Journal Evidence of Law
Vol 5 No 1 2026, 203-210
E-ISSN: 2828-5031 | P-ISSN: 2830-3350
Publisher: CV. Era Digital Nusantara
Website: https://jurnal.erapublikasi.id/index.php/JEL

Law Enforcement on State Intelligence Strengthening in Countering Information System Hacking as a Threat to Sovereignty in North Sumatera

[1]Krismanto Manurung, [2]Muhammad Arif Sahlepi, [3]Suci Ramadani
[1,2,3]Universitas Pembangunan Panca Budi, Medan, Indonesia
[1]risda_purba@yahoo.co.id, [2]arifsahlepi@dosen.pancabudi.ac.id,
[3]suciramadani@dosen.pancabudi.ac.id

Article History
Submission : 25-03-2026
Received : 30-03-2026
Revised : 28-04-2026
Accepted : 30-04-2026

Abstract

This study aims to analyze law enforcement on strengthening state intelligence in an effort to counteract information system hacking as a form of cybercrime that has an impact on national stability and security. The research method used is normative juridical with a legislative and conceptual approach, through a study of relevant regulations such as the Law on Information and Electronic Transactions as well as provisions on state intelligence and cyber defense. The results of the study show that strengthening the state intelligence function, both through increasing the capacity of early detection, coordination between institutions, and optimizing the legal apparatus, is a crucial factor in preventing and overcoming information system hacking. However, there are still challenges in the form of limited resources, regulatory harmonization, and cross-sector collaboration. Therefore, continuous synergy is needed between law enforcement officials, intelligence agencies, local governments, and the community to strengthen the cybersecurity system as part of protecting state sovereignty in the digital era.

Keywords: *Intelligence, Information Systems, Law Enforcement*

Abstrak

Studi ini bertujuan untuk menganalisis penegakan hukum dalam memperkuat intelijen negara dalam upaya menanggulangi peretasan sistem informasi sebagai bentuk kejahatan siber yang berdampak pada stabilitas dan keamanan nasional. Metode penelitian yang digunakan adalah yuridis normatif dengan pendekatan legislatif dan konseptual, melalui studi peraturan terkait seperti Undang-Undang Informasi dan Transaksi Elektronik serta ketentuan tentang intelijen negara dan pertahanan siber. Hasil penelitian menunjukkan bahwa penguatan fungsi intelijen negara, baik melalui peningkatan kapasitas deteksi dini, koordinasi antar lembaga, dan optimalisasi aparat hukum, merupakan faktor penting dalam mencegah dan mengatasi peretasan sistem informasi. Namun, masih terdapat tantangan berupa keterbatasan sumber daya, harmonisasi regulasi, dan kolaborasi lintas sektor. Oleh karena itu, diperlukan sinergi berkelanjutan antara aparat penegak hukum, badan intelijen, pemerintah daerah, dan masyarakat untuk memperkuat sistem keamanan siber sebagai bagian dari perlindungan kedaulatan negara di era digital.

Kata kunci: Intelijen, Penegakan Hukum, Sistem Informasi

Introduction

The development of information and communication technology in the digital era has brought fundamental changes to the order of people's lives, including in the economic, social,

Journal Evidence of Law
Vol 5 No 1 2026, 203-210
E-ISSN: 2828-5031 | P-ISSN: 2830-3350
Publisher: CV. Era Digital Nusantara
Website: https://jurnal.erapublikasi.id/index.php/JEL

political, and national security fields. These advances, on the one hand, provide ease of access to information and public services; But on the other hand, it gives rise to various new forms of cyber threats, such as information system hacking, data theft, and attacks on state-owned digital infrastructure. In this context, cyber security is an integral part of state sovereignty that must be maintained and protected by all state law enforcement and intelligence instruments.

The sovereignty of the Indonesian nation is not only measured by military and political power, but also by its ability to maintain the integrity and security of national cyberspace. Cyberattacks on government information systems can threaten national stability, damage critical infrastructure, and undermine public trust in the state. The case of hacking of state agency data and the spread of false information through digital media is clear evidence that threats to sovereignty are now not only physical, but also non-physical and structured. In the face of this threat, the role of state intelligence agencies is crucial. Intelligence is tasked with collecting, analyzing, and providing early warnings of potential threats, including in the cyber field. Law Number 17 of 2011 concerning State Intelligence has emphasized that intelligence is the front line in maintaining national security from all forms of threats, both from within and outside the country. However, the effectiveness of intelligence will not be maximized without the support of firm, coordinated, and law-based law enforcement. Law enforcement against cybercrime in Indonesia is regulated through Law Number 11 of 2008 concerning Electronic Information and Transactions (UU ITE) and its amendments, which provides a legal basis for law enforcement officials to crack down on perpetrators of hacking and misuse of electronic data. However, in practice, there are still a number of obstacles, such as limited human resources, weak coordination between institutions, and delays in responding to cross-border cyber threats.

In addition, another challenge faced is the low integration between law enforcement and state intelligence. The two often work in a sectoral manner, whereas in the context of complex cyber threats, strategic synergy is needed that includes early detection, prevention, enforcement and post-attack recovery. Thus, strengthening the national intelligence system in the digital realm must be accompanied by the effectiveness of law enforcement that is able to uphold justice while maintaining the country's strategic interests. The effectiveness of law enforcement in this field is not only measured by the number of cases successfully handled, but also by the ability of the legal system to provide a deterrent effect, protection of vital digital infrastructure, and increase national cyber resilience. Strong and responsive law enforcement is the foundation for the formation of a healthy digital security ecosystem, where the state is able to protect data, maintain information confidentiality, and maintain its sovereignty in the world.

Therefore, this research is important to examine the extent to which the effectiveness of law enforcement in Indonesia can strengthen the state intelligence function in countering information system hacking. This analysis is expected to make a conceptual contribution to the formation of a national security policy that is adaptive to technological developments, while emphasizing the importance of coordination between law enforcement officials, intelligence, and society in maintaining the nation's digital sovereignty. Based on the description of the background of the problem, in this study the author raised the title " Law Enforcement on State Intelligence Strengthening in Countering Information System Hacking as a Threat to Sovereignty in North Sumatera".

Methods Research

The type of research used is normative juridical legal research which focuses on the study of positive legal norms, legal principles, and legal doctrines related to the effectiveness

Journal Evidence of Law
Vol 5 No 1 2026, 203-210
E-ISSN: 2828-5031 | P-ISSN: 2830-3350
Publisher: CV. Era Digital Nusantara
Website: https://jurnal.erapublikasi.id/index.php/JEL

of law enforcement in strengthening the state intelligence function to counteract information system hacking as a threat to the sovereignty of the Indonesian nation. This approach focuses on the analysis of laws and regulations, legal concepts, and legal principles without being oriented to empirical phenomena, but to the substance and systematics of the applicable law. The data collection technique is carried out through library research and document studies, by examining primary legal materials such as Law Number 11 of 2008 concerning Information and Electronic Transactions and its amendments, Law Number 17 of 2011 concerning State Intelligence, implementing regulations, and relevant court decisions, supported by secondary legal materials in the form of books, journals, research results, and scientific works by experts. as well as tertiary legal materials such as dictionaries and legal encyclopedias. Data collection tools include interview guidelines, structured question lists, field notes, and document analysis checklists to verify and review legal documents. The data obtained are analyzed qualitatively through systematic and argumentative interpretation to identify the normative gap (legal gap) between positive legal provisions and legal needs in dealing with complex and cross-border cybercrimes, so that conceptual recommendations can be formulated for strengthening the national legal and intelligence system in maintaining state sovereignty in the digital era.

Results and Discussion

Regulation of the Implementation of Law Enforcement on the Strengthening of State Intelligence in Countering the Occurrence of Information System Hacking as a Threat to Sovereignty in North Sumatera

Strengthening state intelligence in countering information system hacking is an integral part of law enforcement efforts to maintain state sovereignty, especially in strategic areas such as North Sumatera. Information system hacking is no longer seen as a mere conventional crime, but as a form of cyber threat that has the potential to disrupt national security stability, state data secrecy, and public trust in government institutions. Therefore, the regulation of law enforcement implementation in this context must be based on a comprehensive and integrated legal framework between intelligence, law enforcement, and cybersecurity aspects.

Normatively, strengthening state intelligence in countering information system hacking relies on intelligence authority to carry out early detection, early warning, and early prevention of various forms of threats, including cyber threats. State intelligence plays a role in collecting, processing, and analyzing strategic information related to potential hacking attacks that can threaten the government's information system, vital infrastructure, and state strategic data. In its implementation in North Sumatera, this intelligence strengthening is very important considering that this region has national vital objects, international ports, economic centers, and local government systems that are integrated with digital systems.

Law enforcement against information system hacking crimes is carried out through synergy between intelligence agencies and law enforcement officials. State intelligence serves as the front line in providing preliminary information regarding indications, patterns, and actors behind cyberattacks. The intelligence information then becomes the basis for law enforcement officials to conduct investigations and investigations in a juridical manner. In this context, coordination between the State Intelligence Agency, the National Police of the Republic of Indonesia, and other related agencies is the key to the effectiveness of law enforcement against hacking crimes.

Journal Evidence of Law
Vol 5 No 1 2026, 203-210
E-ISSN: 2828-5031 | P-ISSN: 2830-3350
Publisher: CV. Era Digital Nusantara
Website: https://jurnal.erapublikasi.id/index.php/JEL

The regulation of law enforcement implementation also requires clarity on work mechanisms, division of authority, and standard operational procedures between intelligence and law enforcement. State intelligence is not authorized to carry out criminal prosecution directly, but it has a strategic role in supporting law enforcement through the provision of accurate data and analysis. Thus, the law enforcement process against information system hacking must still uphold the principles of the rule of law, the protection of human rights, and the principle of due process of law, so that efforts to strengthen intelligence do not lead to abuse of authority.

At the regional level, especially in North Sumatera, the implementation of strengthening state intelligence in countering information system hacking faces a number of challenges, including the limitation of human resources who have cyber expertise, very fast technological development, and the complexity of the modus operandi of hackers who often involve cross-regional and even cross-border networks. Therefore, law enforcement arrangements need to be supported by increasing intelligence capacity through special training in the field of cybersecurity, strengthening information technology facilities and infrastructure, and cooperation with related institutions and agencies. Thus, the regulation of the implementation of law enforcement to strengthen state intelligence in countering information system hacking as a threat to sovereignty in North Sumatera is a strategic effort that requires an integrated approach. The synergy between state intelligence and law enforcement officials, supported by clear regulations and adequate institutional capacity, is a decisive factor in maintaining state sovereignty from the threat of information system hacking in the digital era.

The Urgency of Law Enforcement to Strengthen State Intelligence in Countering Information System Hacking as a Threat to Sovereignty in North Sumatera

The urgency of implementing law enforcement to strengthen state intelligence in countering information system hacking is increasing along with the rapid digital transformation in the administration of government. Information system hacking not only has an impact on technical and economic losses, but also has the potential to threaten state sovereignty because it targets strategic data, government systems, and vital infrastructure. In the North Sumatera region, which has a strategic position as an economic center, international trade route, and indirect border area, the threat of information system hacking is a crucial issue that requires a strong and coordinated law enforcement response.

Strengthening state intelligence has a high urgency because intelligence plays a key role in detecting and anticipating cyber threats from an early age. State intelligence functions to collect, process, and analyze information related to potential hacking attacks, whether carried out by individuals, organized groups, or foreign actors. This intelligence information is an important basis for the state in formulating cybersecurity policies and supporting preventive law enforcement. In this context, the role of the State Intelligence Agency is very strategic in maintaining the security of state information from latent and invisible threats.

The urgency of law enforcement is also reflected in the characteristics of information system hacking crimes that are cross-regional and cross-country. Without strong intelligence support, law enforcement officials will have difficulty identifying the perpetrators, attack patterns, and networks involved. Therefore, strengthening state intelligence must be systematically integrated with law enforcement mechanisms so that any intelligence information can be followed up judicially. Synergy between state intelligence and law enforcement officials, especially the National Police of the Republic of Indonesia, is an urgent

Journal Evidence of Law
Vol 5 No 1 2026, 203-210
E-ISSN: 2828-5031 | P-ISSN: 2830-3350
Publisher: CV. Era Digital Nusantara
Website: https://jurnal.erapublikasi.id/index.php/JEL

need to ensure that the threat of hacking can not only be prevented, but also processed legally to provide a deterrent effect.

At the regional level, this urgency is even more evident considering that North Sumatera has adopted many electronic-based government systems in public services. The dependence on digital systems makes this area vulnerable to cyberattacks if it is not balanced with effective intelligence and law enforcement. The limitation of human resources in the field of cyber security and the rapid development of technology require an increase in the country's intelligence capacity through training, strengthening of intelligence technology, and inter-agency cooperation. Thus, the urgency of implementing law enforcement to strengthen state intelligence in countering information system hacking as a threat to sovereignty in North Sumatera cannot be delayed. Strengthening intelligence integrated with law enforcement is an important foundation in maintaining the stability of national security and state sovereignty in the digital era. Without these steps, the country has the potential to face serious vulnerabilities that can be exploited by parties that threaten national interests.

Obstacles to Law Enforcement to Strengthen State Intelligence in Countering Information System Hacking as a Threat to Sovereignty in North Sumatera

Law enforcement against strengthening state intelligence in countering information system hacking in North Sumatera faces various obstacles of structural, technical, and juridical nature. These obstacles have implications for the non-optimal role of state intelligence in supporting law enforcement against cybercrimes that have the potential to threaten state sovereignty. Given that information system hacking is complex, invisible, and developing very quickly, the challenges faced are increasingly multidimensional.

The first obstacle lies in the limitation of human resources who have special competencies in the field of cyber intelligence and information security. The rapid development of digital technology is not always balanced with increasing the capacity of intelligence and law enforcement apparatus in the regions. In North Sumatera, the limitations of experts in the fields of digital forensics, cyber threat analysis, and information technology intelligence have caused the early detection and tracing process of hackers to not run optimally. This condition has an impact on the slow response to strategic cyber attacks.

The second obstacle relates to the lack of inter-institutional integration and coordination. Law enforcement against information system hacking requires strong synergy between state intelligence and law enforcement officials. However, in practice, coordination between the State Intelligence Agency and the National Police of the Republic of Indonesia at the regional level still faces obstacles, both in the exchange of intelligence information and in the alignment of authority. Strategic intelligence information cannot always be immediately transformed into legally valid evidence, making it difficult to prosecute criminal proceedings. The third obstacle comes from the regulatory and legal proof aspects. Information system hacking crimes often involve perpetrators across regions and even countries, causing difficulties in determining legal jurisdiction. In addition, the characteristics of digital evidence that are easy to change, delete, or disguise are a challenge in the evidentiary process in court. In this context, law enforcement requires strong intelligence support and adaptive technical regulation, but in practice it has not been fully able to keep pace with the complexity of cybercrime.

The fourth obstacle is the limitation of technological facilities and infrastructure to support intelligence and law enforcement. Strengthening state intelligence in countering information system hacking requires the use of advanced technology, such as cyber monitoring systems, big data analysis devices, and digital forensic devices. At the regional

Journal Evidence of Law
Vol 5 No 1 2026, 203-210
E-ISSN: 2828-5031 | P-ISSN: 2830-3350
Publisher: CV. Era Digital Nusantara
Website: https://jurnal.erapublikasi.id/index.php/JEL

level, including North Sumatera, the availability and utilization of this technology is still uneven, so intelligence's ability to carry out monitoring and early prevention is limited. Thus, the obstacles of law enforcement to strengthening state intelligence in countering information system hacking in North Sumatera show that the threat of sovereignty in cyberspace is not only caused by external factors, but also by the internal limitations of the law enforcement system itself. Therefore, continuous efforts are needed to strengthen the capacity of human resources, clarify inter-agency coordination mechanisms, update regulations, and increase technological support so that law enforcement in the field of cybersecurity can run more effectively and responsively to the threat of information system hacking.

CONCLUSION

Strengthening state intelligence in countering information system hacking is a strategic element in the law enforcement system to maintain state sovereignty, especially in the North Sumatera region which has a vital position economically and governmentally. Information system hacking has developed into a cyber threat that has a direct impact on national security stability, strategic data confidentiality, and public trust, so its handling requires a comprehensive and integrated legal framework between intelligence functions, law enforcement officials, and cybersecurity systems. Normatively, the authority of early detection, early warning, and early prevention owned by state intelligence is the main foundation in anticipating cyberattacks, while the enforcement process remains within the legal corridor and upholds the principles of the rule of law and the protection of human rights. The effectiveness of implementation at the regional level still faces challenges in the form of limited resources, rapid technological development, and the complexity of cross-regional crime networks, so it is necessary to increase institutional capacity, strengthen coordination between agencies, and improve regulations. Thus, sustainable synergy between state intelligence and law enforcement officials, supported by clear regulations and adequate facilities, is key in countering information system hacking as a threat to state sovereignty in the digital era.

The urgency of implementing law enforcement to strengthen state intelligence in countering information system hacking is an increasingly urgent need amid the acceleration of the government's digital transformation, especially in North Sumatera as an economically and geopolitically strategic region. Information system hacking not only causes technical and economic losses, but also has the potential to threaten state sovereignty because it targets strategic data, government systems, and vital infrastructure. In this context, strengthening the state's intelligence function is very crucial as an instrument for early detection, threat analysis, and the formulation of preventive measures that are integrated with law enforcement mechanisms. The characteristics of cybercrime that are cross-regional and cross-border require strong synergy between state intelligence and law enforcement officials so that any strategic information can be followed up juridically and provide a deterrent effect. At the regional level, the high dependence on electronic-based government systems and limited cybersecurity resources further emphasizes the importance of increasing capacity, technology, and inter-agency coordination. Thus, strengthening integrated intelligence in the law enforcement system is the main foundation in maintaining national security stability and protecting state sovereignty from the threat of hacking in the digital age.

Law enforcement against strengthening state intelligence in countering information system hacking in North Sumatera still faces structural, technical, and juridical obstacles that result in suboptimal protection of state sovereignty in cyberspace. The limitation of human resources who have special competencies in the field of cyber intelligence and digital forensics

has an impact on the lack of maximum early detection and tracing of perpetrators. On the other hand, weak inter-agency integration and coordination means that intelligence information cannot be fully transformed effectively into the basis for law enforcement. Regulatory and evidentiary barriers, especially related to cross-border jurisdictions and the characteristics of digital evidence, also complicate the law enforcement process. In addition, the limited facilities and infrastructure of supporting technology at the regional level further limits the ability to monitor and prevent early cyber threats. Thus, these obstacles show the need for comprehensive strengthening through increasing the capacity of human resources, improving institutional coordination, adapting regulatory reforms, and modernizing technology so that law enforcement in the field of cybersecurity can run more effectively, responsively, and be able to maintain state sovereignty from the threat of information system hacking.

Bibliography

Adi, Rianto. (2021). *Metodologi Penelitian Sosial Dan Hukum*. Yayasan Pustaka Obor Indonesia.

Afrizal. (2015). *Metode Penelitian Kualitatif*. Jakarta: Raja Grafindo Persada.

Ajayi, E. F. G. (2016). "Challenges To Enforcement Of Cyber-Crimes Laws And Policy." *Journal Of Internet And Information Systems* 6, No. 1 : 1–12. Https://Doi.Org/10.5897/Jiis2015.0089.

Asshiddiqie, Jimly. (2020). *Konstitusi dan Konstitusionalisme Indonesia*. Jakarta: Konstitusi Press.

Benuf, Kornelius, and Muhamad Azhar. (2020). "Metodologi Penelitian Hukum Sebagai Instrumen Mengurai Permasalahan Hukum Kontemporer." *Gema Keadilan* 7, no. 1: 20–33.

Betz, David J., and Tim Stevens. (2019). *Cyberspace and the State: Toward a Strategy for Cyber-Power*. London: Routledge.

Chessya Tivani, Wijaya. (2025). "Perlindungan Hukum Pada Pusat Data Nasional Terhadap Kejahatan Peretasan Data." Universitas Lampung.

Dewi, Sinta. (2021). "Kedaulatan Negara dalam Era Digital." *Jurnal Keamanan Nasional* 6, no. 2.

Firmanto, Taufik, Sufiarina Sufiarina, Frans Reumi, and Indah Nur Shanty Saleh. (2024). *Metodologi Penelitian Hukum: Panduan Komprehensif Penulisan Ilmiah Bidang Hukum*. PT. Sonpedia Publishing Indonesia.

Friedman, Lawrence M. (1975). *The Legal System: A Social Science Perspective*. New York: Russell Sage Foundation.

Habib, Ridwan. (2022). "Sinergitas Intelijen dan Penegakan Hukum dalam Menghadapi Ancaman Siber." *Jurnal Kajian Keamanan Nasional* 4, no. 1.

Hamzah, Andi. (2021). *Hukum Pidana dan Masalah Penegakan Hukum di Indonesia*. Jakarta: Sinar Grafika.

Iqbal, Muhammad. (2025). "Peran Satuan Intelijen Kepolisian Dalam Penyelidikan Tindak Pidana Pembunuhan (Studi Kasus Di Kepolisian Resor Natuna)." Universitas Islam Sultan Agung Semarang.

Ismaidar, Ismaidar, And Rifqi Fairuz Ula. (2025). "Pertanggungjawaban Pidana Korporasi Terhadap Kebocoran Data Pribadi Konsumen Dalam Perspektif Hukum Pidana Siber Di Indonesia." *Hukum Inovatif: Jurnal Ilmu Hukum Sosial Dan Humaniora* 2, No. 3: 44–51.

Ismaidar, Ismaidar. (2023). "The Application Of Money Laundering Law Value-Based Justice To Wealth Obtained Offenders From The Proceeds Of Corruption." *Pena Justisia:*

Media Komunikasi Dan Kajian Hukum 22, No. 001: 137–46.

Jaya, Nyoman Serikat Putra. (2020). *Hukum dan Kejahatan Siber di Indonesia*. Yogyakarta: Deepublish.

Marpaung, Leden. (2019). *Asas-Teori-Praktik Hukum Pidana*. Jakarta: Sinar Grafika.

Moeljatno. (2020). *Asas-Asas Hukum Pidana*. Jakarta: Rineka Cipta.

Muladi. (2021). *Kebijakan Kriminalisasi dalam Rangka Pembaharuan Hukum Pidana Nasional*. Jakarta: Kencana.

Nugraha, S. Fajar. (2023). *Keamanan Nasional di Era Digital: Tantangan dan Solusi*. Jakarta: Rajawali Pers.

Nugroho, Eko. (2022). "Peretasan Sebagai Ancaman terhadap Kedaulatan Digital Negara." *Jurnal Keamanan Nasional* 6, no. 2.

Nye Jr., Joseph S. (2021). "Cyber Power and National Sovereignty." *Harvard International Review* 35, no. 4.

Pakarti, Muhammad Husni Abdulah, Didik Suhariyanto, Taqyuddin Kadir, Andrian Sah, Lilik Prihatin, Sri Ayu Astuti, And Dedy Muharman. (2025). *Hukum Siber: Menyikapi Tantangan Hukum Di Era Digital*. Pt. Nawala Gama Education.

Radbruch, Gustav. (1947). *Einführung in die Rechtswissenschaft*. Leipzig: Quelle & Meyer.

Rahardjo, Budi. (2020). *Keamanan Sistem Informasi: Konsep, Teknologi, dan Implementasi*. Bandung: Informatika.

Rahardjo, Satjipto. (2018). *Ilmu Hukum*. Bandung: Citra Aditya Bakti.

Sahlepi, Muhammad Arif, Charles Rangkuti, And Syahfira Ardani. (2025). "Implementation And Obstacles Faced In Providing Protection For Children As Victims Of Domestic Violence In Lau Gumba Village, Berastagi District, Karo Regency." In *International Conference On Artificial Intelligence, Navigation, Engineering, And Aviation Technology*, 2:123–27.

Santosa, Yudhistira. (2023). *Keamanan Siber dan Ketahanan Nasional Indonesia*. Jakarta: Rajawali Pers.

Sembiring, Tamaulina Br, Dwi Wahyono, Ony Wibriyono Angkejaya, and Lexi Jalu Aji.(2023). "Metodologi Penelitian." PT Mafy Media Literasi Indonesia.

Sholehuddin, M. (2019). *Sistem Sanksi dalam Hukum Pidana: Ide Dasar Double Track System dan Implementasinya*. Jakarta: RajaGrafindo Persada.

Soekanto, Soerjono. (2019). *Faktor-Faktor yang Mempengaruhi Penegakan Hukum*. Jakarta: RajaGrafindo Persada.

Sudarto. (2018). *Hukum dan Hukum Pidana*. Bandung: Alumni.

Tan, David. (2021). "Metode Penelitian Hukum: Mengupas Dan Mengulas Metodologi Dalam Menyelenggarakan Penelitian Hukum." *Nusantara: Jurnal Ilmu Pengetahuan Sosial* 8, No. 8: 2463–78.

Tuju, Marselino Clifer, Suci Ramadani, And Chairuni Nasution. (2025). "Penegakan Hukum Terhadap Tindak Pidana Cyber Dalam Kasus Penipuan Jual Beli Online Dalam Perspektif Kriminologi." *Innovative: Journal Of Social Science Research* 5, No. 2: 1763–76.

Umar, Bambang Widodo. "Sinergitas Penegakan Hukum dan Intelijen dalam Menangkal Ancaman Siber." *Jurnal Hukum & Keamanan Nasional* 5, no. 1 (2023).

Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik, sebagaimana telah diubah dengan Undang-Undang Nomor 19 Tahun 2016.

Undang-Undang Nomor 17 Tahun 2011 tentang Intelijen Negara.

Wardana, A D E. (2025). "Peran Badan Intelijen Negara Dalam Penanggulangan Tindak Pidana Siber Berbasis Kepastian Hukum." Universitas Islam Sultan Agung.