Indonesian Journal of Advanced Research (IJAR)
Vol. 3, No. 8, 2024: 1347 – 1368

Legislative Ratio of Strengthening State Cyber and Cryptography Agencies in Law Enforcement: A Perspective of Legal System Theory

Rd. Yudi Anton Rikmadani[1]*, Elly Sudarti[2], Hafrida[3], Sukamto Sutoto[4]
Universitas Jambi
Corresponding Author: Rd. Yudi Anton Rikmadani yudianton@gmail.com

A R T I C L E I N F O

Keywords: Legal System Theory, Cybercrime, Law Enforcement, BSSN

Received : 5, June
Revised : 25, July
Accepted: 28, August

A B S T R A C T

This research aims to address cyber threats and crimes in Indonesia. Currently, the responsibility for the implementation of cyber security tasks and functions is handled by the State Cyber and Cryptography Agency (BSSN). This situation makes it very difficult for BSSN to operate if its duties, functions, and authorities in cybercrime law enforcement are only regulated through a Presidential Regulation. This study uses a normative juridical method with a legislative approach that examines norms related to the authority of investigative institutions in law enforcement against cyber crimes. These findings highlight that there were 24.6 million cyberattacks recorded from January 1 to September 7, 2022, which caused losses to the community. The existence of BSSN was formed by the President through Presidential Regulation Number 28 of 2021 concerning the State Cyber and Cryptography Agency in carrying out its duties and authority to overcome cybercrime in the face of obstacles. This requires a comprehensive legal due diligence strategy that can be adjusted to legal compliance and potential legal problems of cybercrime. The results of the study show that to ensure security, justice, and legal certainty in the enforcement of cybercrime law can be carried out properly, it is necessary to have special laws and regulations that regulate cybercrime, with the existence of institutions that will implement laws and regulations in special law enforcement to deal with cybercrime, by containing legal compliance based on the applicable national legal system.

INTRODUCTION

The progress of science and technology has brought about complex consequences for human life and international relations. Concurrently, the internet has ushered in substantial transformations across nearly every aspect of human existence. Today, internet technology has become a widely used communication tool across various sectors of society, including scholars, researchers, entrepreneurs, government officials, artists, and the general public.

Since the mid-1990s, the internet has experienced continuous growth and has become an integral part of people's lives worldwide. Development of the Internet will also be felt in Western countries due to increasing industrialization and will eventually increase around the world. In today's global digital era, electronic transactions are inevitable. According to Raquel Ureña, says:

> *"The rise of virtual interaction through online platforms, including social networks like Facebook, Instagram, and Twitter, has significantly increased connectivity among individuals and organizations without prior real-world connections. These interconnected platforms offer diverse functionalities: popular social networks facilitate sharing photos and thoughts among friends and followers, while e-commerce platforms such as Amazon and eBay enable transactions. Moreover, crowd-sourcing platforms like Wikipedia, Slashdot, and Quora promote the sharing of knowledge and expertise, and online sharing platforms such as Uber and Blablacar cater to transportation needs, with Airbnb offering accommodation solutions. Despite the diversity among these online communities, they all share a common feature: a large number of users connected through virtual identities. These growing social media channels allow users to form various social connections, whether broad or specific, and use the network as a global platform for distributing and sharing products, services, information, opinions, and recommendations.*

According to Edmon Makarim, with the advancement of information and communication technology, global relations now transcend national borders and quickly produce significant changes in the social, economic, and cultural fields. This development also seems to have brought the emergence of new types of crime. In the digital world, humans commit various criminal acts that are impossible to happen in the real world. This crime involves using electronic information as a method to perpetrate it.

With the emergence of the Internet, traditional crimes such as extortion, theft, defamation, pornography, gambling, fraud, and even terrorism can now be conducted using online platforms. These different types of crimes can be executed online by individuals or groups, with a low risk of being caught and a greater impact of losses on society and the country. Information technology crime is a relatively new phenomenon when compared to other conventional crimes, appearing along with the information technology revolution.

Given Indonesia's membership in the United Nations and its integration with advanced communication and information technologies, it is no longer suitable for the Indonesian government and nation to adopt a policy of isolationism. An attitude that tends to be chauvinistic philosophy. On the other hand, the Indonesian government and the Indonesian nation do not need to "prostitute" the sovereignty and honor of their country as a civilized nation and

live in the uncertain ups and downs of international life. It is like life between day and night, sometimes interrupted by darkness.

In Indonesia, the government operates according to the legal principles outlined in Article 1, paragraph (3) of the 1945 Constitution. This signifies that the state must adhere to the established laws across all its institutions and facilities. As articulated in the preamble of the 1945 Constitution, Indonesia is a unitary state governed by law, tasked with securing a safe, peaceful, and prosperous life for its citizens, and actively contributing to global peacekeeping efforts. The government has the responsibility to safeguard the sovereignty and security of all its citizens, addressing threats whether they arise domestically or internationally.

Barda Nawawi Arief emphasized that cybercrime, a new facet of contemporary criminal activity, has garnered significant attention from the global community. He highlighted it as a detrimental consequence of technological progress, exerting a broad influence on present-day society. According to Mira Tayyiba, Secretary General of the Ministry of Communication and Information Technology, the primary hurdle confronting all stakeholders in the digital transformation journey is ensuring data security and protection in cyberspace.

In Indonesia's law enforcement system, government agencies possess the jurisdiction to address cybercrime, which encompasses:

1. As per Law Number 2 of 2002 regarding the Indonesian National Police, the Indonesian National Police is empowered to conduct investigations into criminal activities.
2. According to Law Number 1 of 2021, which amends Law Number 16 of 2004 regarding the Prosecutor's Office of the Republic of Indonesia, the Attorney General's Office of Indonesia is entrusted with both the duty and the authority to investigate certain criminal offenses.
3. By Law Number 35 of 2009 concerning Narcotics, the National Narcotics Agency (BNN) is tasked with the responsibility of investigating, prosecuting, and bringing to court cases concerning the misuse and unlawful distribution of narcotics.
4. As per Law Number 5 of 2008, which amends Law Number 15 of 2003 regarding Government Regulations replacing Law Number 1 of 2002 concerning the Eradication of Terrorism, the National Counter-Terrorism Agency (BNPT) is responsible for coordinating law enforcement activities aimed at combating terrorism.
5. According to the Communication and Informatics Regulation of the Republic of Indonesia Number 7 of 2016, the Minister of Communication and Information of Indonesia has the authority to oversee the administration of investigations and enforcement of criminal acts within the realm of information technology and electronic transactions.
6. As per Presidential Regulation Number 28 of 2021 concerning the State Cyber and Cryptography Agency (BSSN), this agency is mandated to implement cyber and cryptography security measures to support the government in fulfilling its duties.

In Indonesia, the law enforcement process involves several ministries, each with designated roles as stipulated by relevant laws governing their respective agencies. For example, law enforcement agencies conduct investigations and oversee criminal cases, prosecutors are responsible for prosecuting and investigating particular criminal offenses, courts deliver criminal verdicts, attorneys advocate for justice seekers, correctional facilities focus on inmate rehabilitation, and governmental investigative bodies carry out inquiries as part of their official responsibilities.

Therefore, all government agencies possess the authority to investigate, prevent, and enforce laws of cybercrime. This results in overlapping in law enforcement related to cybercrime. Therefore, there needs to be synchronization in terms of the authority to tackle cybercrime for state security.

The presence of this controversial law raises several issues, including First, when implemented, the law is not effectively applied to the community. Secondly, they face rejection from the community due to being perceived as not supportive of community interests. Third, it may fail to support efforts to create a favorable business and investment environment and may hinder national development. Moreover, importantly, this could pose a threat to the safeguarding of human rights.

To attain national goals of cyber security, protection, and sovereignty, and to bolster national economic growth, the government has established the BSSN. BSSN is a governmental body created by the President, as outlined in Presidential Regulation Number 28 of 2021 regarding the State Cyber and Cryptography Agency of the Republic of Indonesia. According to the considerations in the Presidential Regulation:

a. Reorganizing the organizational structure of the State Cyber and Cryptography Agency is essential to achieve national cybersecurity, protection, and sovereignty, and to enhance national economic growth.
b. To enhance effectiveness and efficiency in carrying out tasks and functions related to cybersecurity and cryptography, it is necessary to improve the organizational structure of the State Cyber and Cryptography Agency.

As a governmental institution entrusted with cyber security responsibilities, BSSN is anticipated to act as the primary coordinator for cyber security implementation in Indonesia. Broadly, BSSN employs three approaches to address cyber threats in the country, namely:

(1) BSSN prepares a framework for cyber security by designing related legal frameworks, formulating national cyber security strategies, and improving BSSN's efficiency and tasks.
(2) BSSN develops capabilities in cyber security by increasing public awareness campaigns related to cyber issues, designing programs in the fields of cyber-related education, research, and development, and improving training and certification programs in cyber security.
(3) BSSN increases cooperation in cyber security by conducting multilateral and bilateral collaborations with other countries related to cyber issues,

strengthening cooperation between the government and private sectors in the cyber sector, and improving internal coordination between government agencies.

According to information from the State Cyber and Cryptography Agency (BSSN), as of April 2022, there were around 100 million cases of cyber attacks in Indonesia. The most common types of attacks reported by BSSN are ransomware and malware. Furthermore, BSSN reported that from January 1 to September 7, 2022, there were more than 108 million cyber attacks targeting Indonesia, including:

1. Cyber attacks originating from within the country, reaching 21.2 million times;
2. Cyber attacks originating from India, reaching 16.8 million times;
3. Cyber attacks originating from the United States, reaching 12.5 million times;
4. Cyber attacks originating from Bangladesh, reaching 8.7 million times;
5. Cyber attacks originating from Russia reached 6.3 million times;
6. Cyber attacks originating from China reached 5.8 million times;
7. Cyber attacks originating from Vietnam reached 5.2 million times;
8. Cyber attacks originating in Brazil, reaching 2.3 million times; and
9. Bali has become the main destination for cyber attacks in Indonesia throughout this year. There were 24.6 million cyber attacks on the Island of the Gods from January 1 to September 7, 2022;
10. Jakarta is in second place with 23.82 million cyber-attacks; and
11. 18 million cyberattacks directed at Aceh.

This reality reflects the need for special handling related to cybercrime in law enforcement in Indonesia. The creation of a new institution like BSSN carried out directly by the president should have a significant impact, but the reality is the opposite. Cybercrime is on the rise. The law must be able to protect the rights of all parties while providing strict sanctions to the perpetrators of cybercrimes, to ensure smooth national development and protect the achievements that have been achieved and those that still need to be achieved.

This Presidential Regulation mandates the utilization of information technology across various sectors, including within the law enforcement process, to facilitate broader interaction among law enforcement agencies and enhance the dissemination of information regarding the progress of law enforcement efforts. Currently, the State Cyber and Cryptography Agency (BSSN) is responsible for carrying out tasks and functions related to cybersecurity. Although the position of BSSN is only regulated through a presidential decree and has more limited authority compared to state institutions established through law, special legal regulations are needed so that BSSN can function as a law enforcement agency, especially as a cyber security coordinator in Indonesia. This situation makes it very difficult for BSSN to operate if its duties, functions, and authorities are by the provisions of the Presidential Regulation.

Based on this background description, this study is expected to describe in detail the legal framework regarding the authority of institutions in handling cybercrime as part of law enforcement efforts in Indonesia. Thus, it is hoped that this research can be a guide for the optimal application of government agency authority in the future.

LITERATURE REVIEW

Lawrence M. Friedman described that law enforcement within the legal system is shaped by three main components: the structural framework, the substance or content of the laws, and the legal culture. These three elements are interconnected and form a complete legal system. According to Lawrence M. Friedman's Legal System Theory, a legal system comprises three primary components. Firstly, Legal Substance encompasses the body of substantive rules and guidelines concerning how institutions should conduct themselves. This legal substance refers to the legal norms that govern behavior in society. Secondly, Legal Structure is a fundamental and well-defined framework within the legal system. This framework delineates the foundational organization of the system, including the arrangement of its components and the regulatory entities operating within it. Thirdly, Legal Culture encompasses elements of broader culture, traditions, attitudes, perspectives, and behavioral norms that influence people's attitudes and adherence to the law. This legal culture influences how social forces direct or distance themselves from the law in a variety of contexts. Thus, this theory explains that the legal system consists not only of legal rules but also of the governing structures and cultures that influence the acceptance and application of law in society.

In an effective system, there should be no conflict between the parts of the system. In addition, there should be no duplication or overlap between existing elements. Each system has principles that guide its creation process. Bellfroid described the legal system as a structured collection of legal regulations governed by its principles. Meanwhile, Sudikno Mertokusumo characterized the legal system as a cohesive entity comprising interconnected parts or elements, such as rules or directives specifying required actions, thereby establishing it as a normative system.

Thus, a legal system is a set of legal regulations consisting of elements that interact with each other, arranged according to their principles, to achieve a certain result. Each part of the legal regulation must be seen in the context of its relation to the other parts and the system as a whole. No part stands alone without being related to the other but is interconnected with other parts. The legal system must be consistent so that the legal regulations do not conflict with each other.

METHODOLOGY

This study aims to explore and analyze the concept of institutional authority in enforcing laws against cyber crimes, and to assess the strengths and weaknesses of laws and regulations concerning legal certainty. This study employs a normative juridical method in legal research, focusing on statutory analysis to examine norms of the authority of investigative institutions in

combating cyber crimes. This method is expected to be an analytical tool to clarify the problems discussed in this study.

RESEARCH RESULT AND DISCUSSION

BSSN

1. *Background and development leading to the formation of the BSSN*

Since Indonesia gained independence, the responsibility for safeguarding sensitive government information has been entrusted to personnel of the Encryption Agency. It began in the technical division of Bureau B within the Ministry of Defense during the independence struggle, including when the government capital was in Yogyakarta, and continued during the Indonesian emergency government in Bukittinggi. They also support communications and diplomatic operations on the front lines of armed resistance, both for the Ministry of Defense and Indonesian representatives abroad such as New Delhi, The Hague, and New York.

On April 13, 2021, President Joko Widodo of Indonesia signed Presidential Regulation (Perpres) Number 28 of 2021 regarding the State Cyber and Cryptography Agency (BSSN). The issuance of this Presidential Regulation is carried out to tidy up the organizational structure of BSSN to achieve national cyber security, protect sovereignty, and encourage national economic growth. The objective of this Presidential Regulation is to enhance the effectiveness and efficiency of cyber security tasks and functions within the framework of BSSN.

With the establishment of BSSN, this institution will be responsible for all activities in the field of cryptography at the State Cryptography Institute, as well as manage all aspects of information security including the use of telecommunication networks and Internet Protocol-based security. BSSN will also take care of the provision of telecommunication networks and infrastructure for the Ministry of Communication and Information.

2. *Status or position of the BSSN*

The State Cryptography Agency, currently integrated within BSSN, was last governed by Presidential Decree Number 103 of 2001. This decree outlined its role as a non-ministerial government institution tasked with carrying out governmental functions related to cryptography by relevant laws and regulations.

Regarding the duties of BSSN or the State Cipher Agency, two types of tasks related to the institution can be identified, namely, operational tasks carried out by the institution itself, as well as coordination tasks with other institutions that are also responsible for cryptography and cyber security work. As a non-ministerial government agency, BSSN may face certain challenges, especially when it comes to coordinating with state agencies or judicial bodies that have similar mandates in the field of cyber security and cryptography. In its capacity, BSSN requires an independent organizational position, both in the implementation of operational tasks and in ensuring the fulfillment of assigned tasks.

3. *Duties and roles of the State Cyber and Cryptography Agency*

BSSN's responsibilities encompass executing governmental tasks in cybersecurity and cryptography to assist the President in governing. Meanwhile, BSSN's functions are delineated as follows:

a. Formulation and establishment of technical policies of cybersecurity and cryptography;
b. Execution of technical policies regarding cybersecurity and cryptography;
c. Establishment of norms, standards, procedures, and criteria in cryptography;
d. Execution of technical guidance and supervision in cryptography;
e. Coordination of duty implementation, training, and administrative support for all departments within BSSN;
f. Management of state-owned assets under BSSN's responsibility;
g. Provision of substantive support to all departments within BSSN; and
h. Oversight of duty implementation within BSSN

4. *Cyber Threats and Attacks*

1. Cyber Threats

A threat can be described as an effort or behavior originating from within or outside a country that has the potential to threaten national security, state sovereignty, or territorial integrity. This concept of threat encompasses dynamic and evolving elements. Initially, threats to state sovereignty were primarily conventional and physical. However, they have now evolved into multidimensional challenges that include both physical and non-physical threats originating from both domestic and international sources.

Cyber threats refer to situations within the digital realm that can lead to harm, disruption, loss, or instability in information and communication technology infrastructure, whether caused intentionally or unintentionally. Accidental cyber threats can occur such as accidental system damage due to software updates. Intentional cyber threats can be categorized into two types: targeted attacks, where a group or individual specifically aims at a particular cyber asset, and untargeted attacks, which occur without a specific purpose or happenstance. Based on the National Cyber Security Strategy Guide published by the ITU, cyber threats are classified based on their characteristics, the consequences they cause, their origin or source, and the identity of the attacker.

The Ministry of Defense of Indonesia, as outlined in the 2014 Cyber Defense Guidebook, mentioned as follows:

1.1 Threat Sources

Threats come from entities that have a real intention and willingness to violate legal norms and information security rules and take over physical assets to achieve profits, both materially and immaterial. These threats can come from parties representing the government (State Actors) or non-governments (Non-State Actors), which can be individuals, groups, organizations, or even countries. Broadly, potential sources of threat encompass:

a. Sources of internal and external threats.
b. Intelligence operations.
c. Espionage.
d. Surveillance.
e. Organized crime.
f. Hacktivism.
g. Organized criminal syndicates.
h. Rivalry, conflict, and hostility.
i. Technological factors.

1.2 Aspects of Threat Aspects

The aspect of threat encompasses all factors underlying the occurrence of cyber threats and attacks, including ideological, political, economic, social, cultural, national, military, scientific, and technological aspects, as well as other factors related to the existence of the nation, state, and society, including individual interests.

1.3 Types of Threat of Threat

Today, common cyber threats manifest in various situations or events such as:

1) Today, prevalent types of attacks include Advanced Persistent Threats, Denial of Service, and Distributed Denial of Service. These attacks are designed to exceed the system's capabilities, thereby obstructing legitimate users from accessing and utilizing the targeted system or its resources. Their objective is to disrupt system operations by inundating the target with access requests or processes that exceed its capacity. Consequently, the system becomes overwhelmed or may even crash, rendering it incapable of functioning normally. Such attacks present significant threats to organizations reliant on internet connectivity for operational continuity.
2) A defacement attack occurs when an attacker alters or replaces content on a victim's webpage to serve their objectives.
3) A phishing attack happens when an attacker creates a deceptive website that mimics a legitimate one. The objective of this phishing attack is to illicitly acquire critical and sensitive information such as usernames, passwords, and other personal data.
4) In a phishing attack, an attacker creates a fraudulent website that imitates a legitimate one to unlawfully obtain sensitive information such as usernames, passwords, and other personal data. The number of malware attacks continues to increase, and it is currently a significant global threat. Malware is widespread and affects various sectors of activity. The term "virus" is commonly used to refer to malicious computer programs that can multiply and spread to other systems.
5) Cyber penetration involves attempting to gain unauthorized access to a system by exploiting weaknesses such as identifying legitimate user credentials and connection parameters like passwords. Commonly used methods to achieve system access include:

(a) Guess. Passwords that are too simple, such as usernames, surnames, dates of birth, or other personal information are easy to guess.
(b) Unprotected accounts. The use of weak passwords or the habit of sharing passwords with others easily.
(c) Fraud and social engineering. Scammers claim to be administrators or other authorities for technical reasons to request sensitive information. This scam can be done via phone or electronic message.
(d) Monitor data communication traffic. The eavesdropper intercepts unencrypted data transmitted through a communication network using a sniffing device and analyzes the data to extract encrypted passwords.
(e) Trojan Horse. A malicious program that secretly installs itself to record and transmit information to a remote system, often by disguising itself as a legitimate application.
(f) Authentication system. Attempts to access files that store all encrypted user passwords, with the aim of opening or decrypting those passwords.
(g) Encrypted password cracking. The attack is by testing all possible permutations to crack the password. Known as a brute force attack or dictionary attack if it uses a list of common words to guess passwords.
(h) Collecting user connection details using software, spyware, or devices such as cameras and microphones to acquire sensitive information, including passwords.

6) Spam refers to the act of sending large volumes of unsolicited emails, typically with the intention of:
(a) Advertising or promotional;
(b) Introducing risks, such as implanting malicious software (malware, crimeware) into the system;
(c) In severe cases, spam can lead to email bomb attacks, causing overloaded email servers, full mailboxes, and operational challenges. Once viewed merely as a nuisance, spam emails have evolved into a genuine threat, serving as a primary vector for disseminating viruses, worms, trojans, spyware, and phishing attempts.

7) Fraudulent attacks on communication protocols, such as those using Transmission Control Protocol (TCP), exploit TCP's capability to establish a virtual connection between two systems for data exchange. A logical identifier is used to form a TCP connection. TCP port number fraud attacks include attempting to guess or predict the next port number to be used for data exchange, with the intent to take advantage of unauthorized port numbers. The goal is to bypass the firewall and establish a secure connection between the attacker and the target forma

5. *Cyber Attacks*
   Cyber attacks occur when heightened cyber threats manifest into actual activities or actions that involve entering, controlling, altering, stealing, damaging, destroying, or disabling systems or information assets.

6. *Types of Cyber Attacks and Threats*

According to BSSN, there are eight recognized threats, encompassing malicious activities, misuse, interception/eavesdropping, hijacking, disasters, accidental damage, outages, malfunctions, and legal and physical attacks.

Table 6.
Types of Cyber Threats and Attacks

Types of Threats	**Example of an Attack**
Nefarious activity, abuse	a. Manipulation of network configurations or falsification of data: - Manipulation of routing tables. - Destruction of CORE configuration data. - DNS tampering. - Manipulation of network access and radio technology configuration. - Exploitation of improperly configured systems or networks. - Registration of malicious network functions. - Deletion of security data (cryptographic keys, security policies, access settings, etc.). - Deletion of network implementation data. - Deletion of operating system services. b. Software and hardware vulnerability exploitation: - Exploitation of zero-day vulnerabilities. - Improper use of open application programming interfaces at the network edge. c. Prevention of service of service (DoS) - Distributed denial of service (DDoS). - Flooding of core network components. - Flooding of base stations. - Amplification attacks. - MAC layer attacks. - Radio network jamming. - Radio interface jamming devices. - Jamming of base station radio interfaces. - Overloading edge nodes. - Spikes in authentication traffic.
Nefarious activity, abuse	a) Remote access exploits

Types of Threats	Example of an Attack
	- Hijacking of intra-RAT mobility mechanisms. - Hijacking of RAT sessions. b) Malicious code or software - Injection attacks (SQL, XSS). - Rootkits. - Rogueware. - Worms and Trojans. - Botnets. - Ransomware. - Malicious network functions. - Malware attacks on network products. - Malware attacks on enterprise applications. c) Improper use of remote network access - Misuse of external remote services for network products (e.g., VPNs) d) Improper use of leaked information - Theft and/or leakage of network traffic. - Data theft and/or leakage from cloud computing. - Improper use of security data obtained from audit tools. - Misuse or compromise of security keys. - Unauthorized access to the user's data plane. - Unauthorized access to data signaling.
Nefarious activity, abuse	a) Improper use of authentication - Spikes in authentication traffic. - Improper use of user authentication/authorization data by unauthorized personnel. - Exploitation of application management function (AMF) authentication and key agreement procedures. - Misuse of account credentials. b) Abuse of legitimate interception functions. - Manipulation of hardware and software. - Manipulation of hardware equipment. - Manipulation of network resources. - Memory scraping. - Side-channel attacks. - Fake network access points. - Fake MEC gateways. - Exploitation of the UICC format. - EU compromise. - The EU's inadequate security capabilities.

Types of Threats	Example of an Attack
	- Software backdoor. c) Data breaches, leaks, thefts, and information manipulation - Interference in network product logs. - Misuse of writing permission - Misuse of file ownership. - Breach of customer data. - Theft of personal information. d) Unauthorized activity. - IMSI catching attacks. - Sideways movement. - Brute-force. - Port knocking.
Nefarious activity, abuse	a. Unauthorized activity/network disruption. - IMSI catching attacks. - Lateral movement. - Brute-force attacks. - Port knocking b. Forgery. - Identity/account/service compromise. - Identity theft. - Identity spoofing. - IP spoofing. - MAC spoofing c. Spectrum sensing. d. Compromised supply chains, service providers, and vendors. - Misuse of third-party personnel access to the Operator's facilities. - Sabotage of network product development tools. - Sabotage of network product configuration tools. - Sabotage of network product source code. - Manipulation of network product updates. e. Improper use of virtualization mechanisms. - Bypassing network virtualization. - Misuse of virtualized hosts. - Manipulation of virtual machines. - Threats targeting data centers. - Implantation of cloud container images. - Backdooring cloud container images. - Improper use of cloud computing resources. f. Threats related to signaling - Signal storms.

Types of Threats	Example of an Attack
	- Signaling fraud.
Eavesdropping/interception/hacking	1. Espionage over the state. 2. Espionage on corporations. 3. Traffic sniffing. 4. Manipulation of network traffic, network reconnaissance, and gathering of information: - Manipulation of radio network traffic. - Malicious redirection of network traffic. - Redirection of network traffic. - Improper use of roaming interconnections 5. Man in the middle. - Session hijacking using a rogue base station. - Downgrade attacks using a rogue base station. 6. Intercepting information - Intercepting data through small covert cells. - Air interface interception. - Tracking devices and identities using rogue base stations. - Listening in on unencrypted message content.
Natural disasters	a. Natural disasters. - Landslide. b. Environmental disasters. - Floods, storms. - Pollution, corruption, dust. - Fire, strong winds. - Unpredictable weather conditions.
Unintentional damage	a. Improperly configured system/network. b. Insufficient design and planning, or failure to adapt. - Obsolete systems or networks because of neglecting updates or patch management. - Mistakes resulting from inadequate configuration change management. - Subpar network design and system architecture Outdated systems or networks due to lack of updates or patch management. c. Improper utilization or management of networks, systems, and devices. d. Disclosure of information caused by human mistakes. e. Data loss from inadvertent deletion.
Outages	a. Depletion of resources of resources - Personnel resources.

Types of Threats	Example of an Attack
	- Material resources. b. Support services.
Failures/malfunctions	a. Failure of networks, devices, or systems b. Failure or interruption in the communication network. c. Power supply failure or interruption. d. Service provider (supply chain) failure or disruption. e. Equipment damage (device or system).
Legal/policy	a. Breaches of service level agreements (SLAs). b. Breaches of legislation or rules. c. Failure to meet contractual or regulatory obligations.
Physical attack	a. Deliberate damage to network infrastructure (such as radio access and edge servers). b. Destruction of network infrastructure (such as radio access and edge servers). c. Theft of physical assets. d. Acts of terrorism targeting network infrastructure. Fraud committed by operator personnel. e. Unauthorized physical access to base stations in shared locations.

Every threat that occurs/arises is the result of actions taken by threat actors. There are eight categories of threat actors, including cybercriminals, insiders, nation-states, cyber warriors, hacktivists, corporations, cyber terrorists, and script kiddies. As with the phenomenon of cyber attacks and threats, BSSN has a strategic goal to strengthen cyber resilience in the digital economy, improve public sector security, enforce the law in the cyber realm, develop a cyber security culture, and empower cyber security as a whole. Therefore, Indonesia's information security strategy is expected to be an important foothold in building global trust in Indonesia in international cyber security forums. Indonesia's Cyber Security Strategy is considered a positive contribution from Indonesia in encouraging the creation of world peace.

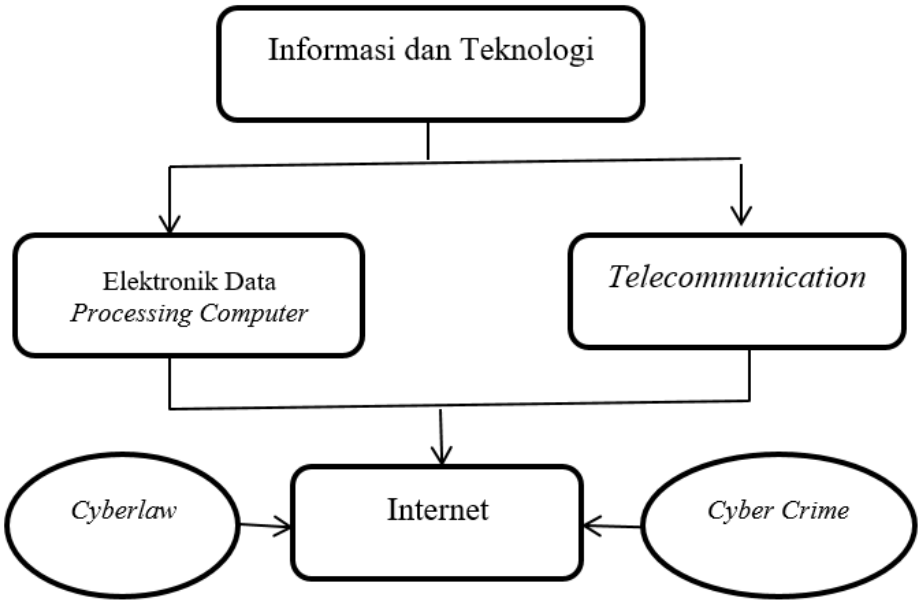
Thus, the ratio legal, or the main purpose of the regulation of the State Cyber and Cryptography Agency (BSSN) plays a role in enforcing laws related to criminal acts in the cyber realm to protect national interests from threats in cyberspace. This includes law enforcement efforts against cybercrime that can cause losses to the state and society, as well as ensuring that state security and sovereignty in the digital space are maintained.

1. Cybercrime

Cybercrime refers to criminal activities that utilize information and communication technology both as a means and as a target of the crime. It encompasses various types of offenses that breach the confidentiality, integrity, and availability of information.

Cybercrime is a form of crime committed by individuals, groups, or legal entities that utilize or target computers, computer systems, or computer networks. Its characteristics are different from conventional crimes because they occur in cyberspace or virtual.

Figure 1.
Characteristics of Information Technology Crime



The composition of the chart can be illustrated by interpreting and understanding the computer and telecommunication work systems that are connected to the internet and how cyber crime requires rules called cyber law.

2. Law enforcement

The implementation of cybercrime laws in Indonesia is influenced by five main factors: legislation, the perspectives of law enforcement officials, societal norms, institutional frameworks, and cultural dynamics. Laws cannot be effectively enforced in isolation; they always require community engagement and human action. Law enforcement agencies play a crucial role because laws alone cannot be enforced. Law enforcement officials must apply the law professionally and judiciously, while also interacting with individuals and groups suspected of criminal activities.

In instances of cybercrime, the perpetrators typically are individuals who possess advanced knowledge and skills in the field of computing. Writers usually have an advanced understanding and are experts in computer programming, and even writers can analyze the operation of systems on computers. This way they can trace loopholes in the existing system and then commit crimes.

According to A. Hamid S. Attamimi, as cited by Siswanto Sunarno, law enforcement involves the application of legal norms, whether they serve as commands or other functions such as empowerment, permission, or derogation. Siswanto Sunarno emphasized that in every country governed by substantive or social laws aimed at promoting the common good and enhancing the nation's quality of life, law enforcement regarding laws and regulations becomes an unavoidable necessity.

Andi Hamzah explained that in English, the term "law enforcement" is known as Law Enforcement, while in Dutch, it is referred to as law enforcement. This concept encompasses overseeing and implementing (or threatening to use) administrative, criminal, or civil measures to ensure compliance with relevant legal and regulatory provisions, both within society at large and concerning individuals. Supervision includes two stages in law enforcement, namely the repressive stage and the compliance stage aimed at prevention. Koesnadi Hardjasoemantri emphasized that law enforcement entails utilizing diverse methods and forms of penalties, which include administrative, civil, and criminal sanctions.

To address the requirements and complexities of global communication via cyberspace, it is presumed that constitutional laws and regulations should be in place. These laws and regulations should evolve with advancements to preempt issues arising from internet misuse, which may encompass diverse motives capable of causing harm to others, both financially and non-financially. For example, the impact can be in the form of losses in terms of property and intangible things.

Based on the discussion in this study subsection, the researcher will address these issues. This is inseparable from the research on the legislative ratio of strengthening the Cyber Agency and State Cryptography in the application of the law against cybercrime in Indonesia, especially in the context of criminal procedure law, this is generally discussed specifically regarding the future as the law that is aspired to in our country. Before explaining the ideal concept in the future, we will first describe how the legal system works in dealing with cyber threats and crimes in Indonesia.

Discussion based on legal system theory, as per Lawrence M. Friedman, suggests that the integrity of the legal system and the process of law enforcement can be analyzed through three fundamental components: legal structure, legal substance, and legal culture. To understand how law enforcement takes place, these elements need to be explained in detail. Firstly, "legal substance" pertains to the content or material of the law, encompassing the laws themselves, the judicial system, and political dimensions. Second, "legal structure" refers to the organization and drafting of laws in a legal system, including the process of making, implementing, and enforcing laws, and legal hierarchies from the lowest to the highest. Third, according to Lawrence, "legal culture" refers to the values, norms, and cultures that exist in society, which influence how law enforcement is conducted.

Weaknesses in the data security of the police digital system contribute to heightened crime risks and an uptick in crime incidents. In addition, the low level of integrity and accountability of law enforcement officials has created a negative reputation for Indonesia at the international level, which in turn reduces public trust in the country's legal system. This needs to be watched out because it can affect cooperation and different perceptions of various parties involved.

Regulation of the BSSN Number 5 of 2020 concerning the Strategic Plan of the BSSN for 2020-2024 stipulates the direction of policies, strategies, regulations, institutional structures, and funding frameworks based on the vision, mission, and objectives of the State Cyber and Cryptography Agency.

BSSN plays an important role in dealing with cybercrime by coordinating all relevant elements in law enforcement and cyber security. It includes detecting, monitoring, countermeasures, recovery, and evaluation of cyber incidents or attacks to ensure cyber security is carried out effectively.

However, the current existence of BSSN is not very effective in conducting cyber security, because there are still law enforcement problems, as follows:

1) Law enforcement agencies' unwillingness to collaborate
   In an integrated system, there is a concern that information managed by one law enforcement agency might be deleted or lost. Consequently, not all agencies are willing to collaborate and fully integrate digital systems into law enforcement efforts. This reluctance can be observed particularly in cases involving smuggling, drug trafficking, terrorism, money laundering, or criminal activities linked to national and international networks.
2) Ego department in law enforcement
   Some law enforcement agencies believe that the systems they build are better than others, and when digital systems are integrated into law enforcement, other agencies are not. It might infringe upon the authority of law enforcement agencies.

In addition, several legal provisions related to law enforcement, such as criminal law related to cybercrime and regulation of third-party applications used in law enforcement, must be constantly updated and adjusted to the advancement of information technology. Therefore, cybercrime is a type of crime that utilizes computer networks, the internet, cyber domains, and cyberspace. Of course, actors use computer technology and the Internet to compete and dominate each other, to disrupt, stop, or even alter the flow of communication and information, content, and other actions that can harm society. The formation of opinions on interests in the form of campaigns, propaganda, and agitation, as well as the formation of international opinions, is now also carried out through the internet.

Based on the above description, it is important in this dissertation research to answer the need for an institution or institution that specifically handles law enforcement issues related to cybercrime, which is in the form of an independent institution or under the authority of the President (executive) in Indonesia.

> *"Establishing an independent institution to oversee comprehensive government regulatory policies and objectives, facilitate coordinated policy implementation, and promote regulatory excellence".*

The intent behind creating specific legislation on cybercrime is to instill fear in offenders and provide guidelines on the admissibility of evidence. With this law regulating cybercrime, law enforcement officials will have an easier time carrying out their law enforcement duties.

Thus, the Ratio of the BSSN Presidential Regulation to strengthen it into law can include several main objectives that lead to protection, regulation, law enforcement, and national cyber security capacity building, as follows:

1. The strengthening of regulations can be used to expand BSSN's authority in responding to, preventing, acting on, and handling increasingly complex cyber security threats. This includes more detailed arrangements related to BSSN's duties in supporting law enforcement against cyber crimes.
2. The strengthening of regulations can establish the organizational structure of BSSN in more detail, including the formation of special divisions or units tasked with detecting, analyzing, and responding to cybersecurity incidents.
3. The strengthening of regulations can give BSSN clearer authority and mandate in cooperation with other institutions, both domestically and at the international level, to increase collaboration in countering cybercrime.
4. The strengthening of regulations can regulate the standards for the protection of personal data and sensitive information managed by BSSN, as well as security procedures to avoid data breaches and cyber-attacks.
5. The strengthening of BSSN regulations can be given a mandate to develop and implement systematic education and training programs for workers involved in cybersecurity, both in the public and private sectors.
6. The strengthening of regulations can regulate the use of advanced technology and innovation in improving BSSN's ability to detect and respond to cyber security threats more effectively.
7. The strengthening of regulations can establish the obligation to conduct periodic cyber security audits and evaluate the performance of BSSN in carrying out its duties.

Departing from the above thoughts to the position of the BSSN in law enforcement of cyber crimes, it is necessary to strengthen and organize the Presidential Regulation into law, this allows the government to provide a more solid legal basis so that BSSN can effectively carry out its duties and missions in facing increasingly complex and rapidly developing cyber security challenges. It will also improve coordination between BSSN and other law enforcement agencies and strengthen national capacity in tackling cybercrime.

CONCLUSIONS AND RECOMMENDATIONS

The purpose of BSSN's existence is to safeguard Indonesia's national interests by addressing threats in cyberspace, which includes enforcing laws against cybercrimes that pose risks to the state and society, ensuring state security, and maintaining sovereignty. The objective of the Indonesian state, as outlined in the preamble of the 1945 Constitution, is to safeguard the entirety of the Indonesian nation and its people, enhance public welfare, promote national

intellectual advancement, and contribute to global peace and social justice based on independence and enduring peace.

Enforcing the law against cybercrime is a critical and pressing concern in the everyday lives of Indonesians. The current position of BSSN is only regulated through a presidential decree, so its authority is more limited compared to state institutions established based on law. Therefore, special legal regulations are needed for BSSN to be able to carry out its duties and functions as a coordinator, especially in law enforcement against cybercrime, as well as cybercrime law enforcement institutions in general in Indonesia.

To ensure effective implementation of security, justice, and legal certainty in cyber law enforcement, it is essential to enhance and fortify the role of the State Cyber and Cryptography Agency within the constitutional framework. Currently, BSSN only has limited authority and is regulated through the Presidential Regulation of the Republic of Indonesia Number 28 of 2021. In the future, the position of BSSN should be regulated through law. Regulating BSSN through legislation will allow BSSN to have special authority in law enforcement against cybercrime, which can coordinate with other institutions that also have relevant authorities regulated by law, by utilizing the principle.

ADVANCED RESEARCH

Every research certainly has limitations. Limitations in the sense of research limitations that affect the researcher's ability to explore the data being studied, limitations of available data, or external factors of research such as limited time and resources. So further research is needed for the perfection of this research.

REFERENCES

Book

Andi Hamzah, Environmental Law Enforcement, Sinar Grafika, Jakarta, 2005.

Doni Budiono, Ratio Legis Dispute Resolution of the Tax Amnesty Law in Tax Courts in Indonesia, *Disertasi* Doctoral Program in Law, Faculty of Law, University August 17, 1945, 2020.

Edmon Makarim, Telematics Law Compilation, Radja Grafindo Persada, Jakarta, 2003.

Friedman, L. M. *The Legal System: A Social Science Perspective*. Russell Sage Foundation, 1975.

Koesnadi Hardjasoemantri, Environmental Law, Gadjah Mada University Press, Yogyakarta, 2006.

Lawrence M. Friedman, *The Legal System A Social Science Perspektive*, Russell Sage Foundation, New York, 1975.

Man Suparman Sastrawidjaja, *Perjanjian* Standard in Cyber Activities, Cyberlaw: An Introduction, Cetakan I, Elips, Jakarta, 2002.

OECD, *Reviews of Regulatory Reform; Indonesia 2012*, *Strengthening Co-ordination and Connecting Market, OECD Publishing*, 2012.

Philemon Ginting, Information Technology Crime Countermeasures Policy Through Criminal Law, Thesis, Master of Law Program, Dipenogoro University Semarang, 2008.

Raquel Ureña, (et al), *A review on trust propagation and opinion dynamics in social networks and group decision-making frameworks, Information Sciences journal, Francisco*, 2019.

Rd. Yudi Anton Rikmadani, Telematics Law, Basics of Civil Aspects and Criminal Aspects, Mujahid, Bandung, 2018.

Rowe, N. C., *Honeypot deception tactics. Autonomous Cyber Deception: Reasoning, Adaptive Planning, and Evaluation of HoneyThings*, 2019.

Siswanto Sunarno, Local Government Laws in Indonesia, Sinar Grafika, Jakarta, 2008.

Sudikno Mertokusumo, *Mengenal Hukum: Suatu Pengantar*, Liberty, Yogyakarta, 2003.

Sugeng Sudarso, Integration of Digital Systems in Law Enforcement to Support Public Security and Order, Individual Scientific Paper (TASKAP) Regular Education Program (PPRA) L XV, Lemhannas RI, 2023.

Teguh Prasetyo dan Arie Purnomosidi, Building Laws Based on Pancasila, Nusa Media, Bandung, 2016.

Academic Manuscript Preparation Team, NA Amendment to LAW No. 15/2003, National Legal Development Agency, 2011.

Journal

Ahmad Budiman, Optimizing the Role of the National Cyber and Cryptography Agency, Brief Magazine, Vol. IX, No. 12/II/Puslit/June/2017, Research Center of the Expertise Agency of the House of Representatives of the Republic of Indonesia, www.puslit.dpr.go.id, ISSN 2088-2351.

Damar Apri Sudarmadi, The Strategy of the State Cyber and Cryptography Agency (BSSN) in Facing Cyber Threats in Indonesia, Journal of National Resilience Strategic Studies, Jurnal Kajian Stratejik Ketahanan Nasional Volume 2 Issue 2 JKSKN Volume 2 No 2 2019.

Dwi Rezki Sri Astarini dan Muhammad Syaroni Rofii, *Siber Intelijen Untuk Keamanan Nasional*, Jurnal Renaissance | Volume 6 No. 01 | Mei 2021.

Ikka Puspitasari, Criminal Liability of Perpetrators of Online Fraud in Positive Law in Indonesia, HUMANI (Hukum dan Masyarakat Madani), Volume 8 No. 1 Mei 2018.

Jurnalis J. Hius, Jummaidi Saputra, Anhar Nasution, Recognize and anticipate cybercrime activities in daily online activities in education, government and industry and applicable legal aspects, Prosiding Snikom 2014. Banda Aceh, 24 Mei 2014.

Secsio Jimec Nainggolan, Edi Yunara Syafruddin Kalo dan Mahmud Mulyadi, Juridical Analysis of the Position of Perpetrator Witnesses as Justice Collaborators in Narcotics Crimes at the Pematang Siantar District Court, USU Law Journal, Vol.5.No.3, Oktober 2017.

Sudarmadi, D. A., & Runturambi, A. J., Strategy of the State Cyber and Cryptography Agency (BSSN) in Dealing with Cyber Threats in Indonesia, *Jurnal Kajian Stratejik Ketahanan Nasional, Vol. 2 No. 2*, 157-178, 2019.

Legislation

Undang-Undang Dasar 1945.

Kitab Undang-Undang Hukum Pidana (KUHP).

Undang-Undang Republik Indonesia Nomor 1 Tahun 2024 Tentang Perubahan Kedua Atas Undang-Undang Nomor 8 Tahun 2011 Tentang Informasi dan Transaksi Elektronik.

Peraturan Presiden Republik Indonesia Nomor 28 Tahun 2021 Tentang Badan Siber Dan Sandi Negara.

Kementerian Pertahanan Republik Indonesia, *Peraturan Menteri Pertahanan Republik Indonesia Nomor 82 Tahun 2014, Tentang Pedoman Pertahanan Siber*, 2014, halaman 6.

Website

DTI-CX 2023, Cybersecurity and Data Protection Play a Critical Part in Speeding Up Digital Transformation, https://digitaltransformation.co.id/expo/**,** accessed on January 16, 2023, at 09.00 WIB.

Ericha Andrea, Joint Anticipation to Improve Systems and Prevent Cyber Attacks Ministry of Communication and Information of the Republic of Indonesia Directorate General of Informatics Applications, https://aptika.kominfo.go.id/2022/09/antisipasi-bersama-tingkatkan-sistem-dan-cegah-serangan-siber/#:~:text=Badan%20Siber%20dan%20Sandi%20Negara,oleh%20serangan%20ransomware%20dan%20malware accessed on January 17, 2023, at 19.45 WIB.

John Herhalt, *Cybercrime – a growing challenge for governments*, KPMG INTERNATIONAL, July 2011, Volume Eight, https://corporatefinance.kpmg.us/content/dam/institutes/en/government/pdfs/2011/cyber-crime-growing-challenge.pdf accessed on January 17, 2023, at 10.00 WIB.

Article 1 paragraph (3) of the 1945 Constitution, reads: The State of Indonesia is a state of law. https://www.dpr.go.id/jdih/Undang-Undang1945, accessed on January 15, 2023, at 14.00 WIB.

Sarnita Sadya, *Sources of Cyber Attacks on Indonesia (1 Januari 2022 - 7 September 2022)*, https://dataindonesia.id/digital/detail/dari-mana-sumber-serangan-siber-ke-indonesia, accessed on January 17, 2023, at 20.15 WIB.

Legal Systems in the World, http://iisaprianti12.blogspot.com/2016/01/sistem-hukum-di-dunia.html?m=1 accessed on March 20, 2023, at 21.15 WIB.

About BSSN,https://www.bssn.go.id/tentang-bssn/, accessed on March 24, 2024, at 19.35 WIB.

Wikipedia, *Sejarah Internet*, https://id.wikipedia.org/wiki/Sejarah_Internet accessed on January 17, 2023, at 09.15 WIB.