THE EFFECTIVENESS OF LAW ENFORCEMENT IN STRENGTHENING STATE INTELLIGENCE TO COUNTERACT INFORMATION SYSTEM HACKING AS A THREAT TO THE SOVEREIGNTY OF THE INDONESIAN NATION

Syukur Kasieli Hulu
Universitas Nias
syukurkasieli88@gmail.com

Abstract: *The rapid development of information technology has opened up opportunities for the emergence of new threats to national security, one of which is the hacking of information systems. Cyber attacks not only cause economic losses and disruption of public services, but also pose a serious threat to Indonesia's digital sovereignty. In this context, state intelligence has a strategic role as the frontline in detecting, analyzing, and counteracting various forms of threats to the country's strategic information systems. However, strengthening the state intelligence function in the face of hacking crimes still faces various obstacles, both from the aspects of regulations that have not been adaptive, weak inter-agency coordination, to limited technology and human resources. This study aims to examine the effectiveness of strengthening state intelligence in counteracting hacking of information systems, and formulate the urgency of national legal policy reforms that support the formation of a strong, integrated, and professional cyber intelligence system. Using normative legal research methods supported by conceptual and case approaches, this study concludes that strengthening state intelligence requires regulatory reform, institutional integration, and investment in technology and human resources to maintain the nation's sovereignty in the digital era.*
Keywords*: State Intelligence, Hacking, Digital Sovereignty, Cyber Security, Legal Policy.*

A. Background

In today's digital era, information systems have become the backbone of various aspects of national life. Starting from the government system, defense, economy, to public services, it relies heavily on information and communication technology. However, the development of this technology also creates new vulnerabilities in the form of cyber threats, one of which is hacking against the state's strategic information system. Hacking of information systems is not just a conventional criminal offense that is materially detrimental, but has developed into a form of threat to state sovereignty. This is evident from the many cases of cyber attacks targeting strategic institutions such as the Ministry of Defense, BSSN (Badan Siber dan Sandi Negara), as well as other financial and government institutions. These attacks have the potential to leak confidential information, paralyze public service systems, and cause social and political instability that threatens the integrity of the Republic of Indonesia.

In this context, state intelligence has a crucial role in detecting, analyzing, and preventing these potential threats. However, intelligence tasks and functions will not run optimally without the support of a strong and responsive legal system. Effective law enforcement is the backbone of strengthening intelligence, especially in terms of coordination, division of authority, and regulation of legal mechanisms against cyber criminals. The effectiveness of law enforcement in dealing with hacking crimes in Indonesia still faces various challenges. Starting from the limitations of specific regulations, overlapping authority between institutions, to the lack of human resource capabilities in the field of cyber law and digital forensics. Law Number 11/2008 on Electronic Information and Transactions (ITE) has indeed become the legal basis for the

prosecution of cybercrime, but in practice it still leaves gray spaces that hinder the speed and accuracy of legal responses to cyber threats that are dynamic and transnational.

Therefore, the study of the effectiveness of law enforcement in strengthening state intelligence is very important to encourage the formation of a strong national cyber resilience system. This research is expected to answer the extent to which law enforcement in Indonesia has been able to support the performance of state intelligence in counteracting hacking of information systems as a form of threat to sovereignty, as well as offering constructive solutions to existing obstacles. The changing national security landscape in the digital era demands a redefinition of conventionally understood threats, such as military aggression or physical espionage. In the current context, cyber attacks carried out by both state and non-state actors have become strategic weapons used to weaken a country without having to involve physical force. Hacking state-owned information systems is now understood as a form of asymmetric aggression that cannot be underestimated. The impact is not only material losses, but also threats to the integrity of national data, government stability, and the nation's political and economic sovereignty.

Cyber attacks against Indonesia are increasing in intensity and complexity. Several times the country's strategic information systems have experienced data leaks, both due to weak cyber defense systems and due to late detection from intelligence agencies. In some cases, the motives and perpetrators of cyberattacks are difficult to trace quickly due to their hidden, cross-border nature and the use of sophisticated encryption technology. This shows that strengthening the cybersecurity system cannot be separated from the proactive, adaptive, and high-tech-based capabilities of state intelligence. However, in reality, the function of state intelligence has not been fully optimized because it is still hampered by regulations that do not support synergy between law enforcement, intelligence agencies, and cybersecurity institutions such as BSSN. There is still dualism of authority and a lack of data integration that causes a slow response to large-scale cyber attacks. On the other hand, law enforcement against hacking perpetrators has not yet provided a deterrent effect, due to weak digital evidence and reactive legal processes.

The existence of the State Intelligence Law (Law No. 17/2011) has not specifically regulated cyber intelligence, which should be part of national defense in facing cyber threats. In addition, law enforcement against hacking crimes is still sporadic and tends to be case-by-case, not yet systematic and integrated nationally. This indicates the need to develop a comprehensive and synchronized national legal policy between intelligence regulations, the criminal justice system, and information technology legal instruments.

Law enforcement is the process of application or implementation of legal norms that apply concretely by law enforcement officials to legal events that occur in society. According to Soerjono Soekanto, the effectiveness of law enforcement is influenced by several factors, including: law itself, law enforcers, facilities, society, and legal culture. In the context of cybercrime, hacking of information systems is a complex criminal offense so that law enforcement must be carried out quickly, accurately, and based on information technology. Law enforcement against hacking crimes requires coordination between law enforcement agencies (police, prosecutors, judges) and institutions that have authority in the field of information security, such as the Badan Siber dan Sandi Negara (BSSN), the Ministry of Communication and Information, and the National Intelligence Agency. This is where the challenge of law enforcement comes into play: whether our national legal system is robust enough to respond to the dynamics of digital threats.

State intelligence is a strategic function of the state in conducting investigation, security, and mobilization activities to anticipate and counteract various forms of threats to national security. According to Law No. 17/2011, state intelligence has the authority to conduct early detection of all forms of threats to the sovereignty, territorial integrity, and

safety of the nation. However, in the midst of growing digital threats and cyber hacking, the role of state intelligence needs to be strengthened in terms of regulations, institutions, and cross-sector coordination. Strengthening intelligence is not enough only from the operational aspect, but must be supported by legal certainty in the form of firm, transparent, and fair rules of the game. The law provides limits and at the same time legitimizes the authority of intelligence to remain within the corridors of democracy and the rule of law.

Cyber crime is a modern form of crime that attacks information technology systems. Hacking is an illegal activity undertaken to access information systems without authorization. The impact of hacking is not only individual, but can attack the country's strategic systems such as government databases, military security, and economic infrastructure. According to Ridwan Khairandy, hacking crimes are now not only seen as a violation of personal data, but have shifted into a form of serious threat to state sovereignty because they target vital sectors and use sophisticated methods that are difficult to detect. In dealing with this crime, effective, integrated, and prevention-oriented law enforcement is needed, not just repressive.

Legal effectiveness in the context of law enforcement against cybercrime is measured by how much the law is able to be implemented and obeyed consistently. Barda Nawawi Arief emphasized that legal effectiveness depends on the accuracy between the written law and the social reality at hand. That is, if the crime faced is digital, but the rule of law is still conventional, then the effectiveness of the law will be weak. On the other hand, hacking into state-owned information systems can be seen as a violation of Indonesia's digital sovereignty. In the era of technological globalization, state sovereignty concerns not only territorial boundaries, but also control over data, systems and national digital architecture. Thus, law enforcement and state intelligence must synergize in maintaining this digital sovereignty.

B. Research Method

This research is a normative legal research, which is conducted to examine the effectiveness of positive legal norms (especially the ITE Law and the State Intelligence Law) in strengthening the role of state intelligence to counteract hacking crimes as a form of threat to national sovereignty. This approach is used to examine the applicable laws and regulations, legal principles, and relevant legal literature. In addition, this research is also empirical juridical**,** as a complement, to see how the implementation of these legal norms in practice, including obstacles and the effectiveness of inter-agency coordination such as law enforcement officials and intelligence agencies in the field.

C. Results and Discussion

Information System Hacking as a Threat to State Sovereignty

In the digital era, state sovereignty is no longer limited to physical territory, but also includes cyberspace, which is a vital part of governance, defense, economy, and social life. Hacking of information systems, both government and private, is a form of attack that can threaten national stability and damage the integrity of the country's data and digital infrastructure. Cyberattacks such as hacking, malware, ransomware, and phishing can cause confidential data leaks, paralysis of public service systems, information manipulation, and social unrest. Several hacking cases in Indonesia, such as the leakage of population data, hacking of the KPU website, and attacks on ministry systems, show how vulnerable Indonesia's strategic information systems are to external and internal threats. Hacking crimes are generally committed by sophisticated persistent threats and are often not easily detected. In some cases, these attacks are carried out by state actors as part of

foreign intelligence operations, so the impact is not only on material losses but also on national sovereignty.

The Strategic Role of State Intelligence in Cyber Threat Detection and Prevention

State intelligence has a vital function in the non-military defense system that focuses on early detection, risk analysis, and prevention of various threats to national security, including cyber attacks. Based on Law No. 17/2011 on State Intelligence, intelligence is tasked with protecting national security through collecting, processing, and presenting strategic information to the President and relevant institutions. However, in the context of digital threats, state intelligence must experience an expansion of functions into cyber intelligence capable of monitoring the movement of virtual threats in real time, analyzing attack patterns, and collaborating with technical institutions such as BSSN, Kominfo, and TNI Cyber Unit.

Strengthening state intelligence in the face of hacking crimes includes:

1) Increased technical capacity and human resources in the field of cybersecurity
2) Establishment of an integrated cyber intelligence unit
3) Inter-agency coordination in the national cyber security system
4) Renewal of policies and legal frameworks that support the flexibility of intelligence tasks

Intelligence must be supported by adequate and law-based authority in order to move preventively and tactically. The role of intelligence that is only reactive is no longer adequate to deal with dynamic and sophisticated cyber crime.

Institutional and Regulatory Weaknesses in Strengthening Cyber Intelligence

To date, regulations governing the specific role of intelligence in the cyber domain remain incomplete. The Intelligence Law does not explicitly regulate cyber warfare, digital intelligence, or the protection of national strategic data**.** This creates a normative vacuum that can weaken the position of intelligence in the face of high-scale cyber threats.

In addition, institutional fragmentation between intelligence agencies, law enforcement, and information technology regulators often leads to overlapping authority and weak coordination. For example, the tasks and functions between BIN, BSSN, and the National Police Cyber Detachment have not been fully integrated into a unified national security system. As a result, responses to cyber threats are often slow and ineffective.

The Urgency of Legal and Policy Reform in Supporting State Intelligence

To strengthen the role of state intelligence in counteracting hacking of information systems, national legal policy reforms are needed that include the following:

1) Revise the State Intelligence Law to add a digital/cyber intelligence clause
2) Synchronization between institutions through derivative regulations in the form of a Perpres or PP
3) Law enforcement oriented towards the protection of strategic information systems
4) Strengthening the cyber-based national security system supported by a clear budget, technology and legal framework.

The state must establish a national cyber intelligence system framework that brings together all the power and information from related institutions. Intelligence cannot work alone without systemic support from the government and the rule of law.

Digital Sovereignty as a Pillar of National Defense

In the modern context, digital sovereignty has become part of the concept of state sovereignty, which concerns the full right of a state to regulate, protect and oversee its digital infrastructure. A state that is unable to counteract hacking crimes and protect its citizens' data will lose legitimacy and public trust. Therefore, strengthening state intelligence is not only a technical necessity, but also part of a national strategy to defend the nation's sovereignty in the digital realm**.** Strong intelligence, effective laws, and integrated policies are inseparable pillars of today's national defense.

D. Conclusion

Information system hacking has become a serious threat to national sovereignty in the digital age. Cyberattacks are no longer limited to ordinary criminal acts, but have developed into a form of aggression that has a direct impact on national stability, public trust, and state integrity. In this context, state intelligence has a strategic role in detecting, analyzing, and counteracting these threats. However, in practice, strengthening state intelligence in dealing with hacking crimes still faces various obstacles, both in terms of regulation, institutionalization, and technical operations. Law No. 17/2011 on State Intelligence has not specifically regulated cyber intelligence, so the space for intelligence to deal with digital threats is still limited. On the other hand, coordination between institutions such as BIN, BSSN, TNI, and Polri has not been fully integrated, which causes responses to threats to often be reactive and inefficient. This condition shows that strengthening state intelligence in the face of hacking information systems must be done thoroughly and systemically. Intelligence must be equipped with advanced technological capabilities, adaptive regulations, and qualified human resource capacity in order to optimally carry out its functions in maintaining Indonesia's digital sovereignty.

Reference

Arief, Barda Nawawi. *Problems of Law Enforcement and Criminal Law Policy in Crime Control. Crime Control*. Jakarta: Kencana, 2015.

Arief, Satria. "Cyber Crime and the Challenge of State Intelligence in Maintaining Cyber Security." *Indonesian Journal of Defense and Security*, Vol. 9 No. 2, 2022.

Barda Nawawi Arief. *Problems of Law Enforcement and Criminal Law Policy in Crime Control. Crime Control*. Jakarta: Kencana, 2015.

Department of Defense of the Republic of Indonesia. *Indonesia's National Cyber Security Strategy*. Jakarta: Ministry of Defense of the Republic of Indonesia, 2021.

Khairandy, Ridwan. *Information Technology Law and Regulation*. Yogyakarta: FH UII Press, 2020.

Law of the Republic of Indonesia Number 11 of 2008 concerning Information and Transactions Electronics.

Law of the Republic of Indonesia Number 17 of 2011 on State Intelligence.

Law of the Republic of Indonesia Number 19 of 2016 concerning Amendments to the ITE Law.

National Cyber and Crypto Agency (BSSN). *Annual Report on National Cyber Security*. Jakarta: BSSN, 2023.

Nugraha, Reza. "The Role of Cyber Intelligence in the National Defense System." *Journal of*
National Security National, Vol. 8 No. 2, 2022.

Nugroho, Wahyu. *Cyber Warfare: National Strategy and Policy in Facing Cyber Threats*. Jakarta: Gramedia, 2022.

Ridwan Khairandy. *Information Technology Law and Regulation*. Yogyakarta: FH UII Press, 2020.

Soekanto, Soerjono. *Factors Affecting Law Enforcement*. Jakarta: RajaGrafindo Persada, 2007.

Sulaiman, Muhammad. *Cyber Law: Dynamics and Enforcement Challenges in the Digital Age*. Yogyakarta: Genta Publishing, 2023.

Yuliana, Meutia. "The Effectiveness of ITE Law in Tackling Cyber Attacks." *Journal of Law & Technology*, Vol. 4 No. 1, 2021.