

COUNTERING CYBER ESPIONAGE CRIMES IN INDONESIA: A CRIMINAL LAW ANALYSIS BASED ON ROUTINE ACTIVITY THEORY

Muh. Sanjaya Sakti¹, Khalid Usman ², Muhammad Wahyudin Naskun³

Faculty of Law, University of Islam Indonesia Yogyakarta, Indonesia¹.
Faculty of Law, University of Lakidende, Unaaha, Indonesia², Advokat,
Peradi SAI, Kendari, Indonesia³

Email: muhsanjayasakti134@gmail.com¹
Khalidusmanperadi@gmail.com² yudhiwahyudin@gmail.com³

Abstract

Cyber espionage represents a serious form of cybercrime with strategic implications for national security, economic stability, and the protection of personal data. In Indonesia, cyber espionage has not yet been explicitly regulated as a distinct criminal offense, resulting in legal uncertainty and limited law enforcement effectiveness. This study aims to analyze cyber espionage crimes from the perspective of criminal law using Routine Activity Theory as an analytical framework. Employing normative juridical research with statutory and conceptual approaches, this study examines secondary legal materials, including legislation, scholarly works, and relevant case studies. The findings indicate that the absence of specific cyber espionage norms forces law enforcement to rely on general provisions of the ITE Law, which do not adequately reflect the strategic nature of espionage crimes. Routine Activity Theory demonstrates that cyber espionage occurs due to the presence of motivated offenders, valuable digital targets, and weak guardianship mechanisms. Therefore, this study recommends the formulation of explicit cyber espionage offenses within national criminal law, strengthening cybersecurity institutions, and enhancing digital literacy as preventive measures.

Keywords: *Cyber Espionage*, Cybercrime, Criminal Law, Routine Activity Theory.

A. Introduction

The development of information and communication technology (ICT) has brought significant changes in various aspects of people's lives.¹ The development of information and communication technology has changed the landscape of threats to national and individual security. One form of threat that is increasingly real in this digital era is cyber espionage,

¹ Manuel Castells, *The Rise of the Network Society* (Oxford: Blackwell Publishers, 1996), 1–24.

which is the activity of collecting confidential information or monitoring people by spying illegally through electronic means, against the state, corporations, and individuals.² These crimes are often committed by infiltrating network systems or through digital interception techniques and are often difficult to detect.³

The phenomenon of cyber espionage crimes in Indonesia has not been widely used as the subject of in-depth criminal law studies.⁴ In fact, in some cases, the practice of wiretapping and spying in an illegal way, which constitutes cyber espionage, has emerged, as seen in the case of the "PAPA MINTA SAHAM" scandal, which has the problem of leaking personal data by unknown parties or hacking of strategic state institutions.⁵

Based on the above statement, it shows the urgency to study cyber espionage not only in terms of technology but also in terms of criminal law, cyber law, and human rights, especially the right to privacy and data protection. Even though the State of Indonesia has legitimized through Article 31 paragraph (1) of Law of the Republic of Indonesia Number 1 of 2024 concerning the Second Amendment to Law of the Republic of Indonesia Number 19 of 2016 concerning Amendments to Law of the Republic of Indonesia Number 11 of 2008 concerning Information and Electronic Transactions (hereinafter referred to as the ITE Law), which states that:

"Every Person intentionally and without rights or unlawfully intercepts or wiretaps Electronic Information and/or Electronic Documents in a certain Computer and/or Electronic System belonging to another Person".

Related to the description above, the special regulation regarding cyber espionage crimes is still partial and has not been formulated as a separate offense in the national positive law. Other countries, such as the United States and Russia, have made cyber espionage part of their national criminal law regimes. The phenomenon of cyber espionage crimes in

² Aldo Rahmandana, "A Juridical Review of Cyber Espionage Based on International Law," *Jurist-Diction* 4, no. 6 (2021): 4724–4732.

³ Nikles Denny Ardiansyah, Bambang Panji Gunawan, and Djasim Siswono, "Application Of The Ite Law In Cyber Law Enforcement In Indonesia Case Study on Articles 27 to 37," *Journal of Legal Reform : Cogito Ergo Sum* 7, no. 2 (August 2024): 17–22, <https://doi.org/10.51804/jrhces.v7i2.16729>.

⁴ Evi Dwi Hastri, "Cyber Espionage as a Threat to the Defense and Security of the Indonesian State," *Law and Justice Review Journal* 1, no. 1 (2021): 10.

⁵ Kompas.com, *Recording of 'Papa Aska Saham' between Setya Novanto and Freeport* (Jakarta: Kompas, 2015), <https://nasional.kompas.com/read/2015/11/17/12134261/>.

Indonesia has not been widely used as the subject of in-depth criminal law studies.⁶ If seen in some cases, the practice of wiretapping and spying in an illegal way that constitutes cyber espionage has emerged, seen as in the case of the "PAPA MINTA SAHAM" scandal, which has the problem of leakage of personal data by unknown parties or hacking of strategic state institutions.⁷

Based on these things, the urgency to study cyber espionage is not only from the technical and information security aspects, but also from the aspects of criminal law, cyber law, and the protection of human rights, especially the right to privacy and personal data, which is very important. This research also introduces a criminological approach, namely Routine Activity Theory, to explain why cyber espionage can occur repeatedly and continue to develop.⁸ This theory states that a crime can occur when there are motivated offenders, suitable targets, and the absence of capable guardians, which are very relevant to explain contemporary cybercrime patterns.⁹

So far, legal studies in Indonesia have not studied cyber espionage from a specific criminal law perspective or applied it within the framework of modern criminology theories such as Routine Activity Theory. In comparison, several previous studies have highlighted the technical aspects of cybersecurity and legal challenges in countering digital crime, but have not specifically examined *cyber espionage* as the main focus from a criminal law perspective and criminological theory. For example, First, research by Hafizh Maulana highlights more technical aspects and cyber defense policies of the state without making *cyber espionage* the main offense that is discussed in depth from the perspective of criminal law.¹⁰ Second, the research by Rizky Fauziah discusses cybercrime in general by

⁶ Paul Rosenzweig, *Cyber Warfare: How Conflicts in Cyberspace Are Challenging America and Changing the World* (Santa Barbara: Praeger, 2013), 47–49.

⁷ Michael N. Schmitt, *Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations* (Cambridge: Cambridge University Press, 2017), 221.

⁸ Thomas J. Holt and Adam M. Bossler, "Examining the Applicability of Lifestyle-Routine Activities Theory for Cybercrime Victimization," *Deviant Behavior* 30, no. 1 (2008): 1–25.

⁹ See also Lawrence E. Cohen and Marcus Felson, "Social Change and Crime Rate Trends: A Routine Activity Approach," *American Sociological Review* 44, no. 4 (1979): 588–608. In N. Akdemir and C. J. Lawless, "Exploring the Human Factor in Cyber-Enabled and Cyber-Dependent Crime Victimization: A Lifestyle Routine Activities Approach," *Internet Research* 30, no. 6 (2020): 1665–1687.

¹⁰ Hafizh Maulana, "National Data Protection from Cyber Espionage Threats: An Overview of Indonesia's Cyber Defense Strategy," *National Security Journal* 7, no. 1 (2021): 85–102.

emphasizing the protection of personal data, but does not integrate criminological theories such as *Routine Activity Theory* as an analytical framework.¹¹ Third, the study by Dewi and Putra focuses more on violations of privacy and human rights in the digital context without discussing the need for the formation of *a specific cyber espionage crime*.¹² Thus, this research has a novelty in the form of integrating legal and criminological approaches in analyzing the need for the formation or reconstruction of cyber criminal laws related to cyber espionage more systematically and responsively.

Regarding cyber espionage offenses, the handling often depends on the interpretation of general articles such as illegal access, data theft, or privacy violations. Thus, this shows the importance of reconstructing cyber criminal law that can respond to the development of digital crime forms more appropriately and systematically. Based on the topic that the author will study, the research problem can be formulated as follows: How are efforts to overcome cyber espionage crimes from the perspective of routine activity theory and legal rules in Indonesia? And How can Routine Activity Theory explain cyber espionage crimes and contribute to their prevention within the Indonesian legal framework?

B. Research Methods

This study employs normative juridical research focusing on legal norms and doctrines. The approaches used include statutory analysis of Indonesian cyber laws and a conceptual approach based on Routine Activity Theory. The data source used in this study is secondary data, which includes primary and secondary legal materials.¹³ The researcher collected data by reading and citing these sources. The data analysis technique is carried out with an approach based on norms, principles, and laws and regulations that apply as positive legal norms, then analyzed qualitatively. Thus, this research aims to produce a comprehensive, complete, and thorough understanding.¹⁴

¹¹ Rizky Fauziah, "Personal Data Protection in the Digital Era: A Review of Indonesia's Positive Law," *Journal of Law and Development* 50, no. 3 (2020): 431–450.

¹² Ayu Dewi and Budi Putra, "The Right to Privacy and Personal Data Protection in the Digital Era: Human Rights Perspective," *Human Rights Journal* 12, no. 2 (2021): 210–225.

¹³ Muhaimin, *Legal Research Methods* (Mataram: Mataram University Press, 2020), 35.

¹⁴ Dyah Ochtorina and A'an Efendi, *Legal Research* (Jakarta: Sinar Grafika, 2014), 67.

C. Discussion

1. Norm Gaps in National Criminal Law and Implications for Legal Certainty

Prohibited acts as stipulated in Article 27 of the ITE Law to Article 36 of the ITE Law include various forms of information technology abuse, such as the distribution of immoral content, electronic insult or defamation, threats, the spread of fake news, illegal access to electronic systems, and the manipulation of electronic data and transactions. Each form of violation is an act that disturbs public order, injures private rights, and even threatens national data sovereignty.

Acts that violate these provisions are subject to criminal sanctions as stipulated in Article 45 of the ITE Law to Article 52 of the ITE Law. These criminal provisions include the threat of imprisonment, fines, and additional criminal possibilities, such as confiscation of electronic evidence or temporary suspension of access to the system. For example, Article 45 paragraph (1) of the ITE Law states that: “any person who deliberately and without the right distributes or transmits electronic information that has content that violates morality can be sentenced to a maximum of 6 (six) years in prison and/or a maximum fine of Rp1 billion”.

This provision shows that the ITE Law not only regulates ethical norms in the use of digital technology, but also applies a criminal mechanism for violations that contain elements of intentionality, without rights, or authority. Therefore, understanding the relationship between Articles 27-36 of the ITE Law as a form of prohibited acts and Articles 45-52 of the ITE Law as the basis for imposing criminal sanctions is important in enforcing criminal law in the cyber field. Therefore, related to this problem, a systemic understanding of the structure of the ITE Law is required to be important in the enforcement of cyber criminal law to ensure legal certainty, protection of citizens' rights, and maintain the stability and security of the digital space proportionately and fairly.

The normative gap in the context of criminal law refers to the absence of an explicit, firm, and comprehensive regulation in the legal system for a certain act that has developed in society, but has not been formally criminalized in the law. In the realm of cybercrime, especially cyber espionage, this vacuum is a serious problem because the threats posed are

strategic, cross-national borders, and have a direct impact on national security and citizens' right to privacy.¹⁵

According to Barda Nawawi Arief,¹⁶ the void in criminal law can occur due to the delay in the law in responding to social dynamics due to technological developments, so that the law becomes "resistant to the changing times." In this context, Indonesia's criminal law has not been able to keep pace with the complexity of new forms of digital crime, including cyber espionage, which have become a crucial issue in many countries.

The absence of specific regulations regarding cyber espionage also has an impact on the lack of legal certainty, both for law enforcement officials and the general public. This is contrary to the principle of legality as stated in Article 1, paragraph (1) of the Criminal Code: "No act can be punished, except on the strength of the criminal rules in the existing legislation." The absence of clear rules results in: First, inequality in legal treatment, because it depends on the subjective interpretation of the apparatus. Second, it is difficult to prove criminal elements, because there are no norms that describe the characteristics of cyber espionage. Third, the potential for impunity for perpetrators because they cannot be properly prosecuted.¹⁷

In Indonesia's current positive law, there is not a single criminal law provision that explicitly formulates cyber espionage as a special criminal offense (formal and material offenses). Even though cyber espionage has special characteristics that distinguish it from conventional crimes, namely: First, it is carried out by digital methods through electronic systems. Second, it aims to access or obtain confidential information (state, private, corporate). Third, it often involves cross-border actors or foreign party proxies. Fourth, it is difficult to prove conventionally because it concerns encryption technology, identity disguise, and remote access.¹⁸

¹⁵ Mohamad Sahid, "Legal Vacuum in the Digital Era and the Urgency of National Cyber Law Formation," *Journal of Law & Development* 51, no. 1 (2021): 78–95, <https://doi.org/10.21143/jhp.vol51.no1.2871>.

¹⁶ Barda Nawawi Arief, *Problems of Law Enforcement and Criminal Law Policy in Crime Prevention* (Jakarta: Kencana, 2021), 47.

¹⁷ Yuniar Rahmawati, "The Principle of Legality and Norm Void in Cyber Criminal Law Enforcement," *Indonesian Legislation Journal* 19, no. 1 (2022): 35–50, <https://ejurnal.peraturan.go.id/index.php/jli/article/view/826>.

¹⁸ Rafiq Dwi Putra, "Law Enforcement Challenges to Cybercrime in a National Security Perspective," *National Security Journal* 8, no. 2 (2022): 112–29, <https://doi.org/10.31289/jkn.v8i2.5678>.

The absence of cyber espionage crimes causes law enforcement to have to enforce the application of general articles in the ITE Law, such as Article 30 on illegal access, Article 31 on unauthorized interception, and Article 32 on data manipulation or theft. However, the formulation of these delicacies does not specifically regulate the objectives of strategic reconnaissance, espionage motives, or the involvement of other state actors. This causes law enforcement to not reflect the substance of the crime that is committed in a cyber espionage case.¹⁹

To close this norm gap, there are two approaches that can be taken, namely expanding the norms in the ITE Law or the Criminal Code, by revising or adding articles that explicitly regulate cyber espionage. For example, by formulating a delicacy, namely: "surveillance or collection of information digitally that is confidential, without rights, against other parties for strategic, political, economic or military purposes". Then, the establishment of the Special Law on Cybersecurity, as Singapore and Russia have done, the special law will regulate the supervision, restriction, investigation, and enforcement of digital espionage activities and infiltration of state networks.²⁰ Including the regulation of actors, the scope of legal objects, and international cooperation for cross-jurisdictional law enforcement.

According to Cahyono, this void creates normative doubts in handling cases related to illegal collection of confidential data, as the available legal instruments tend to be multi-interpreted and do not reflect the purpose of regulating digital espionage-based attacks. In Indonesia's current positive law, there is not a single criminal law provision that explicitly formulates cyber espionage as a special criminal offense (both formal and material offenses). Because cyber espionage has special characteristics that distinguish it from conventional crimes, namely: First, it is carried out digitally through an electronic system connected to the internet. Second, the purpose of accessing or obtaining confidential information relating to the state, person, or corporate entity. Third, it often involves foreign or

¹⁹ Ahmad Yani, "Cybersecurity Law in Comparative Perspective: Lessons from Singapore and Russia for Indonesia," *Indonesian Journal of International Law* 18, no. 3 (2021): 401–18, <https://doi.org/10.17304/ijil.vol18.3.932>.

²⁰ Intan Puspita Sari, "The Construction of Cyber Criminal Law in Overcoming Digital Espionage Crimes," *IUS QUIA IUSTUM Legal Journal* 29, no. 1 (2023): 55–76, <https://doi.org/10.20885/iustum.vol29.iss1.art3>.

third-party actors (proxy states) on a cross-border scale. Fourth, it is proven conventionally, because it concerns identity disguise technology, remote access, data encryption, and digital fingerprint removal.²¹

As a result, law enforcement often has to enforce the application of general articles in the ITE Law, such as Article 30 on illegal access to electronic systems, Article 31 on unauthorized interception, and Article 32 on data manipulation or theft. However, the formulation of these delicacies does not specifically regulate the motives of espionage, strategic reconnaissance, or the involvement of foreign countries in digital crimes. This causes law enforcement to be inaccurate and does not reflect the substance of the crime that was committed. As revealed by Putra and Rakhman, the vacuum of cyber espionage norms can be exploited by perpetrators to move in the "legal gray zone", where there are no provisions that explicitly regulate or prohibit their actions, thus causing the state to be weak in cracking down on dangerous digital threats.

Based on the explanation above, the urgency of establishing special criminal norms *for cyber espionage* is based on at least three main reasons, namely the following:

Table 1. The urgency of establishing norms on cyber espionage crimes

Urgency Aspect	Explanation	Implications of Norm Void	Legal Reform Recommendations
Legal Certainty	Provide clarity on the elements of delicacy, the scope of legal objects, and criminal sanctions according to the principle of <i>lex certa</i> .	It creates uncertainty for law enforcement and the public, opening up opportunities for multiple interpretations.	Revise the ITE Law or the Criminal Code with a special article <i>on cyber espionage</i> that expressly formulates the elements, scope, and sanctions.
Law Enforcement Effectiveness	Facilitate the proof of criminal elements and avoid the application of irrelevant articles.	Investigators are forced to use general articles that do not reflect the substance of the crime, so they	Formulate special offenses so that the criminal elements are in accordance with the characteristics of <i>cyber espionage</i> and

²¹ Markus Djarawula, Novita Alfiani, and Hanita Mayasari, "Juridical Review of Information Technology Crimes (Cybercrime) in Indonesia in the Perspective of National Criminal Law," *Journal of Scientific Horizons* 2, no. 10 (2023): 3799–806, <https://journals.yapilin.com/index.php/djh/article/download/6/5>.

		are prone to free verdicts.	facilitate the proof process.
National Security	Protecting the country's strategic interests from cross-border threats and systemic impacts.	The potential for strategic data leakage, economic losses, and Indonesia's weak position in international cybersecurity cooperation.	Establish a <i>Cybersecurity Act</i> that regulates the prevention, prosecution, and international cooperation in countering <i>cyber espionage</i> .

The urgency of establishing a special criminal norm *for cyber espionage* is based on at least three main reasons: First, legal certainty that requires the formulation of a delict to be clear, firm, and not multi-interpreted according to the principle of *lex certa*, as described by Rusman and Kamaludin that the cyber legal framework in Indonesia still lacks specific rules so that it is prone to multi-interpretation.²² Second, the effectiveness of law enforcement shows that the absence of a special article makes law enforcement officials take advantage of the general article of the ITE Law, which is relevant, so that proof becomes difficult.²³ Third, national security, as stated by Aulianisa and Indirwan, is that *cyber espionage poses* a serious risk to state secrets, defense, and Indonesia's strategic position in international cooperation, so it requires a special legal umbrella.²⁴

Furthermore, within the framework of national legal politics, solutions that can be taken include revising the ITE Law by including a special article on cyber espionage, or the establishment of a comprehensive Cybersecurity Act by regulating aspects of prevention, enforcement, international cooperation, and the country's strategic data protection mechanism. This approach will harmonize national law with international best practices, while

²² Rusman Rusman and Ahmad Kamaludin, "Investigation of Cyber Crime in the Indonesian Legal Framework," *Journal La Sociale* 5, no. 6 (August 2024): 1576–86, <https://doi.org/10.37899/journal-la-sociale.v5i6.1367>.

²³ Dedy Obet, Suharto Suharto, and Henri Mujoko, "Cyber Cooperation In The Framework Of The Asean Regime," *Defense Journal: Information Media About Defense Studies & Strategies That Prioritize Identity, Nationalism & Integrity* 7, no. 2 (August 2021): 254, <https://doi.org/10.33172/jp.v7i2.1264>.

²⁴ Haekal Al Asyari, "Between Freedom And Protection: A Critical Review Of Indonesia'S Cyberspace Law," *Prophetic Law Review* 5, no. 1 (June 2023): 79–103, <https://doi.org/10.20885/PLR.vol5.iss1.art5>.

strengthening Indonesia's position in the global cybersecurity architecture.²⁵

2. Cyber Espionage Crimes in The Perspective of Routine Activity Theory

Routine Activity Theory (RAT) was developed by Lawrence Cohen and Marcus Felson in 1979 which is an important approach in modern criminology to explain the occurrence of crime through three main elements: First, motivated offenders, suitable targets and absence of capable guardians. In the context of cybercrime, especially cyber espionage, this theory is particularly relevant because the perpetrators are often state actors, organized groups or high-powered individuals who take advantage of the vulnerabilities of digital systems to illegally obtain strategic information.²⁶

Cyber espionage targets not only military and political secrets, but also commercial information, technological research and citizens' personal data. The chosen target typically has a high value and access vulnerability through network security weaknesses or a lack of encryption.²⁷ The perpetrator's motivation can be ideological, economic or geopolitical as exemplified by various attacks carried out by APT (Advanced Persistent Threat) that are attributed to a particular country.²⁸ For example, Digital Crime Behavior will be described as follows:²⁹

Table 2. Cyber espionage crime behavior

RAT Elements	Explanation in <i>Cyber Espionage</i>
<i>Motivated Offender</i>	State actors or foreign proxies with strategic motives (military, political, economic). For example, APTs like APT41 show highly motivated, structured, and even espionage organizations within official and external hours for personal and state gain
<i>Suitable Target</i>	The target is in the form of confidential data of the state, corporations, and strategic institutions that have

²⁵ Surya Oktaviandra, "Revisiting The Interpretation Of The Indonesian Criminal Procedure Code: Legal Basis For Witness Teleconferencing," *Journal of Law and Justice* 14, no. 1 (2025): 161–90, <https://doi.org/10.25216/jhp.14.1.2025.161-190>.

²⁶ Sari, "The Construction of Cyber Criminal Law in Overcoming Crime."

²⁷ Rahmawati, Apitta Fitria, dan Yuris Tri Naili, "The Progression of Cybercrime within the Context of Criminal Law Literature: Theoretical Framework and Practical Implications in Indonesia," *Tana Mana Journal* 6, no. 1 (2024): 223–34.

²⁸ Ridwan Muh, "APT Threats and State-Sponsored Cyber Espionage: Indonesian Perspective," *Journal of Digital Security* 3, no. 2 (2022): 87–101.

²⁹ Cropitekus, *Chinese espionage: 'They've targeted Australia'* (Australia: reddit, 2025), https://www.reddit.com/r/IntelligenceNews/comments/htqefc/chinese_espionage_theyve_targeted_australi.

	high value and are easily accessed digitally through system vulnerabilities or phishing.
<i>Absence of Guardian</i>	Lack of effective oversight from national cybersecurity institutions, lack of specific legislation, and weak technical protection against infiltration. This creates the condition of the absence of an adequate "capable guardian".

Based on the description of the table above, it is examined that in cyber espionage crimes, perpetrators are generally state actors, state-sponsored proxies, or organized criminal groups that have strategic motives such as political, military, or economic gains. They have a high technical capacity and are usually organizationally structured. For example, the APT41 group from China is actively spying on the health, financial, and government sectors in various countries, according to the Mandiant report. They use sophisticated malware and work both officially (for the state) and unofficially (for personal gain). Mandiant noted that the APT41 group showed "dual espionage and criminal operations," indicating highly motivated perpetrators who had access to state resources and high technical capabilities to penetrate the system.³⁰

The target in cyber espionage crimes is high-value strategic information such as state secrets, military plans, technological research, or business data of multinational corporations. These targets are feasible because they are easily accessible through system vulnerabilities, such as vulnerabilities, the use of weak passwords, or phishing attacks. An example of this is the hacking incident against cybersecurity company FireEye in 2020, which was used to gain access to various US government agencies through the SolarWinds software. In line with this, research from MIT confirms that sectors such as energy, telecommunications, and defense are the main targets of digital espionage because they store vital information and are often connected to open internet networks without full encryption.³¹

Guardian in RAT refers to parties that can prevent crime, such as law enforcement, legal mechanisms, or security technology. In the case of cyber espionage, these guards are often ineffective because, first, the absence of

³⁰ Mandiant Threat Intelligence, *APT41: A Dual Espionage and Cyber Crime Operation* (Milpitas, CA: FireEye, 2020), <https://www.fireeye.com/current-threats/apt-groups.html>.

³¹ Stuart Madnick, Tom H. Davenport, and Nazli Choucri, *Cybersecurity in the Era of COVID-19: The Threat of Cyber Espionage on Critical Sectors*, nos. 6922–21, MIT Sloan Research Paper (MIT Sloan School of Management, 2021), 10–15, https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3742600.

a specific law that explicitly regulates cyber espionage as a criminal offense in Indonesia, for example. Second, the weakness of early detection of cyber attacks, due to limited human and technological resources. Third, the lack of international cooperation makes cross-border actors act. According to a report by ENISA (European Union Agency for Cybersecurity), one of the main factors for the success of digital espionage is the weak defense system and the absence of comprehensive regulations that protect critical infrastructure from strategic and *persistent threats*.³² So that the prevention of Cyber Espionage by strengthening the national criminal law explicitly calls cyber espionage important to form a repressive framework. Then, the addition of technical protection and increasing cyber literacy of communities and institutions became an urgent need as a guardian. As well as the identification of strategic targets, layered security enhancements in critical sectors can minimize the risk of attack success. With that, RAT emphasizes the importance of a situational approach in cybercrime prevention. This means limiting opportunities for perpetrators through increasing the likelihood of violence and reducing the suitability of the target.

Departing from the discussion above, there should be a need for the establishment of special regulations that explicitly regulate the crime of *cyber espionage* in the Indonesian criminal law system, both through the revision of the ITE Law and the Criminal Code, as well as through the formation of a separate law that is responsive to the development of modern digital crime. In addition, strengthening *guardianship* is urgent, namely by improving the early detection system of cyber attacks, strengthening digital security technology, and increasing public literacy and awareness of the risks of *cyber espionage*. The government also needs to expand international cooperation to strengthen cross-border coordination in dealing with transnational cybercrime. On the other hand, protection strategies for strategic targets such as military, industrial and technological data must also be strengthened through periodic system security audits and the implementation of minimum security standards so that potential crimes can be effectively prevented according to the principles of routine activity theory which emphasizes the importance of reducing crime

³² European Union Agency for Cybersecurity, *Threat Landscape for Supply Chain Attacks* (ENISA, 2021), 5-9, <https://www.enisa.europa.eu/publications/threat-landscape-for-supply-chain-attacks>.

opportunities through strengthening surveillance and protection of vulnerable targets.

The implementation of the RAT in the Indonesian context underlines that strengthening guardianship is one of the main keys in preventing *cyber espionage*, especially considering the characteristics of this crime, which are transnational in nature and use advanced technology that is difficult to detect by conventional security mechanisms. *Cyber espionage* often exploits weaknesses in digital security systems, both in government and private sector infrastructure, requiring an integrated response between legal instruments, technical strategies, and institutional reforms. The RAT views that crime does not only occur because of the existence of perpetrators and decent targets, but also because of weak supervision or guarding. Therefore, strengthening *guardianship* in Indonesia is not enough only through a strict legal tool, but also requires practical steps that are adaptive to the development of the perpetrator's *modus operandi*.

The strengthening includes the establishment of a special article on *cyber espionage* in the ITE Law or the Criminal Code as part of the national criminal law reform, which provides a clear operational definition, the scope of prohibited acts, and proportionate sanctions. However, a strong legal apparatus without the support of a technical strategy will find it difficult to suppress the rate of crime. Therefore, the recommended technical strategies include: the development of an artificial intelligence-based early detection system to monitor the pattern of cyberattacks, the implementation of periodic cybersecurity audits on critical national infrastructure such as government data centers and banking systems, and the improvement of cyber literacy among government employees, law enforcement officials, and the general public.

On the institutional side, a special unit is needed under the coordination of the State Cyber and Cryptography Agency (BSSN) that focuses on *countering cyber espionage*, with the authority to conduct investigations, *threat intelligence sharing*, and preventive measures against potential strategic data leaks. International cooperation is a crucial element, considering that *cyber espionage* often involves perpetrators, servers, and communication networks that are outside Indonesia's jurisdiction. Active participation in global cybersecurity forums, the implementation of *mutual legal assistance* treaties, and the strengthening of extradition treaties with

strategic countries will strengthen Indonesia's position in cross-border law enforcement.

Protection against countries' strategic targets, such as national data centers, weapons systems, energy networks, and the financial sector, needs to adopt a layered security system that follows international standards such as ISO/IEC 27001 and the NIST Cybersecurity Framework. This principle of *defense in depth* ensures that if one layer of defense is penetrated, there is still another layer that is able to withstand the attack. In addition, the implementation of *situational prevention* emphasized by RAT must be realized in the design of systems that reduce the chances of crime, for example, with *access control management*, privilege restrictions, end-to-end encryption, and continuous monitoring.

The success of countering *cyber espionage* in Indonesia will depend heavily on a combination of three main elements: (1) clear and firm regulations to regulate and punish perpetrators; (2) the adoption of cutting-edge and adaptive cybersecurity technology; and (3) cross-sector coordination, both national and international, based on the principles of situational prevention in the style of RAT. This approach not only reduces the chances of crime but also strengthens national cyber resilience in the face of increasingly complex and dynamic threats.

In addition to the three main elements in the RAT, its application in the context of cyber espionage in Indonesia must also consider vulnerability mapping factors in the national digital infrastructure. Based on BSSN's annual report, most of the cyberattacks detected in Indonesia take advantage of weaknesses in system configuration, outdated software, and low cyber hygiene in users. This shows that even though legal and technological tools have been put in place, the human factor remains the weakest point in the security chain. Therefore, countermeasures strategies must emphasize the formation of a sustainable cybersecurity culture through periodic training, attack simulations, and the integration of security awareness in the work procedures of government agencies and strategic companies.

RAT is also relevant in examining the dynamics of changes in cyber espionage modes that increasingly rely on social engineering, phishing, and social media exploitation techniques to gain early access to the target system. Within the framework of this theory, prevention efforts can be directed at reducing target hardening by limiting exposure to sensitive

information online, using network segmentation, and implementing multi-factor authentication. This approach will make the target less attractive or more difficult for the perpetrator to access, thus reducing the chances of a successful attack.

In addition, law enforcement against cyber espionage needs to utilize a proactive law enforcement approach that is in line with the RAT, namely, detecting and intervening with potential perpetrators before the attack is realized. This can be done through cyber threat intelligence sourced from collaboration between law enforcement officials, internet service providers, cybersecurity companies, and the white-hat hacker community. The existence of a national threat intelligence platform connected to the BSSN analysis center will allow for early identification of attack patterns, the location of command and control servers, and cross-border networks of actors.

In the international context, because cyber espionage often involves state actors, Indonesia must adopt a cyber diplomacy strategy to establish international norms and agreements regarding limits and sanctions on digital espionage activities. Ratification of international treaties such as the Budapest Convention on Cybercrime can be a strategic step to strengthen the legal framework and facilitate cross-jurisdictional law enforcement cooperation.

Strengthening RAT-based cyber espionage prevention strategies in Indonesia must integrate legal, technological, and cross-sector collaboration approaches. This approach will create a resilient cybersecurity ecosystem, where the opportunity for actors to operate is minimized, targets are optimally protected, and surveillance is strengthened to close loopholes that can be exploited for attacks.

D. Conclusion

Based on the discussion above, it can be concluded that: First, the lack of clear norms in Indonesia's national criminal law against cyber espionage is an urgent issue. The absence of specific regulation creates legal uncertainty, hinders law enforcement, and leaves a gap of impunity for digital crimes that threaten state sovereignty and human rights. Therefore, Indonesia's cyber criminal law needs to be reconstructed through revisions of the ITE Law and the Criminal Code, as well as the development of new legal instruments that are better suited to modern

digital crimes. Second, from the perspective of Routine Activity Theory, cyber espionage crimes occur because there are motivated perpetrators, suitable targets, and a lack of effective guardianship. Perpetrators are usually state actors or organized groups with strategic political, economic, or military goals, supported by advanced technical skills and access to global digital infrastructure. Their targets are high-value information such as military data, trade secrets, or technological research, which are often accessible through cybersecurity vulnerabilities and weak encryption. Meanwhile, the guardians meant to prevent such crimes through legal regulations, technical systems, and international cooperation are still inadequate, as seen in Indonesia's lack of explicit laws on cyber espionage and weak early detection systems. Therefore, Routine Activity Theory (RAT) highlights the importance of strengthening guardianship by reforming laws, enhancing technical security and digital literacy, and developing strategies to identify and protect strategic targets, which can help reduce the systematic occurrence of these crimes.

E. Daftar Pustaka

- Akdemir, N., and C. J. Lawless. "Exploring the Human Factor in Cyber-Enabled and Cyber-Dependent Crime Victimization: A Lifestyle Routine Activities Approach." *Internet Research* 30, no. 6 (2020): 1665–87.
- Arief, Barda Nawawi. *Problems of Law Enforcement and Criminal Law Policy in Crime Management*. Jakarta: Kencana, 2021.
- Asyari, Haekal Al. "Between Freedom And Protection: A Critical Review Of Indonesia's Cyberspace Law." *Prophetic Law Review* 5, no. 1 (June 2023): 79–103. <https://doi.org/10.20885/PLR.vol5.iss1.art5>.
- Castells, Manuel. *The Rise of the Network Society*. Oxford: Blackwell Publishers, 1996.
- Cropitekus. *Chinese espionage: 'They've targeted Australia.'* Australia: Reddit, 2025. https://www.reddit.com/r/IntelligenceNews/comments/htqefc/chinese_espionage_theyve_targeted_australia.
- Cybersecurity, European Union Agency for. *Threat Landscape for Supply Chain Attacks*. ENISA, 2021. <https://www.enisa.europa.eu/publications/threat-landscape-for-supply-chain-attacks>.
- Goddess, Beauty, and Beauty. "The Right to Privacy and Protection of Personal Data in the Digital Age: A Human Rights Perspective." *Journal of Human Rights* 12, no. 2 (2021): 210–25.
- Djarawula, Markus, Novita Alfiani, and Hanita Mayasari. "A Juridical Review of Information Technology Crimes (Cybercrime) in Indonesia in the Perspective of National Criminal Law." *Journal of Scientific Horizons* 2, no. 10 (2023): 3799–806.

- <https://journals.yapilin.com/index.php/djh/article/download/6/5>.
- Fauziah, Rizky. "Personal Data Protection in the Digital Era: A Positive Legal Review of Indonesia." *Journal of Law and Development* 50, no. 3 (2020): 431–50.
- Hastri, Evi Dwi. "Cyber Espionage as a Threat to the Defense and Security of the Indonesian State." *Law and Justice Review Journal* 1, no. 1 (2021).
- Holt, Thomas J., and Adam M. Bossler. "Examining the Applicability of Lifestyle-Routine Activities Theory for Cybercrime Victimization." *Deviant Behavior* 30, no. 1 (2008): 1–25.
- Intelligence, Mandiant Threat. *APT41: A Dual Espionage and Cyber Crime Operation*. Milpitas, CA: FireEye, 2020. <https://www.fireeye.com/current-threats/apt-groups.html>.
- Kompas.com. *Recording of 'Papa Minta Saham' between Setya Novanto and Freeport*. Jakarta: Kompas, 2015. <https://nasional.kompas.com/read/2015/11/17/12134261/>.
- Madnick, Stuart, Tom H. Davenport, and Nazli Choucri. *Cybersecurity in the Era of COVID-19: The Threat of Cyber Espionage on Critical Sectors*. Nos. 6922–21. MIT Sloan Research Paper. MIT Sloan School of Management, 2021. https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3742600.
- Marzuki, Peter Mahmud. *Legal Research*. Revised Edition. Jakarta: Prenadamedia Group, 2019.
- Maulana, Hafizh. "National Data Protection from Cyber Espionage Threats: A Review of Indonesia's Cyber Defense Strategy." *Journal of National Security* 7, no. 1 (2021): 85–102.
- Muh, Ridwan. "APT Threats and State-Sponsored Cyber Espionage: Indonesian Perspective." *Journal of Digital Security* 3, no. 2 (2022): 87–101.
- Muhaimin. *Legal Research Methods*. Mataram: Mataram University Press, 2020.
- Nikles Denny Ardiansyah, Bambang Panji Gunawan, and Djasim Siswono. "Application Of The It Law In Cyber Law Enforcement In Indonesia Case Study on Articles 27 to 37." *Journal of Legal Reform: Cogito Ergo Sum* 7, no. 2 (August 2024): 17–22. <https://doi.org/10.51804/jrhces.v7i2.16729>.
- Obet, Dedy, Suharto Suharto, and Henri Mujoko. "Cyber Cooperation In The Framework Of The Asean Regime." *Journal of Defense: Information Media on Defense Studies & Strategies That Prioritize Identity, Nationalism & Integrity* 7, no. 2 (August 2021): 254. <https://doi.org/10.33172/jp.v7i2.1264>.
- Ochtorina, Dyah, and A'an Efendi,. *Legal Research*. Jakarta: Sinar Grafika, 2014.
- Oktaviandra, Surya. "Revisiting The Interpretation Of The Indonesian Criminal Procedure Code: Legal Basis For Winessteleconferencing." *Journal of Law and Justice* 14, no. 1 (2025): 161–90. <https://doi.org/10.25216/jhp.14.1.2025.161-190>.
- Son, Rafiq Dwi. "Law Enforcement Challenges to Cybercrime in a National Security Perspective." *Journal of National Security* 8, no. 2 (2022): 112–29. <https://doi.org/10.31289/jkn.v8i2.5678>.

- Rahmandana, Aldo. "Juridical Review of Cyber Espionage Based on International Law." *Jurist-Diction* 4, no. 6 (2021): 4724–32.
- Rahmawati, Apitta Fitria, and Yuris Tri Naili. "The Progression of Cybercrime within the Context of Criminal Law Literature: Theoretical Framework and Practical Implications in Indonesia." *Journal of Mana Mana* 6, no. 1 (2024): 223–34.
- Rahmawati, Yuniar. "The Principle of Legality and Norm Void in Cyber Criminal Law Enforcement." *Journal of Indonesian Legislation* 19, no. 1 (2022): 35–50. <https://ejurnal.peraturan.go.id/index.php/jli/article/view/826>.
- Rosenzweig, Paul. *Cyber Warfare: How Conflicts in Cyberspace Are Challenging America and Changing the World*. Santa Barbar: Praeger, 2013.
- Rusman, Rusman, and Ahmad Kamaludin. "Investigation of Cyber Crime in the Indonesian Legal Framework." *Journal La Sociale* 5, no. 6 (August 2024): 1576–86. <https://doi.org/10.37899/journal-la-sociale.v5i6.1367>.
- Sahid, Mohamad. "Legal Vacuum in the Digital Era and the Urgency of National Cyber Law Formation." *Journal of Law & Development* 51, no. 1 (2021): 78–95. <https://doi.org/10.21143/jhp.vol51.no1.2871>.
- Sari, Intan Puspita. "The Construction of Cyber Criminal Law in Tackling Digital Espionage Crimes." *Journal of Law IUS QUIA IUSTUM* 29, no. 1 (2023): 55–76. <https://doi.org/10.20885/iustum.vol29.iss1.art3>.
- Schmitt, Michael N. *Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations*. Cambridge: Cambridge University Press, 2017.
- Yani, Ahmad. "Cybersecurity Law in Comparative Perspective: Lessons from Singapore and Russia for Indonesia." *Indonesian Journal of International Law* 18, no. 3 (2021): 401–18. <https://doi.org/10.17304/ijil.vol18.3.932>.