RLJ Ratio Legis Journal
ISSN 2830-4624
published by
Master of Law, Faculty of Law
Universitas Islam Sultan Agung
Volume 4 No. 4, December 2025

The Role of The State Intelligence Agency in Combating Cyber Crime Based on Legal Certainty

Ade Wardana [1)] & **Andri Winjaya Laksana** [2)]

[1)]Faculty of Law, Universitas Islam Sultan Agung (UNISSULA), Semarang, Indonesia, E-mail: adewardana.std@unissula.ac.id

[2)]Faculty of Law, Universitas Islam Sultan Agung (UNISSULA), Semarang, Indonesia, E-mail: andri.w@unissula.ac.id

Abstract. *The development of information technology has significantly impacted national security, particularly through the increasing complexity and transnational nature of cybercrime threats. This study aims to analyze the role of the State Intelligence Agency (BIN) in combating cybercrime, identify the weaknesses encountered, and formulate BIN's role based on the principle of legal certainty. The research employs a normative legal method with a qualitative approach through literature review. The findings reveal that BIN holds a strategic role in early detection and prevention of cyber threats, as mandated by the attribution of authority in Law Number 17 of 2011 concerning State Intelligence. However, the implementation of this role faces several weaknesses, including overlapping authority with other agencies, the absence of specific regulations, weak inter-agency coordination, insufficient human resources with cyber expertise, and limited technological capabilities. To ensure legal certainty, it is necessary to strengthen regulations that clearly define BIN's authority, establish coordination mechanisms among institutions, and apply the principles of legality, proportionality, and accountability. Reformulating BIN's role based on legal certainty is expected to enhance the effectiveness of cybercrime mitigation while safeguarding human rights in the digital era.*

Keywords: *Authority; Cybercrime; Legal Certainty; National Security; State Intelligence Agency.*

1. Introduction

The development of information and communication technology in the digital era has had a significant impact on the lives of Indonesians. On the one hand, technological advances have made various aspects of life easier, but on the other hand, they have created new challenges in the form of increasingly complex and widespread cybercrime threats.[1]According to data from the National Cyber and Crypto Agency (BSSN), Indonesia experienced an increase in cyberattacks, reaching 1.6 billion attacks in 2021, a 300% increase from the previous year.[2]

Cybercrime not only threatens individual security but also economic, political, and national stability. Various forms of cybercrime, such as hacking of government systems, personal data theft, online fraud, cyberterrorism, and attacks on critical national infrastructure, require comprehensive and coordinated action.[3]The complexity of cyber threats, which are transnational, anonymous, and difficult to track, requires a special approach involving various state security institutions.

The State Intelligence Agency (BIN), as Indonesia's main intelligence agency, has a strategic role in dealing with cyber threats.[4]Based onArticle 26Law No. 17 of 2011 concerning State Intelligence authorizes BIN to conduct early detection, prevention, and response to threats to national security, including cyber threats. However, in practice, BIN's role in combating cybercrime still faces various obstacles and limitations.

The main problem faced is the overlapping authority between BIN and other law enforcement agencies such as the National Police, the Prosecutor's Office, and other cyber agencies.[5]This creates legal uncertainty in handling cybercrime cases. Furthermore, the limited regulations specifically governing BIN's role in the cyber domain have resulted in suboptimal coordination between agencies.[6]

The aspect of legal certainty is very important in this context because it is related to the legitimacy of BIN's actions, protection of human rights, and the

[1]Barda Nawawi Arief, Cybercrime and Cyberlaw, (Semarang: Pustaka Magister, 2015), p. 23.
[2]National Cyber and Crypto Agency. 2021 Annual Cyber Security Monitoring Report. (Jakarta: BSSN, 2022), p. x
[3]Widodo Muktiyo, "The Development of Cybercrime and Challenges to Law Enforcement", Jurnal Daulat Hukum, Vol. 5, No. 2, (2022), p. 189.
[4]M. Yusuf Samad & Pratama Dahlian Persadha, “Understanding Russian Cyber Warfare and the Role of the State Intelligence Agency in Countering Cyber Threats”, Journal of Science and Technology and Communication (IPTEKKOM), BPSDMP Kominfo Yogyakarta, (2022), p. 136
[5]Hikmahanto Juwana, "Inter-Agency Coordination in Combating Cybercrime", Law Development Journal, Vol. 4, No. 3, (2023), p. 234.
[6]Romli Atmasasmita, Contemporary Criminal Justice System, (Jakarta: Kencana, 2020), p. 178.

effectiveness of law enforcement.[7] Gustav Radbruch, through his theory, emphasizes that legal certainty is one of the fundamental objectives of law, alongside justice and utility.[8]In the context of combating cybercrime, legal certainty is needed to provide a clear basis for BIN in carrying out its duties and functions.

This research is relevant considering that Indonesia is facing a significant escalation in cyber threats. Cyberattacks on vital infrastructure such as banking, telecommunications, and government systems demonstrate the urgency of strengthening national capacity to combat cybercrime.[9]BIN, as the vanguard of the national intelligence system, is required to be able to adapt to the dynamic development of cyber threats.

Furthermore, this research is also motivated by the gap between technological developments and existing regulations. Many laws and regulations have not yet accommodated the latest technological developments, creating a legal vacuum in handling cybercrime.[10] This condition has the potential to hamper the effectiveness of BIN's role in carrying out cyber intelligence tasks.

From an academic perspective, research on the role of the State Intelligence Agency (BIN) in combating cybercrime based on legal certainty remains limited. Most existing studies focus on general technical or institutional aspects, but have not yet examined in-depth the legal certainty aspect as the foundation of BIN's role in the cyber domain.[11]Therefore, this research is expected to provide a significant academic contribution to the development of legal science, particularly in the field of cyber law and intelligence.

Based on this background, this study will examine the role of BIN in combating cybercrime from the perspective of legal certainty, identify existing weaknesses, and formulate an ideal concept of BIN's role based on legal certainty to face the challenges of cybercrime in the future.

2. Research Methods

This research uses a normative legal research method with a qualitative approach.[12]Normative legal research is research conducted by examining library

[7]Satjipto Rahardjo, Legal Science, Revised Edition, 8th Edition, (Bandung: Citra Aditya Bakti, 2019), p. 89.
[8]Gustav Radbruch, Rechtsphilosophie, 8. Auflage, (Stuttgart: Koehler Verlag, 1973), p. 169.
[9]Mahrus Ali, Corporate Crime: A Study of the Relevance of Sanctions for Combating Corporate Crime, (Yogyakarta: Arti Bumi Intaran, 2018), p. 134.
[10]Andi Hamzah, Criminal Aspects in the Computer Sector, (Jakarta: Sinar Grafika, 2017), p. 67.
[11]Teguh Prasetyo, "Legal Analysis of BIN's Role in Countering Cyber Threats", Jurnal Daulat Hukum, Vol. 6, No. 1, (2023), p. 78.
[12]Peter Mahmud Marzuki, Legal Research, Revised Edition, (Jakarta: Kencana, 2019), p. 35.

materials or secondary data as basic material for research by conducting searches of regulations and literature related to the problem being researched.[13]

The characteristics of normative legal research in this study include: first, examining law conceptualized as norms or rules that apply in society; second, focusing on the inventory of positive law, legal principles and doctrines, legal discovery in cases in concreto, legal systematics, the level of legal synchronization, and legal comparison; and third, using literature studies as a way to obtain research data.[14]

3. Results and Discussion

3.1. The Role of the State Intelligence Agency (BIN) in Combating Cybercrime Today

a. Analysis of the Role of BIN Based on Lawrence M. Friedman's Legal System Theory

In analyzing the role of the State Intelligence Agency (BIN) in combating cybercrime, the author uses the legal system theoretical framework proposed by Lawrence M. Friedman. According to Friedman, a legal system consists of three main components: legal structure, legal substance, and legal culture. These three components interact with each other and influence the effectiveness of legal implementation within a system.

1) Legal Structure in the Role of BIN

From a legal perspective, the role of the State Intelligence Agency (BIN) in combating cybercrime has a clear institutional basis through Law Number 17 of 2011 concerning State Intelligence. BIN's institutional structure as a state intelligence agency provides legitimacy to carry out investigative, security, and mobilization functions within the context of national security, including the cyber domain. However, the existing legal structure still faces challenges in terms of the clarity of the division of authority with other institutions. The inter-agency coordination structure, which includes BIN, the National Cyber and Crypto Agency (BSSN), the Indonesian National Police (Polri), and the Indonesian National Armed Forces (TNI), lacks a clear hierarchy for handling cyber incidents. This creates the potential for overlapping authority and institutional conflict in operational implementation.

BIN's internal organizational structure has also undergone adaptations to address cyber challenges. The establishment of a cyber intelligence analysis

[13]Soerjono Soekanto and Sri Mamudji, Normative Legal Research: A Brief Review, Tenth Edition, (Jakarta: Raja Grafindo Persada, 2018), p. 13.
[14]Peter Mahmud Marzuki, Introduction to Legal Science, Revised Edition, (Jakarta: Kencana, 2019), p. 35

center and specialized units to address cyber threats represents a structural evolution within BIN. However, this structure is still being refined to achieve optimal effectiveness in addressing the ever-evolving dynamics of cyber threats.

2) Legal Substance Regulating the Role of BIN

The legal substance governing BIN's role in the cyber domain stems from various laws and regulations. Article 5 of the State Intelligence Law mandates BIN to conduct intelligence activities in the interests of national security. Article 26 of the same law authorizes it to conduct early detection of national security threats, which in contemporary interpretations includes cyber threats.

Government Regulation No. 4 of 2015 concerning the Implementation of the State Intelligence System provides a more specific operational framework for BIN's coordination with other institutions in identifying and anticipating national security threats. This regulatory framework serves as the basis for BIN's involvement in the national cybersecurity ecosystem.

However, existing legal substance does not explicitly and in detail regulate the technical aspects of BIN's operations in the cyber domain. Unclear definitions of cyber threats, cyber incident handling procedures, and operational authority limitations constitute substantial weaknesses in the legal framework governing BIN's role.

b. BIN's Operational Functions from the Perspective of Authority Theory

An analysis of BIN's role in combating cybercrime also needs to be viewed from the perspective of authority theory. According to HD van Wijk/Willem Konijnenbelt, authority can be obtained through three mechanisms: attribution, delegation, and mandate. BIN's authority in the cyber domain is a combination of these three mechanisms.

1) BIN Attribution Authority

BIN's attribution authority stems directly from Law Number 17 of 2011 concerning State Intelligence. Article 5 of this law grants BIN attribution authority to conduct intelligence activities including investigation, security, and mobilization. In the cyber context, this attribution authority legitimizes BIN's ability to conduct cyber intelligence activities in the interests of national security.

BIN's attributive authority also includes early detection functions, as stipulated in Article 26 of the State Intelligence Law. This authority provides the legal basis for BIN to monitor and analyze cyber threats that could endanger national security and interests.

However, the scope of BIN's attributable authority in the cyber domain still requires more detailed clarification. Unclear boundaries of attributable authority could lead to potential abuse or overlap with the authority of other institutions.

2) Delegated Authority in BIN Operations

Delegated authority within the context of BIN's role can be seen in the delegation of certain authorities from BIN leadership to subordinate operational units. This delegation of authority is necessary to ensure operational effectiveness and efficiency in addressing cyber threats that require a rapid response.

Government Regulation No. 4 of 2015 provides a framework for the delegation of authority within the state intelligence system. This delegation of authority covers aspects of coordination with other institutions and operational implementation at the technical level.

However, the mechanism for delegation of authority within BIN must adhere to the principles of accountability and oversight. Delegation of authority without adequate control mechanisms can pose a risk of abuse of authority or actions that exceed the limits of the authority granted.

c. Operational Implementation of BIN's Role

1) Cyber Threat Early Detection System

The State Intelligence Agency (BIN) has implemented an early detection system for cyber threats by developing integrated monitoring and analysis capabilities. This system uses advanced technologies, including artificial intelligence and machine learning, to identify cyber threat patterns that could endanger national security.

The implementation of this early detection system involves collecting and analyzing data from various sources, including international signals intelligence, internet traffic analysis, and monitoring of national critical infrastructure. This proactive approach allows BIN to identify threats before they develop into actual attacks.

However, the effectiveness of early detection systems still faces limitations in terms of data quality, analytical capacity, and coordination with external information sources. Improving technical capabilities and human resources is key to optimizing early detection systems.

2) Cyber Intelligence Capabilities

BIN is developing comprehensive cyber intelligence capabilities that encompass the collection, processing, and analysis of information related to cyber threats.

These capabilities include cyber threat intelligence focused on identifying threat actors, analyzing their mechanisms of action, and mapping attack vectors.

BIN's cyber intelligence activities also include cyber geopolitical analysis, which examines the implications of cyberattacks on national political and economic stability. This multidisciplinary approach integrates technical aspects of cybersecurity with strategic analysis to produce actionable intelligence.

Developing cyber intelligence capabilities requires continuous investment in technology, human resources, and analytical methodologies. BIN must continuously adapt its capabilities in line with technological developments and the evolution of cyber threats.

d. BIN's Role in Critical Infrastructure Protection

1) Infrastructure Vulnerability Assessment

The State Intelligence Agency (BIN) conducted a vulnerability assessment of the nation's critical information infrastructure as part of its role in combating cybercrime. This assessment included identifying vulnerable points, analyzing risks, and evaluating the level of threat to vital sectors.

Vulnerability assessments were conducted for the banking, telecommunications, energy, transportation, and other critical sectors that rely heavily on information systems and technology. BIN coordinated with infrastructure managers to conduct comprehensive assessments.

The results of the vulnerability assessment form the basis for developing risk protection and mitigation strategies. BIN provides recommendations to infrastructure managers regarding the security measures to be implemented.

2) Development of Security Standards

BIN is involved in developing cybersecurity standards for national critical infrastructure. This involvement includes contributing to the development of guidelines, technical standards, and security procedures applicable to various sectors.

Security standards development is carried out through a collaborative approach involving stakeholders from the government, private sector, and academia. BIN contributes to threat intelligence and security risk analysis.

Implementing security standards requires outreach, training, and compliance monitoring. BIN plays a role in ensuring that the developed standards can be effectively implemented by infrastructure managers.

3.2. BIN's Weaknesses in Combating Cybercrime at This Time

a. Analysis of Weaknesses from the Perspective of Friedman's Legal System Theory

1) Weaknesses in the Legal Structure

From the perspective of legal structure within Lawrence M. Friedman's legal system theory, BIN faces several fundamental weaknesses in combating cybercrime. The existing institutional structure has not fully accommodated the unique characteristics of cyber threats, which are cross-border, multidimensional, and require a rapid response.

The fragmented coordination structure between institutions is a major weakness in the system. The State Intelligence Agency (BIN), the National Cyber and Cyber Security Agency (BSSN), the National Police (Polri), the Indonesian National Armed Forces (TNI), and related ministries have separate organizational structures with coordination mechanisms that are not yet optimally integrated. The lack of a single authority to handle national cyber incidents leads to inefficiency and potential conflicts of authority.

BIN's internal organizational structure, which remains hierarchical and bureaucratic, is not fully suited to the needs of cyber operations, which require flexibility and rapid response. Lengthy decision-making processes can hamper effective responses to cyber incidents requiring immediate action.

The oversight and accountability structure for BIN's cyber operations also remains weak. The lack of a specific oversight mechanism for cyber operations poses a risk of abuse of authority and human rights violations.

2) Weaknesses in Legal Substance

The legal substance governing the role of the State Intelligence Agency (BIN) in combating cybercrime faces several fundamental weaknesses. Law Number 17 of 2011 concerning State Intelligence does not explicitly regulate BIN's specific authority in handling cybercrime, creating legal uncertainty in its operational implementation.

The unclear definitions of cyber threats, cybercrimes, and cyber incidents in existing laws and regulations create ambiguity in determining BIN's jurisdiction and authority. This can lead to overlapping authority with other institutions or, conversely, a lack of authority in certain cases.

The operational gaps governing procedures and mechanisms for combating cybercrime constitute a serious legal weakness. The absence of comprehensive and detailed Standard Operating Procedures (SOPs) leads to inconsistencies in task execution and potential procedural violations.

Existing legal provisions also do not adequately regulate human rights protection in BIN cyber operations. Unclear boundaries of surveillance and data collection authority could potentially lead to violations of privacy rights and other constitutional rights.

b. Weaknesses in the Regulatory Aspects and Legal Certainty

1) Unclear Authority and Jurisdiction

A fundamental weakness in the regulatory aspect lies in the unclear operational authority of BIN in the cyber domain. Law Number 17 of 2011 concerning State Intelligence provides a general mandate without specific specifications regarding authority to handle cybercrime. This lack of clarity creates ambiguity in operational implementation and potential conflicts of authority with other institutions.

The issues raised are increasingly complex given the often transnational nature of cybercrime. BIN faces challenges in determining territorial and personal boundaries of authority when handling cyber cases involving multiple jurisdictions.

The unclear division of roles and responsibilities between BIN and BSSN, institutions with specific mandates in cybersecurity, has become a source of legal conflict. The lack of clear delineation of each institution's respective domains of authority has led to duplication of effort and resource inefficiencies.

The BIN's authority to conduct surveillance and interception of communications in the cyber context has also not been explicitly regulated. This lack of clarity could pose a risk of constitutional rights violations and legal challenges to its operations.

2) Operational Regulatory Void

The State Intelligence Agency (BIN) faces a significant operational regulatory gap in combating cybercrime. The absence of specific implementing regulations governing operational standards, procedures, coordination mechanisms, and protocols for handling cyber incidents creates uncertainty in implementation.

This regulatory gap impacts the accountability and transparency of BIN operations. Without a clear legal framework regarding the limits of authority and oversight mechanisms, there is potential for power protection and process abuses. The absence of regulations governing inter-agency cooperation in handling cyber incidents leads to ad hoc and unstructured coordination. This hampers effective responses to cyber threats that require coordinated action.

The regulatory gap is also evident in international cooperation in handling transnational cybercrime. The State Intelligence Agency (BIN) lacks a legal

framework to collaborate with foreign intelligence agencies to share information and coordinate responses.

c. Weaknesses in Institutional and Structural Aspects

1) Fragmentation of Inter-Institutional Coordination

The national cybersecurity institutional structure, which is spread across various institutions, creates significant coordination challenges. The State Intelligence Agency (BIN), the National Cyber and Security Agency (BSSN), the National Police (Polri), the Indonesian National Armed Forces (TNI), and related ministries have overlapping mandates but lack an optimally integrated coordination mechanism.

This fragmentation is exacerbated by persistent sectoral egos within each institution. Each institution tends to maintain its own domain of authority and resources without considering the need for synergy in addressing multidimensional cyber threats.

The absence of a clear lead agency for handling national cyber incidents creates confusion within the command and control structure. This can hinder the rapid decision-making necessary for crisis management.

Existing coordination mechanisms are ad hoc and not yet well institutionalized. Coordination often relies on personal relationships rather than established institutional frameworks.

2) Limited Organizational Capacity

BIN faces limited organizational capacity to address the increasing complexity and volume of cyber threats. Its conventional organizational structure has not fully adapted to the characteristics of cyber operations, which require flexibility and agility.

These limitations are reflected in the suboptimal resource allocation to support cyber operations. BIN faces challenges in allocating human resources, technology, and budget to develop adequate cyber capabilities.

The organization's hierarchical and bureaucratic culture hinders the implementation of agile and adaptive work methodologies. Lengthy decision-making processes can hinder responsiveness to cyber threats that require immediate action. Capacity building within the organization also faces challenges in terms of knowledge management and institutional learning. BIN lacks an effective system for capturing, storing, and sharing the knowledge necessary for continuous improvement.

d. Weaknesses in Human Resources Aspects

1) Technical Skills Deficit

BIN faces a shortage of personnel with specific technical expertise in cybersecurity. This skills gap is significant given the complexity and rapid evolution of technology and cyber threats. The lack of expertise in malware analysis, digital forensics, incident response, and cyber threat hunting is a critical weakness.

This skills gap is increasingly concerning given the rapid pace of technological development. BIN is struggling to keep up with the latest technological trends, such as artificial intelligence, quantum computing, and blockchain, which are beginning to be exploited by cybercriminals.

This limited expertise is also reflected in a lack of understanding of advanced persistent threats and sophisticated attack vectors used by state actors. BIN requires personnel with specialized expertise in cyber attribution, geopolitical analysis, and strategic intelligence analysis. Recruitment challenges also pose a serious challenge in addressing the skills deficit. BIN faces stiff competition from the private sector in attracting high-quality talent. The compensation and career paths offered by the private sector are often more attractive than those offered by the government sector.

2) Limitations of Capacity Development Programs

The capacity development program for BIN personnel in cybersecurity remains limited in both quantity and quality. The lack of a comprehensive and up-to-date ongoing training program has led to a widening skills gap between personnel capabilities and operational needs. Existing training programs are often ad hoc and not integrated into strategic human resource development plans. BIN lacks a structured curriculum to systematically develop expertise in various aspects of cybersecurity.

Limited international training opportunities also hamper personnel capacity development. Exposure to international best practices and cutting-edge technology is crucial for enhancing operational capabilities. Quality assurance within training programs is also weak. BIN lacks a standardized assessment and certification mechanism to ensure that training achieves its stated learning objectives.

3.3. The Role of BIN in Combating Cybercrime Based on Legal Certainty

a. Conceptualization of Legal Certainty in the Context of Cyber Security Based on Gustav Radbruch's Theory

1) Theoretical Basis of Legal Certainty by Gustav Radbruch

InanalyzeTo examine the role of BIN in combating cybercrime based on legal certainty, the author uses the theoretical framework of legal certainty developed by Gustav Radbruch. According to Radbruch, legal certainty is one of the three

basic values of law (rechtswerte) along with justice (gerechtigkeit) and utility (zweckmäßigkeit).

Radbruch emphasized that legal certainty relates not only to predictability in law enforcement but also to aspects of legitimacy and consistency within the legal system. In the context of combating cybercrime, legal certainty is a crucial foundation for ensuring that BIN's actions have a clear and accountable legal basis.

Radbruch's theory also recognizes the tension between legal certainty and other legal values. In certain circumstances, legal certainty can conflict with substantive justice or practical utility. However, Radbruch emphasizes the importance of finding a balance between these three values in an ideal legal system.

In its application to the cyber domain, Radbruch's theory provides a framework for analyzing how legal certainty can be achieved without sacrificing BIN's operational effectiveness in dealing with dynamic and evolving cyber threats.

2) Dimensions of Legal Certainty in BIN Cyber Operations

Legal certainty in preventing cybercrime by BIN encompasses three main dimensions based on the Radbruch framework. First, normative surety, which refers to the clarity of the laws and regulations governing BIN's authority and operational limitations in the cyber domain.

Second, implementation certainty (certainty of implementation) relates to the standardization of procedures and operational methods. This dimension ensures that every BIN personnel clearly understands the procedures to be followed in conducting cyber operations.

Third, enforcement certainty, which includes consistency in the application of sanctions and accountability measures. This dimension ensures that violations of legal requirements and procedures will result in appropriate and consistent consequences.

This third dimension of legal certainty must be integrated into a comprehensive legal framework governing the role of BIN in cybercrime. This integration is necessary to create a coherent and effective system.

b. Regulatory Framework for Legal Certainty of BIN Operations

1) Specific and Firm Reformulation of Authority

The role of the State Intelligence Agency (BIN) in combating cybercrime based on legal certainty requires a comprehensive reformulation of the legal framework governing BIN's authority. This can be achieved through amendments to Law No.

17 of 2011 concerning State Intelligence or the issuance of a specific law on national cybersecurity.

This reformulation must include a clear and comprehensive definition of cyber threats, cyber incidents, and cybercrimes within the jurisdiction of BIN. This definition must be specific enough to provide clear guidance yet flexible enough to accommodate the changing nature of global threats. The new legal framework must also regulate the mechanism for the division of authority between BIN and other institutions such as the National Cyber and Cyber Security Agency (BSSN), the Indonesian National Police (Polri), and the Indonesian National Armed Forces (TNI). This delineation should be based on each institution's functional specialization and comparative advantages in addressing various types of cyber threats.

Aspects of international cooperation must also be explicitly regulated in the new legal framework. BIN requires clear legal authority to engage in information exchange and joint operations with foreign intelligence agencies to combat transnational cyber threats.

2) Development of Comprehensive Standard Operating Procedures

Ensuring legal certainty in BIN operations requires the development of comprehensive and detailed Standard Operating Procedures (SOPs). These SOPs should govern all aspects of cybersecurity operations, from threat detection and analysis to response and recovery procedures. SOPs should include clear guidelines for decision-making in various scenarios. Decision trees and escalation procedures should be established to ensure personnel can make informed decisions in time-sensitive situations without violating legal requirements.

Human rights and privacy protection must be integrated into every stage of operational procedures. SOPs should include specific provisions to protect constitutional rights and minimize collateral damage to non-target individuals. Quality control and compliance monitoring mechanisms should also be incorporated into SOPs. Regular audits and assessments should be conducted to ensure compliance with established procedures and identify areas for improvement.

3) Monitoring and Accountability Mechanism

The legal certainty framework must include robust oversight and accountability mechanisms to ensure that BIN operates within the bounds of the law. A multi-layered oversight system must be established, encompassing internal oversight, executive oversight, legislative oversight, and judicial oversight. The internal oversight mechanism should include an independent inspector general or ombudsman with the authority to investigate complaints and conduct

compliance audits. This internal oversight body should have access to all relevant information and the authority to make binding recommendations.

Legislative oversight should be conducted by a special parliamentary committee with security clearance and technical expertise to effectively oversee cyber operations. This committee should have a regular briefing schedule and investigative powers. Judicial oversight mechanisms should be established for specific categories of cyber operations involving intrusive surveillance or data collection. Specialized cyber courts or appointed judges with technical expertise could provide effective judicial review.

c. Legal Certainty-Based Coordination Framework

1) Institutional Coordination Mechanism

The role of the State Intelligence Agency (BIN) in combating cybercrime based on legal certainty requires a legally and formally regulated institutional coordination mechanism. This mechanism could include the establishment of a National Cyber Security Coordination Center (NCSCC) with a clear legal mandate. The NCSCC should be led by a high-ranking official with members from BIN, the National Cyber Security Agency (BSSN), the Indonesian National Police (Polri), the Indonesian National Armed Forces (TNI), and relevant ministries. The NCSCC's structure and authority should be stipulated in a specific legal instrument to ensure legitimacy and effectiveness.

The legal framework should clearly define the roles and responsibilities of each member of the NCSCC. Functional delineation should be based on each institution's comparative advantages and core competencies. Decision-making procedures within the NCSCC should also be detailed in the legal framework. Consensus-building mechanisms, voting procedures, and binding mechanisms should be established to facilitate effective decision-making.

2) Information Sharing Framework

Legal certainty in inter-agency information exchange requires a comprehensive legal framework governing information classification, declassification procedures, sharing protocols, and the protection of sensitive information. This framework must balance operational needs with security requirements. The legal framework should include liability protections for personnel and agencies involved in the exchange of information in good faith. Indemnity clauses should provide adequate safeguards to encourage openness in the sharing of threat intelligence.

Data protection and privacy protection should also be incorporated into the information-sharing framework. Procedures for handling accidentally collected personal data should be established to ensure compliance with privacy rights.

International information exchange should also be regulated within a legal framework with appropriate safeguards to protect national security information. Reciprocal agreements with foreign institutions should have an adequate legal basis.

3) Integrated Response Mechanism

The legal framework should establish a unified response mechanism for major cyber incidents requiring multi-agency coordination. A clear command and control structure should be established to facilitate a rapid and effective response. An incident classification system should be developed to determine the appropriate level of response and agency involvement. Classification criteria should be objective and measurable to ensure consistent application.

Resource allocation mechanisms should be regulated within a legal framework to ensure equitable sharing of costs and resources in joint operations. The burden-sharing formula should be transparent and fair. Post-incident review procedures should also be established to facilitate learning and improvement. After-action reports should be required for all major incidents, with recommendations for improving future response capabilities.

d. Protection of Human Rights and Civil Liberties

1) Privacy Protection Framework

The State Intelligence Agency (BIN)'s role in combating cybercrime must implement a robust privacy protection framework that aligns with constitutional guarantees and international human rights standards. This framework should regulate data collection limits, retention periods, sharing limitations, and notification requirements. Privacy impact assessments should be required for all cybersecurity operations involving the collection or processing of personal data. These assessments should be conducted prior to the implementation of any new program or technology.

The principle of data minimization must be applied in all collection activities. BIN must collect only data necessary for legitimate security purposes and avoid excessive or indiscriminate data collection. Individual rights mechanisms must be established to allow citizens to access information about collected data and any unlawful collection or processing. The right to redress must be provided to individuals affected by wrongful surveillance.

2) Fair Legal Process Safeguards

Because security processes must be embedded in every BIN operational activity in the cyber domain. Procedural safeguards should include the right to notify (with exceptions for ongoing operations), the right to challenge surveillance orders, and the right to legal representation. Warrant requirements should be

established for specific categories of intrusive cyber operations. Judicial authorization should be required for operations involving significant privacy intrusions or restrictions on constitutional rights.

Appeal mechanisms should be available for individuals who believe their rights have been violated in cybersecurity operations. An independent review body should be established to handle complaints and provide solutions. Compensation mechanisms should be provided for damages caused by erroneous cyber operations. Victims should have access to adequate remedies, including monetary compensation and corrective action.

3) Public Transparency and Accountability

While operational security considerations limit full transparency, BIN must provide adequate public information on the general framework and policies of cybersecurity operations. Annual public reports should be published with appropriate editorials. Public consultation mechanisms should be established for major policy changes impacting civil liberties. Stakeholder engagement should be facilitated through appropriate forums and channels.

Media relations policies should be developed to provide the public with accurate information about cybersecurity threats and government responses without compromising operational security. Educational outreach programs should be implemented to increase public understanding of cybersecurity threats and individual protection measures. Public awareness campaigns can help create an informed public.

4. Conclusion

Based on a comprehensive analysis that has been conducted using the theoretical framework of Lawrence M. Friedman's Legal System, the Theory of Authority, and Gustav Radbruch's Theory of Legal Certainty, it can be concluded that the role of BIN in combating cybercrime currently still faces various fundamental challenges that require systemic reform. From a legal structure perspective, BIN has a fundamental legal basis, but it is not specific to the cyber domain. The legal substance governing BIN's role is not yet comprehensive and contains various regulatory limitations. The legal culture in its implementation is still adapting to the complexity of cyber issues. The proposed legal certainty framework, based on Gustav Radbruch's theory, offers a comprehensive solution to address existing weaknesses. Implementing this framework requires strong political will, adequate resource allocation, and long-term commitment from all stakeholders. With the implementation of a comprehensive legal certainty framework, the State Intelligence Agency (BIN)'s role in combating cybercrime can be more effective, accountable, and sustainable in the face of evolving cyber threats. The State Intelligence Agency (BIN) plays a vanguard role in detecting, preventing, and addressing cyber threats through cyber intelligence activities.

This role is realized through data collection and analysis, mapping potential attacks, securing strategic infrastructure, and coordinating with relevant institutions such as the National Cyber and Cyber Security Agency (BSSN), the Indonesian National Police (Polri), and the Ministry of Communication and Informatics. BIN also conducts cyber counterintelligence operations to prevent infiltration by foreign parties and cybercriminal groups that threaten national security. The State Intelligence Agency (BIN) faces several weaknesses, including: 1. Regulations regarding BIN's authority in the cyber domain are not yet specific, resulting in overlap with other institutions. 2. Limited human resources and technology in dealing with increasingly complex cyber attacks. 3. The lack of transparency and accountability in the implementation of cyber tasks, which has the potential to give rise to conflicts of authority. 4. Coordination between institutions is not optimal, causing responses to cyber threats to often be slow. To ensure legal certainty, BIN's role must be based on clear regulations regarding the limits of its authority, data collection procedures, and mechanisms for cooperation with law enforcement. This legal certainty is necessary to prevent BIN's actions from resulting in human rights violations or jurisdictional conflicts. BIN must also adhere to the principles of legality, proportionality, and accountability in all its cyber operations to ensure compliance with Indonesian law.

5. References

Journals:

Abdul Latif. "Kepastian Hukum dalam Era Digital". Jurnal Daulat Hukum, Vol. 7, No. 1, 2024.

Agus Raharjo. "Kepastian Hukum dalam Era Digital". Jurnal Daulat Hukum, Vol. 12, No. 1, 2025.

Ahmad Rifai. "Implementasi Kepastian Hukum dalam Operasi Intelijen". Law Development Journal, Vol. 10, No. 2, 2025.

Ahmad Santoso. "Cyber Intelligence dalam Perspektif Keamanan Nasional". Law Development Journal, Vol. 6, No. 2, 2024.

Anna Erliyana. "Koordinasi Kewenangan dalam Penanggulangan Kejahatan Siber". Law Development Journal, Vol. 9, No. 2, 2025.

Bagir Manan. "Kewenangan Atribusi, Delegasi dan Mandat dalam Hukum Administrasi". Jurnal Daulat Hukum, Vol. 10, No. 1, 2025.

Edy Santoso. "Sistem Peringatan Dini dalam Keamanan Nasional". Law Development Journal, Vol. 5, No. 2, 2022.

Hikmahanto Juwana. "Koordinasi Antar Lembaga dalam Penanggulangan Kejahatan Siber". Law Development Journal, Vol. 4, No. 3, 2023.

Joko Widodo. "Keamanan Siber sebagai Bagian Keamanan Nasional". Jurnal Daulat Hukum, Vol. 8, No. 1, 2025.

M. Yusuf Samad & Pratama Dahlian Persadha. "Memahami Perang Siber Rusia dan Peran Badan Intelijen Negara Dalam Menangkal Ancaman di Bidang Siber". Jurnal IPTEK dan Komunikasi (IPTEKKOM), BPSDMP Kominfo Yogyakarta, 2022.

Marcus Lukman. "Concurrent Authority dalam Sistem Hukum Indonesia". Jurnal Daulat Hukum, Vol. 11, No. 1, 2025.

Teguh Prasetyo. "Analisis Yuridis Peran BIN dalam Penanggulangan Ancaman Siber". Jurnal Daulat Hukum, Vol. 6, No. 1, 2023.

Widodo Muktiyo. "Perkembangan Kejahatan Siber dan Tantangan Penegakan Hukumnya". Jurnal Daulat Hukum, Vol. 5, No. 2, 2022.

Books:

A.S.S. Tambunan. Intelijen: Teori, Aplikasi dan Modernisasi. Jakarta: Pustaka Sinar Harapan, 2018.

Adrian Sutedi. Hukum Perizinan dalam Sektor Pelayanan Publik. Jakarta: Sinar Grafika, 2021.

Badan Intelijen Negara, Analisis Efektivitas Pertukaran Informasi Siber 2024, Laporan Internal, Jakarta, BIN, 2024

Badan Siber dan Sandi Negara, Laporan Tahunan Pemantauan Keamanan Siber 2021, Jakarta, BSSN, 2022

Charles R. Beitz, Political Theory and International Relations, Revised Edition, Princeton: Princeton University Press, 1999

Christine M. Korsgaard, Creating the Kingdom of Ends, Cambridge: Cambridge University Press, 1996

Danrivanto Budhijanto. Cyberlaw dan Revolusi Digital. Bandung: Logoz Publishing, 2022.

David Miller, Principles of Social Justice, Cambridge: Harvard University Press, 1999

Edmon Makarim. Kompilasi Hukum Telematika. Jakarta: Raja Grafindo Persada, 2019.

Frances M. Kamm, Intricate Ethics, New York: Oxford University Press, 2007

Franz Magnis-Suseno. Etika Politik: Prinsip-prinsip Moral Dasar Kenegaraan Modern, Edisi Kelima. Jakarta: Gramedia Pustaka Utama, 2021.

G.A. Cohen, If You're an Egalitarian, How Come You're So Rich?, Cambridge: Harvard University Press, 2000

Gustav Radbruch. Legal Philosophy, translated by Kurt Wilk. Cambridge: Harvard University Press, 1950.

H.L.A. Hart, The Concept of Law, 3rd Edition, Oxford: Oxford University Press, 2012

Hans Kelsen, Pure Theory of Law, translated by Max Knight, Berkeley: University of California Press, 1967.

Indroharto. Usaha Memahami Undang-undang tentang Peradilan Tata Usaha Negara, Cetakan Kelima. Jakarta: Pustaka Sinar Harapan, 2019.

Isaiah Berlin, Two Concepts of Liberty, Oxford: Oxford University Press, 1969

Jeffrey Carr. Inside Cyber Warfare, 2nd Edition. Sebastopol: O'Reilly Media, 2012.

Jeremy Bentham, An Introduction to the Principles of Morals and Legislation, Oxford: Oxford University Press, 1996

Kementerian Komunikasi dan Informatika, Laporan Evaluasi Penanganan Insiden Siber 2023, Laporan Internal, Jakarta, Kementerian Kominfo, 2024

Lawrence M. Friedman. American Law: An Introduction. New York: W.W. Norton & Company, 1984.

Lili Rasjidi dan I.B. Wyasa Putra. Hukum sebagai Suatu Sistem, Edisi Kedua. Bandung: Remaja Rosdakarya, 2020.

Mahrus Ali. Kejahatan Korporasi: Kajian Relevansi Sanksi Tindakan bagi Penanggulangan Kejahatan Korporasi. Yogyakarta: Arti Bumi Intaran, 2018.

Marcia Baron, Kantian Ethics Almost Without Apology, Ithaca: Cornell University Press, 1995

Neil MacCormick, Legal Reasoning and Legal Theory, Oxford: Clarendon Press, 1978

Onora O'Neill, Justice Across Boundaries, Cambridge: Cambridge University Press, 2000

Paul Guyer, Kant on Freedom, Law, and Happiness, Cambridge: Cambridge University Press, 2000

Paulus Effendie Lotulung. Beberapa Sistem tentang Kontrol Segi Hukum terhadap Pemerintah. Jakarta: Bhuana Ilmu Populer, 2018.

Richard A. Clarke and Robert K. Knake. Cyber War: The Next Threat to National Security. New York: Ecco Books, 2010.

Richardus Eko Indrajit. Cyber Intelligence dan Ketahanan Nasional. Jakarta: Andi Publisher, 2020.

Samuel Scheffler, The Rejection of Consequentialism, Revised Edition, Oxford: Oxford University Press, 1994

Satjipto Rahardjo. Ilmu Hukum. Bandung: Citra Aditya Bakti, 2000.Satjipto Rahardjo. Ilmu Hukum, Edisi Revisi, Cetakan VIII. Bandung: Citra Aditya Bakti, 2019.

Tom L. Beauchamp and James F. Childress, Principles of Biomedical Ethics, 7th Edition, New York: Oxford University Press, 2013

Tony Honoré, Responsibility and Fault, Oxford: Hart Publishing, 1999

Regulation:

The 1945 Constitution of the Republic of Indonesia

Law Number 17 of 2011 concerning State Intelligence