Global Journal of Law, AI & Ethics (GJLAE)

Journal homepage: https://journals.cognispectra.com/index.php/gjlae/index
Vol. 1, No. 1, August, pp. 26-32
P-ISSN : XXXX-XXXX
E-ISSN : XXXX-XXXX

Legal Impacts of Ransomware Threats to Government Application: Srikandi

Ridho Bawana Jati[1*], Ani Munirah Mohamad[2]

[1] Universitas Muhammadiyah Surakarta
[2] School of Law and Centre for Testing, Measurement and Appraisal (CeTMA), Universiti Utara Malaysia

https://doi.org/xx.xxxxx/gjlae.xxxxxx

ABSTRACT

The ransomware threat affecting Indonesia is a serious one because it has crippled the government's public service platforms and the government's application called SRIKANDI, rendering them temporarily unusable. This ransomware attack also occurred because the government was careless in creating malware (security systems) that was easily breached by malicious hackers, allowing them to damage the operating system and steal data from the public service platform and the SRIKANDI application. The objective of this paper is to analyze the legal implications of ransomware threats on the government application SRIKANDI. The research method used for this writing is the normative method, which emphasizes literature review of previously existing problems and collecting relevant literature according to the issues discussed. The data collection technique for this research uses the library research technique (research library) by gathering relevant theories related to this issue, such as legal journals, books, or existing and relevant research. That in this ransomware attack issue, it has legal consequences for the suspect because it violates Indonesian legal regulations, namely the ITE Law (Electronic Information and Transactions) as stated in Article 32 Paragraph (1), Article 33, Article 48, and Article 49, and its enforcement refers to the Criminal Procedure Code (KUHAP) Article 30 Paragraph (2). The conclusion that can be drawn regarding the problems in this research is that the government is obliged to be vigilant by immediately restoring the operating system that has been hacked and the data stolen so that the Indonesian people can use it again. The government is also obligated to constantly strengthen malware (security systems) that are difficult for malicious hackers to breach, ensuring that the operating systems of government platforms and government-owned applications are always secure.

Keywords: Ransomware, Legal Impact, Malware, SRIKANDI.

Received: 20 June 2025
Revised: 23 June 2025
Accepted: 28 August 2025
Available online: 30 August 2025

Corresponding Author:
Ridho Bawana Jati
E-mail Address : ridhobj9.7@gmail.com

1. INTRODUCTION

In the current era, which is the increasingly advanced digital age, the challenges for digital security are growing. One of the serious threats that the world is concerned about is ransomware attacks. Ransomware is a type of malicious software designed to encrypt or lock access to a victim's system. The ransomware perpetrators then threatened to demand a ransom payment in digital currency for the data or system to be returned to its owner. One of the recent ransomware cases in Indonesia is the data theft from the PDNS (Temporary National Data Center), which completely paralyzed all government service activities and government applications. [1] At that time, the ransomware perpetrators successfully hacked and stole data nationwide, taking a large amount of data from Indonesian citizens. This causes significant discomfort and concern for the Indonesian public.
The recent impact of ransomware has been very serious, as it not only disrupted government services and applications but also reduced the level of trust among Indonesians in those government services and applications. One government application that has been seriously impacted by recent

ransomware attacks is the Srikandi application. The Srikandi application is a general application in the field of archives aimed at electronic-based archive management and governance, targeted for both Central and Regional governments. [2] The threat from ransomware has become very serious in the digital world today. The attack on this device became very dangerous, causing significant losses across various sectors, especially the Srikandi application. Online security heavily relies on 3 (three) important aspects: data protection, preventive measures, and effective security solutions.

The Srikandi application itself was affected when the ransomware attacked Indonesia, causing it to be hindered and even unusable for approximately two weeks. The application should be the central digital hub for Indonesia's national digital archives, issued by ANRI (National Archives of the Republic of Indonesia). This presents new challenges in maintaining the overall security of the system. Solutions for proper security and robust data protection efforts are crucial in the face of this threat.

Against ransomware attacks, being a key factor in combating this threat. Ransomware is often associated with specific criminal groups seeking profit from their criminal activities. [3] Therefore, research in the field of law is important to understand the dynamics, technology, security, and social implications of ransomware. Thru a deep understanding of ransomware and collaborative efforts between security agencies, researchers, and users, effective preventive measures can be taken. These steps include regular software updates, user awareness of ransomware threats and prudent security measures, and regular data backups. [4]

The threat from this ransomware attack is also highly illegal, as it involves demanding a ransom that must be paid immediately by stealing data and damaging the systems of government service applications and the SRIKANDI application itself. This violates the ITE Law Article 33 Paragraph 1 concerning ITE (Information Technology and Electronic) which states that a person intentionally and without rights or against the law by performing an act that results in the electronic system being disrupted and/or an electronic system becoming unusable.

Accordingly, the primary objective of this paper is to analyze the legal implications of ransomware threats to the government application SRIKANDI. This paper addresses the questions of how ransomware attacks affect the SRIKANDI system, with a focus on the SRIKANDI application, followed by what legal rules govern ransomware threats at the international level in general, and the Indonesian level in particular.

This research will examine ransomware attacks, the legal consequences of stealing data from the SRIKANDI government application, and the steps that can be taken to prevent and overcome ransomware attacks. By gaining a deeper understanding of ransomware attacks and making strong efforts to implement robust security policies, individuals and organizations can protect themselves from potential threats in this rapidly evolving digital world.

2. RESEARCH METHODOLOGY

The research method used in this writing is the normative method. In support of this research, the author used a method that emphasized literature review, focusing on previously existing problems and gathering relevant literature to support the discussion of this research. Qualitative methods are research that is descriptive and tends to use inductive analysis. [5] The data collection technique for this research is the literature study technique, which is a technique that involves studying theories from various sources such as legal journals, books, or existing research, relevant to the discussion in this study.

Accordingly, the methodology employed in this study can be summarised in the following **Table 1**.

Table 1. Overview of methodology for the study

Dimension	Method employed	Purpose
Research approach	Normative	This approach is ideal when the research aims to evaluate, interpret, or propose legal standards focusing on ransomware threats
Data source	Library-based	This method is appropriate for doctrinal or normative legal research, which relies heavily on existing legal materials
Data	Secondary sources such as written laws, cases, textbooks, journal articles and past research	These sources are crucial for understanding how the laws are applied, enforced, and perceived in practice

The authors believe that the methodology employed in this study are adequate and appropriate for the purpose of answering the research questions and achieving the research objective of the study.

3. RESEARCH RESULTS AND DISCUSSION

3.1 Understanding Ransomware

Ransomware is a malicious software (malware) used to encrypt data on computer systems or other devices, threatening victims with a ransom demand for the data to be restored or decrypted. Ransomware typically enters a system thru a suspicious link or attachment in an email, an infected website, or by exploiting vulnerabilities in software or an operating system. [6] Ransomware itself can be a very significant threat because it causes damage to the systems of government application systems and the services provided by the government itself. Some types of ransomware threats also have the ability to spread to other networks within an organization or lock down a system, resulting in very severe consequences.

3.2 Ransomware Events

The ransomware incident itself has occurred in the world, as explained below:

1) WannaCry: In 2017, the WannaCry ransomware attack targeted thousands of organizations

worldwide. The ransomware exploits vulnerabilities in unpatched Windows operating systems and spreads rapidly thru networks. The attack encrypted data and demanded a ransom payment in Bitcoin.[7]
2) NotPetya: In 2017, the NotPetya ransomware attack occurred, targeting large companies worldwide and originating in Ukraine. NotPetya used the same method as Wannacry, which is exploiting system vulnerabilities in the Windows operating system. However, NotPetya was more like a destructive attack than an extortion attempt, as it did not provide any description after the ransom payment.
3) GandCrab: This ransomware attacked in 2018 and 2019. This ransomware spreads thru spam emails and exploit kits. GandCrab encrypts victim data and demands ransom payments in cryptocurrency. In this case, the GandCrab operation was shut down after security researchers successfully cracked its encryption algorithm. However, the ransomware had already caused significant financial losses. [8]
4) Ryuk: Ransomware Ryuk first attacked in 2018, targeting the financial and healthcare sectors. These attacks typically began with an initial infection using the Emotet or Trickbot Trojan. Ryuk then encrypted data and demanded a very large ransom payment in Bitcoin. [9]
5)REvil/Sodinokibi: REvil or Sodinokibi ransomware is a ransomware family active since 2019. This attack often targets large companies and IT service providers. REvil encrypts data and demands a ransom in the form of Bitcoin. This ransomware uses the "double extortion" practice, which involves stealing data before encrypting it and threatening to publish it if the ransom is not paid. [10]

3.3 How Ransomware Work

The way ransomware works involves several steps, as follows: first, ransomware enters the victim's system thru suspicious-looking links or attachments in emails, infected websites, or by exploiting vulnerabilities in software or operating systems. Once inside, the ransomware enters thru a strong encryption algorithm, making it inaccessible to the owner. Then, the ransomware displays a ransom message containing instructions for the victim to pay the ransom, usually using Bitcoin, as a condition for obtaining the decryption key that is essential for restoring the data.[11]
An example of how ransomware works could be summarised into the following **Figure 1**.

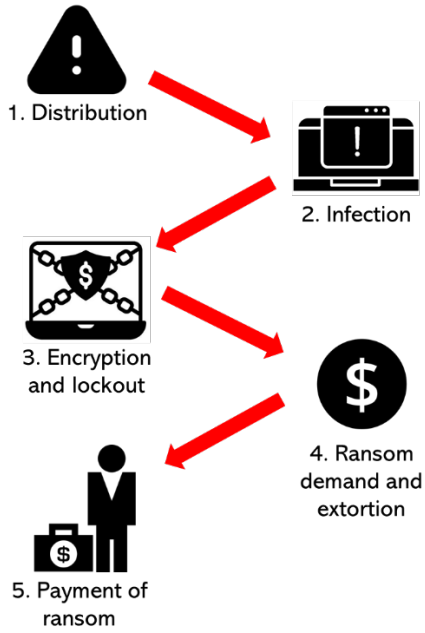

Figure 1. How ransomware works

1) Distribution: Ransomware enters thru several methods, including in links found in phishing emails, infected websites, or by exploiting vulnerabilities in unpatched operating system software. This initial infection often occurs when users are unaware or careless when interacting with malicious content.
2) Infection : Once it can enter the target system, ransomware will spread to other connected devices on the network. This can be done by exploiting vulnerabilities in the system or using methods such as exploiting weak passwords or insecure network configurations..
3) Encryption and lockout : After the ransomware spreads, the next step is to encrypt the data on the target system or device. The ransomware will encrypt the files using a strong encryption algorithm that makes them inaccessible and renders them unusable to their owner. This process can affect various file types, including documents, images, videos, and other important files..
4) Ransom demand and extortion : After encrypting the data, the ransomware will display a message or warning on the victim's screen. This message will inform the victim that their data has been encrypted and demand a ransom payment for the encryption key to be provided. This message usually contains instructions on how to pay the ransom, including paying into a Bitcoin wallet or other instructions.
5) Payment of ransom : Ransomware typically demands ransom payments in the form of cryptocurrencies such as Bitcoin, Ethereum, or Monero. These payments are intended to make transactions difficult to trace and benefit the attackers. However, it's important to note that there is no guaranty that the data can be recovered after the ransom payment is made.

3.4 Ransoware Prevention

Application in preventing ransomware attacks can help individuals and organizations mitigate against ransomware attacks. However, it's still necessary to stay updated on the latest developments in digital security to ensure optimal protection. Preventive measures to reduce ransomware attacks:

1) Back up data regularly: Regularly back up data to a separate and secure location, such as external storage or the cloud. Ensure backups are performed automatically and verified for validity. By doing this, you can have a copy of your data that can be recovered in case of a ransomware attack.
2) Update software and operating systems: Ensure that the operating system, application software, and hardware used are always updated with the latest releases.
3) Use strong security solutions: Install reputable security software, such as antivirus, antispyware, and firewalls. Make sure the software is updated regularly with the latest virus definitions to detect and block ransomware threats.
4) Be wary of suspicious emails and links: Do not click on links or open attachments in emails from unknown or unexpected sources.
5) Use strong and unique passwords: Use complex passwords consisting of a combination of letters, numbers, and special characters.
6) Limit access rights: Grant access rights appropriate for users and user groups. Limit administrator rights to those who need them.
7) Consider firmware updates: In addition to software updates, it's important to update hardware firmware such as routers, switches, and other network devices. Updated firmware can protect hardware from vulnerabilities that ransomware could exploit.
8) Increase user awareness: Provide training and education to users about safe digital security practices. Teach them not to click on suspicious links or open suspicious attachments, and the importance of reporting suspicious activity to the security team.
9) Use firewalls and traffic filters: Enable firewalls on network devices and use traffic filters to restrict access to malicious or suspicious websites that are sources of ransomware.
10) Security monitoring and detection: Implement robust threat monitoring and detection systems to identify and address ransomware attacks as quickly as possible.

3.5 Criminal Offenses Related to Ransomware Attacks

At the international level, there is no specific law that governs ransomware. Nevertheless, there are general rules and treatises that promote criminalisation of attacks against computers and networks, such as the United Nation's Convention against Cybercrime (published in 2024), as well as the Tallinn Manual 2.0 on Nation-State Cyber Operations (published in 2017). Although these two documents are not binding, they offer guidance on applying existing international laws, such as sovereignty and non-intervention, to cyber incidents, including ransomware attacks [12].

Additionally, there are also rules that promote the protection of human rights, such as the United Nation's International Declaration of Human Rights, and the International Human Rights Law. Despite being not binding on the member states, these rules are significant in shaping the development of human rights law in the respective countries. Given that ransomware attacks are oblivious threats to humans and properties, these international set of rules are, to a certain extent, recognise the fundamental rights of persons which should be protected, including right to life, right to economic, social, and cultural rights, as well as right to own and enjoy things [13]. Any acts of ransomware against persons would be considered as threats against the victim's human rights.

Apart from the above, there are other international laws that could also inform the Indonesian legal landscape of ransomware governance. A summary of the laws is produced in the following **Table 2**.

Table 2. International Laws on Ransomware

Name of Law	Relevance to ransomware context
Budapest Convention on Cybercrime (2001)	Covers computer-related offenses including unauthorized access and data interference, applicable to ransomware.
Second Additional Protocol to the Budapest Convention (2023)	Facilitates streamlined procedures for accessing data relevant to ransomware investigations.
Regulation (EU) 2023/1543	Supports legal access to data needed for ransomware case investigations.
Directive (EU) 2022/2555	Mandates risk management and incident reporting, including ransomware threats.
Cybersecurity Act (EU 2019/881)	Promotes secure systems to reduce ransomware vulnerabilities.
NIS Directive (EU 2016/1148)	Requires incident reporting and security measures against ransomware.
Oxford Process on International Law Protections in Cyberspace	Addresses ransomware under principles of sovereignty, due diligence, and non-intervention.

These international laws are relevant to the context of Indonesian legal framework on ransomware threats and cybersecurity, in the sense that they serve as a model for harmonising cybercrime laws and facilitating international cooperation. Although Indonesia is not yet a party to some of the laws (such as the UN Convention against Cybercrime 2024, and Budapest Convention on Cybercrime 2021) it is inspiring to note that the laws might provide guidance on applying international law to ransomware threats. This would be useful for academic and policy development in Indonesia.

In the context of Indonesia, ransomware attacks on computers, whether by the creators or those who spread it, resulting in losses, involve an element of intent to commit a crime. Therefore, the perpetrators are charged under Article 32 Paragraph 1 of the ITE Law (Electronic Information and Transactions), which states, "Every person who intentionally and unlawfully, against the law, by changing, adding, reducing, transmitting, damaging, eliminating, moving, or concealing electronic information and/or electronic documents belonging to another person or the public," Article 33 of the ITE Law (Electronic Information and Transactions), which states, "Every person who intentionally and unlawfully, against the law, performs any action that disrupts the Electronic System and/or causes the Electronic System to malfunction," and Article 36, which states, "Every person who intentionally and unlawfully, against the law, commits the actions referred to in Articles 27 thru 34, which have caused losses to others." The violation of Article 33 is linked to the provisions in Article 49, which outlines the legal consequences of the violation.

Before the enactment of the ITE Law (Information and Electronic Transactions), legal violations in ransomware attacks were regulated in Article 378 of the Criminal Code regarding fraud, as it is known that ransomware attacks generally fall under the category of fraud. The fraud defined in Article 378 of the Criminal Code reads as follows:

"Whoever, with the intention of unlawfully benefiting themselves or others, by using a false name or false title, employing deception, or a series of lies, to induce others to hand over something to them, or as a source of debt or to cancel a claim, shall be punished with imprisonment for a maximum of 4 (four) years."

Based on the elements of the sound of Article 378 of the Criminal Code itself, it can be concluded that "whoever" is the subject, meaning the perpetrator who commits the act of fraud. There is an intention to benefit oneself or others, meaning there is a deliberate act done with a specific purpose (oogmerk). Furthermore, such actions can be unlawful, meaning the perpetrator of the fraud has no right whatsoever to enjoy the profits, which are the result of the fraud. [14] Based on the two laws governing cybercrime, namely the Criminal Code (KUHP) and the Electronic Information and Transactions Law (ITE), we must be familiar with the principle of "Lex Specialis Derogat Legi Generali." According to this principle, more specific legal rules take precedence over more general legal rules. Therefore, it can be concluded that the current law governing cybercrime is regulated by Law Number 1 of 2024 concerning the Second Amendment to Law Number 19 of 2016 concerning Amendments to Law Number 11 of 2008 concerning Electronic Information and Transactions, because this law is specific[15]

From the human rights perspective, ransomware attacks are seen as a violation of right to privacy and protection of personal data. It is undeniable that humans enjoy the right to privacy and personal data protection. When ransomware takes place, the individuals are forced to make a choice either to accede to the demands of the perpetrators by paying the ransom, or lose control of their data in the system or device. The primary law in this context is Law No. 27 of 2022 on Personal Data Protection (PDP Law) which was enacted on 17 October 2022 and requires full compliance by 17 October 2024. It affirms the right to data privacy by granting individuals control over their personal data, including rights to access, correct, delete, and object to its processing. The law also mandates organizations to implement security safeguards and notify individuals in the event of a data breach. As Indonesia's first comprehensive data protection law, it marks a significant step toward aligning national privacy standards with global frameworks such as the EU's GDPR. In this regard, ransomware attacks are indeed in contravention to the rights of data subjects accorded by the PDP Law.

Additionally, Ministerial regulations in Indonesia, particularly MOCI Regulation No. 20 of 2016 and MOCI Regulation No. 5 of 2020 (as amended by Regulation No. 10 of 2021), play a crucial role in shaping the country's data privacy landscape. These regulations govern the protection of personal data in electronic systems and impose obligations on private sector operators to safeguard user information. However, the lack of clear enforcement mechanisms and overlapping regulatory authorities pose a threat to the human right to privacy. Without consistent oversight and accountability, individuals remain vulnerable to data misuse, breaches, and unauthorized surveillance in the digital environment.

In a recent ransomware attack, the suspects intentionally stole data and damaged government systems, which impacted government public service applications and the government's national archive application, causing them to be temporarily damaged and unusable. The suspect also demanded a ransom from the government, an act that can be prosecuted under Article 32 Paragraph (1) in conjunction with Article 33 of the ITE Law (Electronic Information and Transactions). Article 32 Paragraph (1) reads as follows:

"Someone intentionally/and without right or unlawful act and by any means has changed, added to, or reduced, and carried out transmission activities by damaging, moving, removing, and concealing electronic information and/or electronic data documents that are public property or belong to others."

The ransomware attack itself has also met the subjective and objective elements contained in Article 32 Paragraph (1) and Article 48 of the ITE Law (Electronic Information and Transactions), so anyone who has met these elements can be sentenced to eight years in prison and a fine of up to two billion rupiah. Based on Article 49 of the ITE Law (Electronic Information and Transactions), anyone who has met the elements of Article 33 can be sentenced to imprisonment or jail for ten years or a fine of up to ten billion rupiah.

3.6 Law Enforcement for Ransomware Attacks Based on Law Number 8 of 1981 Concerning Criminal Procedure Law (KUHAP)

There is Article 30 of Law Number 8 of 1981 concerning Criminal Procedure Law (KUHAP) which states, "If the detention period as referred to in Articles 24, 25, 26, 27, and 28 or the extension of detention as referred to in Article 29 is not valid, the suspect or defendant is entitled to request compensation in accordance with the provisions contained in Articles 95 and 96." This can be applied in ransomware attack cases. This is because ransomware attacks are considered to have intentionally stolen data and damaged government-owned application systems, which is illegal. However, ransomware attacks are very difficult to prove, considering that all the equipment used as evidence has information and documents in electronic form. Nevertheless, ransomware attacks that steal data and damage government-owned application systems can be used as evidence in accordance with Article 5 of the Criminal Procedure Code (KUHAP), which states that access to information and documents and their printouts can be used as valid evidence. Article 5, Paragraph (2) of the KUHAP states that there is an expansion of valid evidence in accordance with Indonesian procedural law. Other provisions regarding evidence are also mandatory criminal provisions, meaning that the evidence must not be added to or subtracted from to comply with those provisions. This evidence is expanded upon by Article 184 of the Criminal Procedure Code (KUHAP), which states that evidence related to ransomware attacks involving data theft and damage to government application systems is valid evidence. This evidence cannot be separated from Article 188 Paragraph (2) of the Criminal Procedure Code, which grants judges the authority to seek evidence from various statements from witnesses, the accused, and written statements. [16] The government application system damaged by the ransomware attack is SRIKANDI, the national archiving application from ANRI, which can be used as an extension of the clues in the evidence used by the judge to prove the case falls under ransomware attacks, as previously explained. The criminal actions taken against this ransomware attack case allow for the involvement of more than one legal system and from various countries, making this ransomware attack a crime in multiple countries, considering factors such as the interests of various countries in a crime, whether the perpetrator, victim, or location of the crime, or a combination of these elements, are involved.

The criminal act of stealing data and damaging government application systems in this ransomware attack case involves several people from different countries, so cooperation with those countries is necessary during the enforcement process. Ransomware attacks are an international crime with jurisdictional implications for the enactment of laws, how to punish, and how to punish the perpetrators of such attacks. The criminal violations committed by the ransomware attack itself certainly involve more than one legal system or country.

The existence of the Electronic Information and Transactions Law in Indonesia also regulates various activities in cyberspace. However, the recent ransomware attacks that have affected Indonesia are not specifically addressed in this law. Nevertheless, the provisions of Article 30 Paragraph (2) of the Criminal Procedure Code can be applied in this case. Based on what has been explained above, the recent ransomware attacks targeting Indonesia are very dangerous because they have violated the law by stealing data and damaging government applications. These ransomware attacks steal data from various government platforms, such as stealing data from Indonesian citizens thru the immigration system, which caused domestic and international tourists to be stranded at airports because the online immigration system was disrupted and temporarily unusable. As for the damage to government applications, one example is the SRIKANDI application, which is the government's national archive application used to store digital documents created by ANRI (National Archives of the Republic of Indonesia). This application experienced system damage, rendering it temporarily unusable as well. This ransomware attack was also caused by the government's malware (security system) being easily hacked by malicious hackers. This made it easy for these malicious hackers to steal data or hack and damage the Indonesian government's application systems. Nevertheless, this ransomware attack must be followed up on and the perpetrators immediately sought because it is a form of law violation that violates the laws in force in Indonesia, namely the ITE Law (Information and Electronic Transactions Law). Indonesia’s legal framework for handling ransomware cases, particularly through the ITE Law and the KUHAP, remains limited in scope and effectiveness. While the ITE Law criminalizes interference with electronic systems, it lacks specific provisions addressing ransomware’s coercive nature, such as data encryption and demands for ransom. KUHAP, meanwhile, is procedural and does not accommodate the technical complexities of cybercrime investigations. Enforcement is hindered by limited digital forensic capabilities, inconsistent coordination among agencies, and outdated investigative tools. Challenges in evidence gathering—especially in tracing system logs and securing digital proof—further weaken prosecution efforts.

4. CONCLUSIONS

Based on the results and discussion explained above, the researcher can conclude that the ransomware attack case is a serious issue for Indonesia because it can cause all public service platforms and government-owned applications, including SRIKANDI, to be affected. SRIKANDI itself is a digital national archive application created by ANRI (National Archives of the Republic of Indonesia). In the ransomware attack, public service platforms and government applications were temporarily unusable because the ransomware had

damaged their operating systems and stolen their data, resulting in severe damage. This ransomware attack case is also an international case because it involves various affected countries, necessitating the involvement of other countries' laws in addition to Indonesian law. This makes the recent ransomware attacks in Indonesia subject to the laws in effect in Indonesia. These laws are the ITE Law (Electronic Information and Transactions), which is found in several articles as follows: Article 32 Paragraph (1), Article 33, Article 48, and Article 49. The implementation of its enforcement can be seen in the Criminal Procedure Code (KUHAP) Article 30, which is clearly explained.

The steps the government needs to take to prevent this event from happening again are to do various things such as: regularly backing up data; periodically updating software and operating systems; using strong security solutions; being vigilant against suspicious emails and links; using strong and unique passwords; limiting access rights; paying attention to firmware updates; increasing user awareness; using firewalls and traffic filters; and monitoring and detecting security threats. In law enforcement, the Indonesian government is taking action against ransomware cases by creating lists of accounts that hacked the SRIKAND system to be imprisoned for violating applicable laws, namely the ITE Law.

Apart from the suggestions above, to further strengthen Indonesia's governance of ransomware threats, the public-sector cybersecurity regulations must be reinforced through the proposed Cybersecurity and Resilience Bill 2025, which would clarify institutional roles and mandate incident reporting. Additionally, digital forensics capabilities should be enhanced by investing in forensic tools, training law enforcement, and establishing a Cyber Incident Review Board to improve evidence handling and response times. Finally, Indonesia should expand international cooperation by joining the Budapest Convention on Cybercrime and developing real-time threat intelligence platforms. These measures collectively support stronger enforcement, better prevention, and protection of digital rights and data privacy.

REFERENCES

[1] BBC News Indonesia: Pusat Data Nasional Sementara lumpuh akibat ransomware, mengapa instansi pemerintah masih rentan terhadap serangan siber?.

[2] Kominfo: SRIKANDI

[3] Hartono, B.: Ransomware: Memahami Ancaman Keamanan Digital. Bincang Sains dan Teknologi. 2, 55–62 (2023). https://doi.org/10.56741/bst.v2i02.353

[4] Wazid, M., Zeadally, S., Das, A.K.: Mobile Banking: Evolution and Threats: Malware Threats and Security Solutions. IEEE Consumer Electronics Magazine. 8, 56–60 (2019). https://doi.org/10.1109/MCE.2018.2881291

[5] Dehalwar, K. S. S. N., & Sharma, S. N. (2024). Exploring the distinctions between quantitative and qualitative research methods. *Think India Journal*, *27*(1), 7-15.

[6] Jimmy, F. N. U. (2023). Understanding Ransomware Attacks: Trends and Prevention Strategies. *DOI: https://doi. org/10.60087/jklst. vol2*, (1), p214.

[7] Jayadatta, S. (2025). Impact and Effect of Spyware, Adware, and Malware on Digital Environment in Modern Society. In *Digital Transformation in the Customer Experience* (pp. 73-89). Apple Academic Press.

[8] Jiang, Y., Li, G., Li, S., Guo, Y., & Zhou, K. (2024). Crowdsourcing Malware Family Annotation: Joint Class-Determined Tag Extraction and Weakly-Tagged Sample Inference. *IEEE Transactions on Network and Service Management*.

[9] CrowdStrike: 2019 CrowdStrike Global Threat Report

[10] Arditama, Y.: REvil Ransomware: Mengguncang Dunia Digital dengan Model Ransomware "Double Extortion"

[11] Sunggara, M. A., & Hariansah, S. (2024). Challenges and Threats of Cybercrime in Indonesia: A Review of Legal and Information Technology Aspects Related to Ransomware Attacks on Indonesia's National Data Center. *Pakistan Journal of Criminology*, *16*(431).

[12] Oğurlu, E. (2023). International Law in Cyberspace: An Evaluation of the Tallinn Manuals. *Annales de La Faculté de Droit d'Istanbul*, *0*(73), 327–344. https://doi.org/10.26650/annales.2023.73.0010.

[13] Ani Munirah Mohamad, Felicia Yong Yan Yan, Nurhazman Abdul Aziz, Shuhairy Norhisham, Grace Sharon, (2024). Modus Operandi, Factors, Implications And Governance Of Ransomware Attacks On Transportation Systems. *Proceedings Of The 12th UUM International Legal Conference 2023 (UUMILC 2023)*, 1(1), 32 - 54.

[14] Andi Hamzah: Delik-Delik Tertentu (Speciate Delicten) Didalam KUHP Edisi Kedua. . Sinar Grafika, Jakarta (2015)

[15] Dodi Parlagutan dan Eka Putri Oktaviani: Penegakan Hukum Terhadap Tindak Pidana Phising Ditinjau Berdasarkan Hukum yang Berlaku di Indonesia. UPNV Jakarta Journal. 1, 6–7 (2023)

[16] Irfan Arief Kurniawan, Hadi Mahmud, Nourma Dewi: PENYEBARAN VIRUS RANSOMWARE WANNACRY BERDASARKAN UNDANG-UNDANG NO. 11 TAHUN 2008 . Jurnal Inovasi Penelitian (JIP). 2, 428–429 (2021)