DE LEGA LATA Jurnal Ilmu Hukum
Volume 10 Nomor 2, July-December 2025
E-ISSN: 2477-7889 I ISSN: 2477-653X I Akreditasi: SINTA 3, SK No: 28/E/KPT/2019
http://jurnal.umsu.ac.id/index.php/delegalata

Legal Protection Of Cybercrime Crimes From Ransomware Attacks And Evaluation Of The Cyber Security And Resilience Bill 2025 In Indonesia'S Defense

Seri Mughni Sulubara[1], **Virdyra Tasril**[2], **Nurkhalisah**[3]
[1,3]Fakultas Hukum Universitas Muhammadiyah Mahakarya Aceh, Indonesia
[2] Software Engineering Technology Program Politeknik Negeri Medan
Email: serimughni@ummah.ac.id (Corresponding Author)

Accepted: 15-06-2025. Revised: 16-06-2025 Approved: 09-07-2025 Published: 11-06-2025
DOI: 10.30596/dll.v10i2.25786

How to cite:
Sulubara, S M. (2025). "Legal Protection Of Cybercrime Crimes From Ransomware Attacks And Evaluation Of The Cyber Security And Resilience Bill 2025 In Indonesia'S Defense", De Lega Lata: Jurnal Ilmu Hukum, Volume 10 (2): p. 287-297

Abstract

The legal safeguarding against ransomware cybercrime is found in multiple regulations. Indonesia possesses various legal frameworks to combat cybercrime, such as the Electronic Information and Transaction Law (UU ITE), the Personal Data Protection Law (UU PDP), and the Criminal Code (KUHP). Ransomware is a type of harmful software. Ransomware locks a user's data within a computer network, preventing an individual or business from accessing their information. Hackers subsequently extort the victim for a ransom to allow the data owner to regain access to the data. Usually, the payment of the ransom is conducted through cryptocurrency to ensure it remains untraceable. The research methodology, or a means to reach the objectives outlined in the study, employs a qualitative descriptive approach grounded in juridical or normative legal research. This method aims to assess how well the 2025 cyber security and resilience bill can enhance Indonesia's digital defense. The ITE law establishes a legal framework for prosecuting cyber offenders, including ransomware, but it lacks detailed regulations regarding the terminology and methods of ransomware. This creates difficulties in law enforcement, particularly in demonstrating criminal aspects and gathering electronic evidence. Law number 27 of 2022 regarding personal data protection (PDP LAW) establishes a robust legal structure to safeguard personal data from abuse, particularly in relation to ransomware offenses that frequently involve data theft and manipulation. Article 368 of the criminal code concerning conventional extortion can be utilized in ransomware situations, despite not explicitly addressing the digital format. Article 368 of the criminal code addresses the crime of conventional extortion applicable to ransomware incidents, even if it doesn't specifically cover the digital format. The cybersecurity and resilience bill of 2025 aims to enhance Indonesia's cyber defense, emphasizing the protection of cyberspace and the national digital ecosystem. In this regard, the cybersecurity and resilience bill (RUU KKS) 2025 represents a vital measure for the government to bolster national cyber defense. This legislation is intended to outline the responsibilities of various parties in ensuring cybersecurity, set incident reporting requirements, and impose severe penalties for breaches, including prison terms of up to 20 years and fines reaching Rp20 billion.

Keywords: Legal Protection, Cybercrime Crimes, Ransomware Attacks, Cyber Security, Resilience Bill 2025 In Indonesia's Defense.

INTRODUCTION

The legal safeguarding of ransomware cybercrime is found within different regulations. (Bhunia et al., 2025). The legal safeguards are outlined in the Criminal Code, ITE Law, and National Defense Law (Wissink et al., 2023). This is carried out in Indonesia's defense initiatives in line with Article 30 of the 1945 Constitution (Makhortykh et al., 2024). The advancement of information technology in Indonesia has greatly influenced multiple facets of life, including the security of the nation. Amid swift digital change, the risk of cybercrime particularly ransomware attacks has emerged as a significant challenge for the nation. Ransomware represents a type of cybercrime that operates by compromising a computer system, encrypting the victim's information, and subsequently requiring a ransom to regain access to the information. The effect of this assault extends beyond financial loss; it may lead to the leakage and improper use of personal information and jeopardize the stability of the national digital framework (Gruber et al., 2022).

Cybercrime refers to unlawful activities that employ computer technologies or internet networks (Tubaishat & Alaleeli, 2024) Ransomware is a model of malicious software (malware) (Alzakari et al., 2025). Ransomware encrypts a person's data in a computer network causing a person or company to be unable to access the data (Onwuadiamu, 2025a). Hackers then blackmail the victim for a ransom so that the data owner can access the data again (Botchkovar et al., 2025). Typically, the ransom is paid using cryptocurrency to make it untraceable (Wright & Kumar, 2023). Indonesia possesses multiple legal frameworks to combat cybercrime, such as the Electronic Information and Transaction Law (UU ITE), the Personal Data Protection Law (UU PDP), and the Criminal Code (KUHP). The ITE Law governs illegal activities in cyberspace, such as ransomware extortion, whereas the PDP Law offers a broader legal structure for personal data protection, incorporating criminal penalties and fines for breaches concerning unlawful data collection and utilization. Nevertheless, the efficacy of current regulations encounters obstacles, particularly regarding law enforcement and the all encompassing protection of ransomware attack victims (Djenna et al., 2024). Cybercrime involves hacking, unauthorized data access, fraud, and the distribution of malware (Grimberg et al., 2021). Cybercrime can inflict damage on the involved parties (Onwuadiamu, 2025b). Cybercrime refers to unlawful activities that take place in the digital realm, targeting computer networks (Tariq, 2024). Cybercrime can affect anyone, from individuals and businesses to government entities and entire nations.

Legal safeguards against ransomware and enhancing regulations through the PSC Bill are vital for constructing Indonesia's digital security. Cyberattacks aimed at personal information, critical infrastructure, and government systems can jeopardize national security and sovereignty. Consequently, prevention initiatives, incident management, and rigorous law enforcement are essential for establishing a secure and robust digital environment. The presence of the KKS Bill aims for Indonesia to obtain a thorough legal framework to address cyber threats, enhance inter-sector cooperation, and boost the capability of national digital security in response to the changing nature of global threats (Botchkovar et al., 2025). In order to enhance

legal safeguards in the digital age, the Indonesian government is preparing the Cyber Security and Resilience Bill 2025 (Achuthan et al., 2025). This legislation seeks to enhance the safeguarding of the nation's cyberspace, outline the responsibilities and duties of different organizations in ensuring cybersecurity, and impose severe penalties for breaches, including written reprimands, imprisonment, and hefty fines. The KKS Bill is anticipated to establish a legal framework that is more flexible and reactive to the evolving nature of cyber threats, particularly ransomware, while enhancing national cyber resilience against the rising complexity and organization of attacks (Rahmath Nisha & Muthurajkumar, 2023).

The danger of ransomware impacts not just individuals or businesses, but can also pose a risk to national interests, affecting critical areas like finance, energy, and government. Consequently, assessing the efficacy of current regulations and the preparedness of the PSC Bill is crucial for enhancing Indonesia's cyber security. By establishing a robust legal framework and ensuring effective implementation, Indonesia can enhance digital resilience and safeguard state sovereignty in the cyber age. Ransomware damages victims by preventing access to crucial information or systems of an individual, organization, or government until the ransom is settled. Therefore, legal safeguards against cybercrime, particularly ransomware incidents, and assessment of the Cyber Security and Resilience Bill 2025 are crucial aspects in enhancing national defense and security in the digital age. In Law Number 3 of 2002 regarding State Defense, it states that the difficulties and challenges in Indonesia's national defense framework consist of military threats as well as non-military threats, such as cybercrime.

METHOD RESEARCH

The research method or approach to attain the outlined objectives employs a qualitative descriptive technique rooted in juridical or normative legal research (Soekanto, 2019). Juridical or normative legal research emphasizes positive legal norms represented by laws and regulations as the primary or main legal sources (Zainuddin & Karina, 2023). Performing qualitative descriptive analysis of ransomware incidents in Indonesia and examining the legal protections in place. The normative legal approach emphasizes the examination of legal occurrences linked to pertinent statutes, including the Criminal Code, Law Number: 11 of 2008 on Electronic Information and Transactions (ITE), Law Number: 3 of 2002 on State Defense, and the Cyber Security and Resilience Bill 2025. This method seeks to examine the legal safeguards available for ransomware victims and how these laws and regulations can be enacted effectively, thoroughly, and in a cooperative manner. This method aims to assess how effectively the Cyber Security and Resilience Bill 2025 can enhance Indonesia's digital security (Sumarna & Kadriah, 2023).

Article 368 of the Criminal Code concerning conventional extortion may be applicable to ransomware situations, even though it does not specifically address the digital method. Article 368 of the Criminal Code addresses the offense of conventional extortion, which is applicable to ransomware incidents despite the lack of specific regulation for the digital format. The Cyber Security and Resilience Bill 2025 aims to enhance Indonesia's cyber protection, concentrating on safeguarding cyberspace and the national digital environment. In this context, the Cybersecurity and Resilience Bill (RUU KKS) 2025 represents a vital measure for the government to enhance national cyber defense. This legislation aims to oversee the functions and duties of multiple organizations in safeguarding cybersecurity, create requirements for incident reporting, and enforce severe penalties for breaches, including imprisonment for as long as 20 years and fines reaching Rp20 billion.

DISCUSSION

1. Legal Framework for Legal Protection to Handle Ransomware Crimes

Ransomware, as a form of cybercrime, is addressed in Article 368 Paragraph (1) of the Criminal Code concerning extortion, prescribing a prison term of up to 9 years (Hussain et al., 2024). Article 27 Paragraph (4) of the ITE Law expressly makes it a crime to distribute content that includes extortion or threats via electronic methods, punishable by a prison term of up to 6 years (Luuk et al., 2023). The Criminal Code and ITE Law govern the legal protection of cybercrime offenses (Ferretti, 2025). Nevertheless, the enforcement of laws regarding cybercrime has not been applied due to the transnational and international nature of cybercrime (Chimmanee & Jantavongso, 2024). Victims remain at risk of data leakage after paying ransom due to the lack of comprehensive regulations on personal data protection.

Ransomware attacks in today's digital age pose a challenge as they encrypt critical data, compelling victims to pay ransom. Subsequently, the Cyber Security and Resilience Bill 2025 and its execution are scheduled. The legislation is an essential strategy required to safeguard Indonesia in the digital age (Sulubara, 2024b). The assessment of this bill is conducted in the National Legislation Program. The government demonstrated considerable focus on tackling intricate cybercrim.(Onwuadiamu, 2025b) This legislation is a vital matter for legal safeguards against ransomware offenses in the realm of Indonesia's defense (Arroyabe et al., 2024).

The assessment of the Cyber Security and Resilience Bill 2025 is a joint initiative and demonstrates the government's forward movement in addressing the rising cybercrime (A Yassa et al., 2023). The benefits of this legislation offer actual penalties for cybercrime perpetrators, enforcing prison sentences of 2 to 20 years. The enhancement of the Cyber Security and Resilience Bill 2025 is anticipated to decrease ransomware attacks by 45% in 2026, addressing cybercrime effectively. The execution of simulations conducted by the National Cyber and Crypto Agency (BSSN) has the potential to elevate Indonesia's cybercrime defense index ranking from 24th to 15th in ASEAN, consequently boosting technology investments valued at IDR 45 trillion by enhancing investor trust in digital enterprises (Sulubara, 2024a). The effectiveness of this legislation hinges on a dedicated budget allocation of no less than 2% of the state budget for the cyber sector and a regular assessment process every 6 months (Oh et al., 2024). Collaborative and suitable regulations among the Criminal Code, ITE Law, National Defense Law, and the Cyber Security and Resilience Bill 2025 can effectively safeguard essential infrastructure. This concerns Indonesia's defense, which includes creating a National Cyber Defense agency to address cybercrime challenges (Sulubara, 2021).

Collaboration with the Ministry of Communication and Information, the Ministry of Defense, and the TNI is essential to safeguard integrated and comprehensive cyber security in enhancing Indonesia's defense in the digital age. This aligns with the directive of Article 30 of the 1945 Constitution (Sulubara, 2023). This article requires citizens to engage in efforts for national defense and security (Mughni & Prayetno, 2023). The necessity for an assessment of the Cyber Security and Resilience Bill 2025 is crucial for its efficacy in addressing cybercrime, particularly ransomware, which poses a threat to Indonesia's defense. Technological progress contributes to the rise of digital crime. Comprehensive, anticipatory, repressive, and collaborative legal protection is necessary (Dib et al., 2024). An approach is required for the Criminal Code, ITE Law, and National Defense Law, along with the 2025 Cyber Security and Resilience Bill. Indonesia presently depends on three key tools to address ransomware offenses: Law Number 11/2008 on Electronic Information and Transactions (UU ITE)

The ITE Law establishes a legal framework for prosecuting cyber offenders, such as those involved in ransomware, even though it does not specifically address the terminology and mechanisms of ransomware comprehensively. This creates difficulties for law enforcement, particularly in demonstrating criminal elements and gathering electronic evidence.

Furthermore, the administration via the National Cyber and Crypto Agency (BSSN) highlighted the stance of refusing ransom payments and prioritizing the restoration of services along with forensic inquiries to pinpoint culprits and avert comparable attacks moving forward. Therefore, the ITE Law serves as the primary legal framework for addressing ransomware offenses in Indonesia, though there remains a necessity to enhance and align regulations for improved effectiveness against advancing cyber threats. The regulations governing ransomware attacks are (Unson & Zhuang, 2025):

a. Article 27 paragraph (4) of the ITE Law defines ransomware as a form of cyber extortion, subject to a prison sentence of a maximum of 6 years and/or a fine of Rp1 billion.
b. Article 27B section (1): Governs the offense of extortion using electronic information or electronic documents. Ransomware is classified as extortion since the offender deliberately transmits or distributes electronic information unlawfully to gain benefits for themselves or others, while coercing the victim by threatening violence to obtain something, such as a ransom. The aspect of extortion in this text is closely linked to the methods used in ransomware, even though the word "ransomware" is not directly referenced.
c. Artikel 30 Absatz (2) jo. Article 46 paragraph (2): Governs unauthorized access to computers or electronic systems to acquire electronic information or documents. Individuals who engage in ransomware attacks by infiltrating victims' systems to encrypt files may face charges under this article, potentially resulting in incarceration for up to 7 years and/or a fine reaching Rp700 million.
d. Artikel 32 ayat (1) jo. Article 48 paragraph (1): Governs the alteration, destruction, removal, or concealment of electronic information or electronic documents that belong to someone else.

Criminal Code (KUHP)

Article 368 of the Criminal Code regarding conventional extortion can be utilized in ransomware incidents, even though it does not explicitly address the digital format. Article 368 of the Criminal Code governs the offense of traditional extortion, which can be relevant to ransomware incidents even though it does not explicitly address the online method. This article indicates that (Gaber et al., 2024).

> *"Any person who, with intent to unlawfully benefit himself or another, forces a person by force or threat of force to give property wholly or partially belonging to that person or to another, or to incur a debt or to cancel a debt, shall, being guilty of extortion, be punished by a maximum imprisonment of 9 years".*

The elements that must be met in order for an act to be qualified as extortion according to Article 368 of the Criminal Code include (Kwon et al., 2024):

a. The intent to unlawfully benefit oneself or others.
b. The coercion is carried out by physical violence or threat of violence, including psychological violence that causes fear to the victim.
c. The coercion aims to make the victim give something, create a debt, or write off a debt that is detrimental to the victim.

In ransomware scenarios, the offender unlawfully compels the victim through intimidation (i.e. encrypts the information and threatens not to restore it unless a ransom is paid), thus it qualifies as a type of extortion fulfilling the criteria of Article 368 of the Criminal Code. Nonetheless, since this article was designed for traditional extortion, its relevance to cybercrimes like ransomware demands flexible interpretation by law enforcement agencies. The prescribed criminal penalties are notably harsh, specifically a maximum incarceration term of 9 years, which offers a legal foundation to capture ransomware offenders. The primary difficulty lies in demonstrating the presence of violence or threats in the digital space and

pinpointing offenders who frequently employ anonymity methods. Consequently, Article 368 of the Criminal Code serves as a crucial legal tool for addressing ransomware in Indonesia, although it requires backing from specific regulations and digital forensic technology to ensure effective law enforcement (Kim et al., 2025).

2. Personal Data Protection Law (PDP Law) in Handling Ransomware Cybercrime in Indonesia

The PDP Law mandates that personal data controllers must issue a written notice to data subjects and pertinent institutions within 3x24 hours following a personal data breach or leak, including incidents caused by ransomware attacks. These stringent sanctions seek to create a deterrent impact on cyber criminals who exploit personal information. Nonetheless, the implementation of criminal penalties in UU PDP continues to encounter obstacles, particularly regarding evidence and efficient law enforcement in practice (Hossain et al., 2025). The PDP Law enhances legal safeguards against ransomware offenses by targeting offenders involved in unlawful data gathering and data manipulation, thus serving as a crucial tool in the pursuit of national cyber security and resilience. Law No. 27 Year 2022 regarding Personal Data Protection (PDP Law) offers a robust legal structure to safeguard personal data against misuse, particularly concerning ransomware offenses that frequently entail data theft and manipulation. Beberapa ketentuan penting dalam UU PDP yang berkaitan dengan sanksi pidana adalah sebagai berikut (Oh et al., 2024):

a. Article 67 of the PDP Law states that anyone who willfully and illegally acquires or gathers personal data not belonging to them for personal gain or for others, potentially causing harm to the data owner, shall face imprisonment for a maximum of 5 years and/or a fine of up to Rp5 billion.
b. Article 68 of the PDP Law states that anyone who deliberately produces false personal data or alters personal data to gain an advantage for themselves or others, potentially causing harm to others, shall face imprisonment for up to 6 years and/or a maximum fine of Rp6 billion.
c. Alongside the primary criminal penalties, the PDP Law also governs supplementary sanctions such as the seizure of profits and/or assets derived from criminal activities and the obligation to compensate victims.

3. Evaluation of the Cyber Security and Resilience (CSR) 2025 Bill

The Cyber Security and Resilience Bill 2025 aims to enhance Indonesia's cyber defenses by prioritizing the protection of cyberspace and the national digital environment. The legislation seeks to safeguard essential national infrastructure like the energy, telecommunications, transportation, and financial industries, which are extremely susceptible to cyberattacks, including ransomware. It also governs the overall management of cyber incidents from prevention and mitigation to recovery, thereby enhancing national digital resilience. The legislation mandates that Information Infrastructure Providers (IIPs) and Critical IIPs must adopt rigorous cybersecurity protocols, which include the requirement to report cyber incidents within a designated timeframe. This establishes a clear guideline for both public and private organizations in ensuring the safety of electronic systems and information (Afraji et al., 2025).

The bill’s penalties are quite severe, imposing prison terms ranging from 2 to 20 years and fines that may go up to Rp20 billion for breaches of cybersecurity requirements. This demonstrates the government's commitment to combatting cyber criminals and organizations that are careless in upholding cyber security. The legislation further promotes partnership among the government, private industry, and the public to enhance awareness and understanding of digital security, a crucial element in addressing emerging cyber threats.

Moreover, the legislation is anticipated to unify multiple cybersecurity initiatives that have been dispersed across different sectors.

Though the PSC Bill offers a thorough legal structure, the primary difficulty is in its execution and alignment with current regulations like the ITE Law and PDP Law. For this regulation to be practically effective, the government must guarantee coordination among agencies and enhance the skills of human resources in cybersecurity. By ratifying the Cybersecurity Bill, Indonesia will mirror the actions of ASEAN nations like Singapore and Malaysia, which possess robust cybersecurity legal structures, thereby enhancing Indonesia's role in regional cybersecurity governance. The Cyber Security and Resilience Bill 2025 represents a crucial strategic move to bolster Indonesia's national cyber defense. This regulation not only offers more defined legal safeguards against cyber threats like ransomware but also enhances collaboration among stakeholders in ensuring the security of the digital realm, which is becoming increasingly crucial for the nation's survival. Below are several instances of ransomware incidents that have taken place in Indonesia:

a. Bank Syariah Indonesia (BSI), Mei 2023. The LockBit 3.0 ransomware assault effectively hijacked BSI's systems and exfiltrated around 1.5 terabytes of data related to customers and employees, comprising loan details and internal files. The group responsible for the crime demanded a ransom exceeding IDR 200 billion. BSI opted to prioritize system restoration without submitting to the ransom and safeguarding against any data exposure to the public.
b. Centro Nacional de Datos Temporal 2 (PDNS 2), junio de 2024. A variant of Brain Cipher (derivative of LockBit 3.0) ransomware affected PDNS 2 servers, leading to service interruptions at 210 central and regional agencies, among them the Directorate General of Immigration. The assailant requested a ransom of US$8 million, but the authorities declined to pay and initiated an investigation and system recovery.
c. Bank Rakyat Indonesia (BRI), Desember 2024. Reportedly fell victim to the Bashe ransomware attack that effectively breached the system and compromised sensitive information. Specific details about the compromised data have not been released yet.
d. Dharmais Hospital and Harapan Kita Hospital, May 2017. Both hospitals were affected by the WannaCry ransomware attack, which interrupted services such as medical records and patient administration. RS Dharmais also paid a ransom in Bitcoin totaling approximately 200 million rupiah to retrieve the data.
e. These instances demonstrate that ransomware attacks in Indonesia have affected numerous critical sectors, including banking, government entities, and healthcare facilities, leading to substantial consequences for services and data protection. Ransomware attacks can devastate business operations, lead to significant financial damages, and negatively impact a company’s reputation. Numerous companies' security and prevention strategies remain inadequate as they fail to fully grasp these concerns. Ultimately, ransomware incidents in Indonesia reveal considerable vulnerabilities in the nation's digital systems and necessitate enhanced preparedness and stronger legal protections to ensure data security, continuous public service delivery, and vital national operations.

The Cyber Security and Resilience Act 2025 is essential for Indonesia in addressing the difficulties of a rapidly evolving and hazardous digital age. This regulation aims to safeguard the nation's essential infrastructure, including energy, transportation, telecommunications, and financial sectors, which underpin the economy and security of the country. Cyberattacks targeting these sectors can disrupt the nation's functions and result in far-reaching effects on society. The enactment of the Cyber Security and Resilience Law 2025 is a crucial and timely measure to enhance Indonesia's digital security, safeguard national interests, and create a secure, reliable, and competitive digital environment on a global scale.

Conclusion

A recommendation is necessary to enhance current regulations among the Criminal Code, ITE Law, and the National Defense Law, along with an assessment of the Cyber Security and Resilience Bill 2025, to be more effective in combating cybercrime, particularly ransomware. The enforcement of legal protection against ransomware cybercrime is crucial, as this form of crime is a damaging, prevalent, and organized issue in Indonesia's digital landscape. A new element is anticipated to ensure the bill transforms into the Cyber Security and Resilience Law to enhance Indonesia's digital security.

Ransomware incidents, a type of cybercrime, pose a significant risk to Indonesia's digital safety and national stability. This offense not only results in substantial financial damage but also endangers data integrity and the ongoing functionality of essential infrastructure. Indonesia presently depends on various legal frameworks including the Electronic Information and Transactions Law (ITE Law), the Criminal Code (KUHP), and the Personal Data Protection Law (PDP Law) to ensure legal safeguards against ransomware assaults. Nonetheless, the intricacy and changing nature of cyber threats require more thorough and flexible regulations.

In this regard, the Cybersecurity and Resilience Bill (RUU KKS) 2025 represents a crucial initiative for the government to bolster national cyber defense. This legislation aims to govern the duties and functions of different organizations in safeguarding cybersecurity, set requirements for incident reporting, and enforce harsh penalties for breaches, with prison terms reaching 20 years and fines up to Rp20 billion. By prioritizing the safeguarding of national critical infrastructure and improving cooperation among the government, private sector, and community, the KKS Bill aims to establish a safer and more robust digital environment. The approval and enforcement of the KKS Bill will elevate Indonesia to the level of other ASEAN nations with robust cybersecurity laws, while simultaneously enhancing national defenses against ransomware risks and various cybercrimes. Consequently, the 2025 KKS Bill serves as a crucial basis for establishing a robust cyber defense, safeguarding data and digital infrastructures, and upholding national sovereignty in an era of rapid digital transformation.

REFERENCES

A Yassa, H., N Zakaria, R., & Z Abdellah, N. (2023). COVID-19 Pandemic Fuels Rise in Cybercrime. *Journal of Information Security and Cybercrimes Research*, *6*(1), 01–10. https://doi.org/10.26735/kuxw6317

Achuthan, K., Khobragade, S., & Kowalski, R. (2025). Cybercrime through the public lens: a longitudinal analysis. *Humanities and Social Sciences Communications*, 1–16. https://doi.org/10.1057/s41599-025-04459-x

Afraji, D. M. A. A., Lloret, J., & Peñalver, L. (2025). Deep learning-driven defense strategies for mitigating DDoS attacks in cloud computing environments. *Cyber Security and Applications*, *3*(September 2024), 100085. https://doi.org/10.1016/j.csa.2025.100085

Alzakari, S. A., Aljebreen, M., Ahmad, N., Alhashmi, A. A., Alahmari, S., Alrusaini, O., Al-Sharafi, A. M., & Almukadi, W. S. (2025). An intelligent ransomware based cyberthreat detection model using multi head attention-based recurrent neural networks with optimization algorithm in IoT environment. *Scientific Reports*, *15*(1), 1–21. https://doi.org/10.1038/s41598-025-92711-4

Arroyabe, M. F., Arranz, C. F. A., De Arroyabe, I. F., & de Arroyabe, J. C. F. (2024). Revealing the realities of cybercrime in small and medium enterprises: Understanding fear and taxonomic perspectives. *Computers and Security*, *141*(February), 103826. https://doi.org/10.1016/j.cose.2024.103826

Bhunia, S., Blackert, M., Deal, H., DePero, A., & Patra, A. (2025). Analyzing the 2021 Kaseya Ransomware Attack: Combined Spearphishing Through SonicWall SSLVPN Vulnerability. *IET Information Security*, *2025*(1). https://doi.org/10.1049/ise2/1655307

Botchkovar, E., Cui, K., Antonaccio, O., Perkins, R., & Maimon, D. (2025). Technology in Society The organized activities of ransomware groups : A social network approach. *Technology in Society*, *82*(February), 102873. https://doi.org/10.1016/j.techsoc.2025.102873

Chimmanee, K., & Jantavongso, S. (2024). Digital forensic of Maze ransomware: A case of electricity distributor enterprise in ASEAN. *Expert Systems with Applications*, *249*(PB), 123652. https://doi.org/10.1016/j.eswa.2024.123652

Dib, O., Nan, Z., & Liu, J. (2024). Machine learning-based ransomware classification of Bitcoin transactions. *Journal of King Saud University - Computer and Information Sciences*, *36*(1), 101925. https://doi.org/10.1016/j.jksuci.2024.101925

Djenna, A., Belaoued, M., Lifa, N., & Moualdi, D. E. (2024). PARCA: Proactive Anti-Ransomware Cybersecurity Approach. *Procedia Computer Science*, *238*, 821–826. https://doi.org/10.1016/j.procs.2024.06.098

Ferretti, G. (2025). A World Shaped by Computer Technologies: For a Hermeneutic Analysis of Computer Protocols. *Digital Studies/ Le Champ Numerique*, *15*(1), 1–22. https://doi.org/10.16995/dscn.11066

Gaber, M., Ahmed, M., & Janicke, H. (2024). Zero Day Ransomware Detection with Pulse: Function Classification with Transformer Models and Assembly Language. *Computers & Security*, *148*(August 2024), 104167. https://doi.org/10.1016/j.cose.2024.104167

Grimberg, F., Asprion, P. M., Schneider, B., Miho, E., Babrak, L., & Habbabeh, A. (2021). The Real-World Data Challenges Radar: A Review on the Challenges and Risks regarding the Use of Real-World Data. *Digital Biomarkers*, *5*(2), 148–157. https://doi.org/10.1159/000516178

Gruber, J., Voigt, L. L., Benenson, Z., & Freiling, F. C. (2022). Foundations of cybercriminalistics: From general process models to case-specific concretizations in cybercrime investigations. *Forensic Science International: Digital Investigation*, *43*, 301438. https://doi.org/10.1016/j.fsidi.2022.301438

Hossain, M. A., Hasan, T., Ahmed, F., Cheragee, S. H., Kanchan, M. H., & Haque, M. A. (2025). Towards superior android ransomware detection: An ensemble machine learning perspective. *Cyber Security and Applications*, *3*(July 2024), 100076. https://doi.org/10.1016/j.csa.2024.100076

Hussain, A., Saadia, A., Alhussein, M., Gul, A., & Aurangzeb, K. (2024). Enhancing ransomware defense: deep learning-based detection and family-wise classification of evolving threats. *PeerJ Computer Science*, *10*, 1–44. https://doi.org/10.7717/peerj-cs.2546

Kim, K., Lee, S., Ramachandran, S., & Alzahrani, I. (2025). Cryptocurrency-driven ransomware syndicates operating on the darknet : A focused examination of the Arab world. *Egyptian Informatics Journal*, *30*(January), 100665. https://doi.org/10.1016/j.eij.2025.100665

Kwon, D., Borrion, H., & Wortley, R. (2024). Measuring Cybercrime in Calls for Police Service. *Asian Journal of Criminology*, *19*(3), 329–351. https://doi.org/10.1007/s11417-024-09432-2.

Law No. 3 of 2002 on State Defense.

Law Number 27 of 2022 on the Protection of Personal Data (UU PDP), and Law No. 3 of 2002 on State Defense.

Law Number: 1 Year 2024 on the Second Amendment to Law Number: 11 Year 2008 on Electronic Information and Transactions.

Luuk, B., (Maria) Susanne, V. H. de G., Ellen, M. ter H., Ynze, V. H., Remco, S., & Eric Rutger, L. (2023). Protecting your business against ransomware attacks? Explaining the motivations of entrepreneurs to take future protective measures against cybercrimes using an extended protection motivation theory model. *Computers and Security*, *127*, 103099. https://doi.org/10.1016/j.cose.2023.103099

Makhortykh, M., Sydorova, M., Baghumyan, A., Vziatysheva, V., & Kuznetsova, E. (2024). Stochastic lies: How LLM-powered chatbots deal with Russian disinformation about the war in Ukraine. *Harvard Kennedy School Misinformation Review*, *5*(4), 1–21. https://doi.org/10.37016/mr-2020-154

Mughni, S., & Prayetno, B. E. (2023). Cakrawala : Jurnal Pengabdian Masyarakat Global Mengetahui Aturan Hukum dengan Menghafal Naskah Pembukaan UUD 1945 dan Pasal- Pasal UUD 1945 Secara Tekstual dan Mengetahui Makna yang Tekandung di Dalamnya Bagi Siswa-Siswi IPA-IPS SMA Negeri 7 Takengon Kno. *Cakrawala: Jurnal Pengabdian Masyarakat Global*, *2*(4). https://doi.org/https://doi.org/10.30640/cakrawala.v2i4.1758

Oh, D. Bin, Kim, D., & Kim, H. K. (2024). volGPT: Evaluation on triaging ransomware process in memory forensics with Large Language Model. *Forensic Science International: Digital Investigation*, *49*(S), 301756. https://doi.org/10.1016/j.fsidi.2024.301756

Onwuadiamu, G. (2025a). Cybercrime in criminology; A systematic review of criminological theories, methods, and concepts. *Journal of Economic Criminology*, *8*(February), 100136. https://doi.org/10.1016/j.jeconc.2025.100136

Onwuadiamu, G. (2025b). Cybercrime in criminology; A systematic review of criminological theories, methods, and concepts. *Journal of Economic Criminology*, *8*(December 2024), 100136. https://doi.org/10.1016/j.jeconc.2025.100136

Rahmath Nisha, S., & Muthurajkumar, S. (2023). Semantic Graph Based Convolutional Neural Network for Spam e-mail Classification in Cybercrime Applications. *International Journal of Computers, Communications and Control*, *18*(1), 1–12. https://doi.org/10.15837/ijccc.2023.1.4478

Soekanto, S. (2019). Penelitian Hukum Normatif. *Hukum*, *1*(1), 4.

Sudjito, B., Majid, A., Sulistio, F., & Ruslijanto, P. A. (2016). Tindak Pidana Pornografi dalam Era Siber di Indonesia. *Wacana, Jurnal Sosial Dan Humaniora*, *19*(02), 66–72. https://doi.org/10.21776/ub.wacana.2016.019.02.1

Sulubara, S. M. (2021). Pemahaman Constitusional System of Indonesia (UUD) 1945 Understanding. *Sejahtera: Jurnal Inspirasi Mengabdi Untuk Negeri*, *48*(2), 39–62. https://doi.org/https://doi.org/10.58192/sejahtera.v3i3.2356

Sulubara, S. M. (2023). Gen Z Wajib Tau! Edukasi dan Penguatan Pasal-Pasal UUD 1945 bagi Generasi Z (Pasca Milenal) bagi Siswa-Siswi SMA Negeri 4 Takengon. *Karunia: Jurnal Hasil Pengabdian Masyarakat Indonesia*, *01*(4), 1–23. https://doi.org/https://doi.org/10.58192/karunia.v2i4.1552

Sulubara, S. M. (2024a). Menyajikan Berbagai Insiden Cybercrime yang Terjadi di Indonesia , Termasuk Pencurian Data dan Peretasan Situs Web Pemerintah. *Konsensus: Jurnal Ilmu Politik Dan Komunikasi*, *1*(6), 199–206. https://doi.org/https://doi.org/10.62383/konsensus.v1i6.692

Sulubara, S. M. (2024b). Perlindungan Data Pribadi dalam Kasus Ransomware : Apa Kata Hukum ? *Eksekusi: Jurnal Ilmu Hukum Dan Administrasi Negara*, *2*(4), 426–434. https://doi.org/DOI: https://doi.org/10.55606/eksekusi.v2i4.1823

Sumarna, D., & Kadriah, A. (2023). Penelitian Kualitatif Terhadap Hukum Empiris. *Jurnal Penelitian Serambi Hukum*, *16*(02), 101–113. https://doi.org/10.59582/sh.v16i02.730

Tariq, U. (2024). Combatting ransomware in ZephyrOS-activated industrial IoT environments. *Heliyon*, *10*(9), e29917. https://doi.org/10.1016/j.heliyon.2024.e29917

Tubaishat, A., & Alaleeli, H. (2024). A Framework to Prevent Cybercrime in the UAE. *Procedia Computer Science*, *238*, 558–565. https://doi.org/10.1016/j.procs.2024.06.060

Unson, I., & Zhuang, J. (2025). Resource allocation in multi-layer, continuous defense, security games versus strategic attackers. *Risk Sciences*, *1*(December 2024), 100010. https://doi.org/10.1016/j.risk.2024.100010

Wissink, I. B., Standaert, J. C. A., Stams, G. J. J. M., Asscher, J. J., & Assink, M. (2023). Risk factors for juvenile cybercrime: A meta-analytic review. *Aggression and Violent Behavior*, *70*(March), 101836. https://doi.org/10.1016/j.avb.2023.101836

Wright, D., & Kumar, R. (2023). Assessing the socio-economic impacts of cybercrime. *Societal Impacts*, *1*(1–2), 100013. https://doi.org/10.1016/j.socimp.2023.100013

Zainuddin, M., & Karina, A. D. (2023). Penggunaan Metode Yuridis Normatif dalam Membuktikan Kebenaran pada Penelitian Hukum. *Smart Law Journal*, *2*(2), 114–123. https://journal.unkaha.com/index.php/slj/article/view/26