pornography; and (3) prevention of the making, distribution, and use of pornography, including community participation in prevention. This law firmly stipulates the form of punishment for violations of the making, distribution, and use of pornography which is adjusted to the level of violation committed, namely serious, moderate, and light, and provides for aggravation of criminal acts involving children. In addition, it is given to perpetrators of criminal acts committed by corporations by multiplying the main sanctions and providing additional penalties;

2. Law No. 11 of 2008 as last amended by Law No. 1 of 2024 concerning Information and Electronic Transactions (ITE Law): although this law has caused various controversies, it cannot be denied that the main regulation regarding cybercrime protection is this Law. This can be seen that based on Article 40 paragraph (2) of the ITE Law, the Government guarantees

[21]Ibid, p. 26
[22]Ibid
[23]Pancasila Ideology Development Agency, Sigma Pancasila – Weaving Diversity Strengthening Indonesianness, (Jakarta: BPIP, 2020), p. 141
[24]Also compare with https://media.neliti.com/media/publications/43295-ID-perlindungan-hukum-terhadap-korban-kejahatan-cyber-crime-di-indonesia.pdf Dheny Wahyudi, "Legal Protection for Victims of Cybercrime in Indonesia", Journal of Legal Science No Year: 104 (accessed on May 21, 2024)

E-ISSN: 2988-3334
ISSN: 1907-3319
Vol. 20 No. 1 March 2025

to protect the public interest from all types of disturbances as a result of misuse of Electronic Information and Electronic Transactions that disrupt public order, in accordance with the provisions of the Laws and Regulations. In its first amendment, especially in the explanation of Article 45B, it also states that this Law provides legal protection up to entering the cyber world, especially regarding cyber bullying, which contains elements of threats of violence or intimidation and results in physical, psychological violence, and/or material losses;

3. Law No. 28 of 2014 concerning Copyright (Copyright Law); in this digital era, of course, software, films, animations, games in digital form are increasingly widespread. Of course, this is a loophole for some irresponsible people who have more ability to create or copy (crack) some of this content so that it can be enjoyed for free, without having to buy or have an official license from the developers or creators. This is certainly very detrimental to the developers or creators, because they do not get any profit from the results of their hard work. In overcoming cybercrime in this form, Indonesia already has a Copyright Law to protect and provide legal certainty to its citizens;

4. Law No. 23 of 2019 concerning Management of National Resources for National Defense (National Resource Management Law for National Defense): Article 4 of this Law states that National Resource Management for National Defense is prepared to face various military, non-military or hybrid threats, one of which can be in the form of cyber attacks. Also see in Article 20 cyber facilities and infrastructure are included in the category of Supporting Components;

5. Law No. 1 of 2023 concerning the Criminal Code (KUHP): for the time being, this National Criminal Code cannot be enforced, but its new values can be used as a reference in reviewing several criminal law issues. Several criminal acts related to cybercrime that were previously contained in special laws outside the Criminal Code, are now based on this Law included in one regulation but are embedded in the Special Criminal Acts Chapter, so as not to eliminate its lex specialis nature;

6. Government Regulation No. 71 of 2019 concerning the Implementation of Electronic Systems and Transactions: This PP guarantees that Public Electronic System Providers must have a plan for the continuity of activities to overcome disruptions or disasters in accordance with the risks of the impacts they cause. In addition, it also mandates the Government to protect the public interest from all types of disruptions as a result of misuse of Electronic Information and Electronic Transactions that disrupt public order;

7. Government Regulation No. 80 of 2019 concerning Trading Through Electronic Systems: based on Article 61 of this PP, Payment system service providers are required to comply with the security level standards of Electronic Systems in accordance with the provisions of laws and regulations that have been determined by the head of the government agency that organizes government affairs in the field of cybersecurity and state codes, the Governor of Bank Indonesia, and/or the Chairman of the Financial Services Authority;

8. Government Regulation No. 3 of 2021 concerning Implementing Regulations of Law Number 23 of 2019 concerning Management of National Resources for National Defense: Is the implementing regulation of the Law on Management of National Resources for National Defense;

E-ISSN: 2988-3334
ISSN: 1907-3319
Vol. 20 No. 1 March 2025

9. Presidential Regulation No. 82 of 2022 concerning the Protection of Vital Information Infrastructure: based on the provisions of Article 2 of this Presidential Regulation, the protection of IIV aims to: a. protect the continuity of the implementation of IIV in a safe, reliable, and trusted manner; b. prevent disruption, damage, and/or destruction of IIV due to cyber attacks, and/or other threats/vulnerabilities; and c. increase readiness in dealing with Cyber Incidents and accelerate recovery from the impact of Cyber Incidents;

10. Presidential Regulation No. 47 of 2023 concerning the National Cyber Security Strategy and Cyber Crisis Management: This Presidential Regulation is a reference for State Organizing Agencies and Stakeholders to realize cyber strength and capabilities in order to achieve Cyber Security stability. Article 4 states that the National Cyber Security Strategy and Cyber Crisis Management aims to: a. realize Cyber Security; b. protect the national digital economy ecosystem; c. increase reliable and resilient Cyber Security strength and capabilities; and d. prioritize national interests and support the creation of an open, safe, stable, and responsible global cyberspace.

11. Presidential Regulation No. 82 of 2023 concerning the Acceleration of Digital Transformation and Integration of National Digital Services: in short, one of the reasons this Presidential Regulation was formed is to realize quality and trusted public services, an integrated and comprehensive electronic-based government system and one Indonesian data, high-performance bureaucracy and public services, strengthening corruption prevention, and strengthening aspects of cybersecurity and information security, it is necessary to accelerate digital transformation. So based on this regulation, the President has given direct orders to strengthen aspects of cybersecurity in Indonesia.

In addition, if we look at how broad the spectrum of cybercrime is, it is reasonable to say that this crime can be categorized as an extra ordinary crime. The embodiment of the extra ordinary measure in responding to the problem of cybercrime, in Indonesia there are several institutions that handle this, namely:

1. National Cyber and Crypto Agency of the Republic of Indonesia (BSSN);[25]
2. State Intelligence Agency of the Republic of Indonesia (BIN);[26]
3. Ministry of Communication and Information of the Republic of Indonesia (Kominfo RI);[27]

[25]See Presidential Decree No. 28 of 2021 concerning the National Cyber and Crypto Agency in conjunction with BSSN Regulation No. 6 of 2021 concerning the Organization and Work Procedures of the National Cyber and Crypto Agency

[26]See Article 25 A in conjunction with 25 B of Presidential Decree No. 90 of 2012 as last amended by Presidential Decree No. 79 of 2020 concerning the State Intelligence Agency, that BIN has a Deputy for Cyber Intelligence (Deputy VI)

[27]See Article 80 of the Regulation of the Minister of Communication and Information No. 12 of 2021 concerning the Organization and Work Procedures of the Ministry of Communication and Information, although in terms of cybercrime in this regulation it is not specifically stated which Echelon I unit in the Ministry of Communication and Information will handle it. However, if you look at the phrase "... information security ..." in this article and several reports in the media, it can be concluded that it will be handled by the Directorate General of Informatics Applications

E-ISSN: 2988-3334
ISSN: 1907-3319
Vol. 20 No. 1 March 2025

4. Ministry of Defense of the Republic of Indonesia (Kemenhan);[28]
5. Indonesian National Army (TNI);[29]
6. The Republic of Indonesia National Police (Polri).[30]

Based on the analysis, it can be said that Indonesia has had various instruments, both in terms of preventive, preemptive, and repressive aspects. This is in line with Muladi's opinion, that to overcome these crimes, it is not only necessary to use a repressive approach or warmaking criminology or harm creating on crime which is hostile (adversarialism), but must also be combined with a preventive approach of mutualism or togetherness on the basis of peacemaking criminology.[31]

4. Conclusion

As a conclusion in this study, it can be concluded that cybercrime is a form of virtual crime by utilizing computer media connected to the internet, and exploiting other computers connected to the internet. Cybercrime is also an "evolving form of transnational crime". This is due to the complexity and nature of the crime which is in "the borderless realm of cyberspace" which is exacerbated by the increasing participation of organized criminal groups in committing cybercrime. So based on this, cybercrime can be classified as an extra ordinary crime.

Overall, both in terms of preventive, preemptive, and repressive aspects, Indonesia has it. If it is associated with criminal law policies based on Pancasila, all of these things can be said to be the embodiment of Pancasila values, both in terms of Divinity, just and civilized humanity, and social justice for all Indonesian people. Although it cannot be denied that there are still some shortcomings. The thing that needs to be considered is that during the implementation to strengthen cyber security, all related officials as previously stated must work together. This is because the 6 (six) Ministries/Institutions have overlapping duties, so they have the potential to overlap with each other, in addition, it is feared that there will be a dispute over authority in handling cybercrime.

5. References

Books:

Arief, Barda Nawawi and Muladi. (2010). Criminal Law Anthology. Bandung: Alumni

[28]See Article 44 of Presidential Decree No. 94 of 2022 concerning the Ministry of Defense, that the Ministry of Defense has a Defense Information and Communication Agency which has the task of implementing the management of strategic defense information and communication systems and cyber defense.

[29]See Article 54 of Presidential Decree No. 66 of 2019 concerning the Organizational Structure of the Indonesian National Army, stating that the TNI has a TNI Cyber Unit tasked with carrying out cyber operations within the TNI environment in order to support the TNI's main tasks. In addition, based on Article 90, it can be seen that the TNI also has an Army Cyber and Crypto Center tasked with providing guidance to TNI AD personnel regarding crypto and cyber functions in order to support the TNI AD's tasks.

[30]See the Circular Letter of the Chief of Police No: SE/2/11/2021 concerning Ethical Cultural Awareness to Realize a Clean, Healthy, and Productive Indonesian Digital Space. That basically there is no regulation found in any regulation that specifically states that it is necessary to form a "Cyber Police", the ITE Law only mandates that the investigation process in the context of ITE involves Investigators from the Police which is carried out based on the Criminal Procedure Code

[31]Muladi and Diah Sulistyani, Op.Cit

Arief, Barda Nawawi. (2014). Anthology - Criminal Law Policy. Jakarta: Kencana Paramedia Group

Muladi and Diah Sulistyani. (2016). Complexity of Development of Criminal Acts and Criminal Policy. Bandung: Alumni

National Cyber and Crypto Agency. (2023). Indonesian Cyber Security Landscape 2023. Jakarta: National Cyber and Crypto Agency

National Legal Development Agency. (2019). Final Report of the Working Group on Legal Analysis and Evaluation related to Strengthening Pancasila Ideology. Jakarta: Ministry of Law and Human Rights of the Republic of Indonesia

Pancasila Ideology Development Agency. (2020). Sigma Pancasila - Weaving Diversity Strengthening Indonesianness. Jakarta: Pancasila Ideology Development Agency

Pujiono. (2007). Collection of Criminal Law Writings. Bandung: Mandar Maju

Soekanto, Soerjono. (2009). Normative Legal Research. Jakarta: Raja Grafindo Persada

Journals:

Amin Suhaemin and Muslih, "Characteristics of Cybercrime in Indonesia", EduLaw: Journal of Islamic Law and Jurisprudence, Vol. 5 No. 2 (2023): 18

Dheny Wahyudi, "Legal Protection for Victims of Cybercrime in Indonesia", Journal of Legal Studies No Year: 104

Internet:

https://www.britannica.com/topic/cybercrime (accessed 19 May 2024)

https://www.unodc.org/romena/en/cybercrime.html (accessed 19 May 2024)

https://bpptik.kominfo.go.id/Publikasi/detail/jenis-jenis-serangan-siber-di-era-digital (accessed on May 22, 2024)

https://www.bbc.com/indonesia/indonesia-62870532 (accessed on 22 May 2024)

https://www.bbc.com/indonesia/articles/c51v25916zlo (accessed on 22 May 2024)

https://www.dpr.go.id/berita/detail/id/44937/t/BSI+Data+Leak%2C+OJK+Requested+to+Run+the+Function+of+Digitalization+Acceleration+of+All+Banks (accessed on May 22, 2024)

Legislation:

Government Regulation No. 3 of 2021 concerning Implementing Regulations of Law Number 23 of 2019 concerning Management of National Resources for National Defense

Government Regulation No. 71 of 2019 concerning the Implementation of Electronic Systems and Transactions

Government Regulation No. 80 of 2019 concerning Trading Through Electronic Systems

Law No. 1 of 2023 concerning the Criminal Code

Law No. 11 of 2008 as last amended by Law No. 1 of 2024 concerning Electronic Information and Transactions

Law No. 23 of 2019 concerning Management of National Resources for National Defense

Law no. 28 of 2014 concerning Copyright

E-ISSN: 2988-3334
ISSN: 1907-3319
Vol. 20 No. 1 March 2025

Law No. 44 of 2008 concerning Pornography

Presidential Regulation No. 47 of 2023 concerning National Cyber Security Strategy and Cyber Crisis Management

Presidential Regulation No. 82 of 2022 concerning the Protection of Vital Information Infrastructure

Presidential Regulation No. 82 of 2023 concerning the Acceleration of Digital Transformation and Integration of National Digital Services

The 1945 Constitution of the Republic of Indonesia