E-Spionage: Unraveling the Realm of Cyber Espionage Law in Indonesia

Abraham Ethan Martupa Sahat Marune
Doctor of Law Program, Faculty of Law, Pelita Harapan University, Indonesia

Abstract:

Cyber espionage, as one of the increasingly frequent forms of cybercrime, utilizes information technology, particularly the internet, as its primary means. In this digital era, where cybercrime has a serious impact on individuals, organizations, national security, and privacy as a whole, it is important to understand how the law regulates this phenomenon. The research method used is normative legal research method by examining legislation in Indonesia and internationally. The results show that the regulation of cyber espionage in Indonesia has been regulated in the Telecommunications Law and the ITE Law, with the threat of serious criminal sanctions for violators. The Constitutional Court has strengthened the protection of citizens' privacy against wiretapping. However, in international law, the discussion on cyber espionage is still minimal. International cooperation is important in the development of international law, but there is no specific regulation governing cyber espionage in the context of peacetime and wartime.

Keywords: cyber espionnage; cybercrime; ITE Law.

Introduction

Cybercrime, which emerged along with the rapid development of information technology, has become a significant challenge in this digital era. One form of cyber crime that is increasingly occurring is *cyber espionage* , which utilizes information technology [1], especially the internet, as the main means. Crimes that occur on the internet or computers often require careful investigation to gather the necessary evidence. [2]The concept of *cyber espionage* itself combines two terms, namely " *cyber* " which refers to the internet or cyberspace, and " *espionage* " which refers to *espionage* or spying activities. Thus, *cyber espionage* can be interpreted as an act of spying carried out on electronic data or other criminal activities that use the internet network as a means of infiltrating or spying on other parties, by entering computer network systems [3]or in other words, it is a form of crime that using the internet network by entering the computer network system of the party who will be targeted as a target

[1]Barda Nawawi Arief, Mayantara Crime, Development of Cyber Crime Studies in Indonesia, (Jakarta: Rajawali Pers, 2005), p. 12
[2]Imam Riadi, Sunardi, and Panggah Widiandana, "Investigation of Cyberbullying on WhatsApp Using Digital Forensics Research Workshop", *RESTI Journal (Information Systems Engineering and Technology)* , Vol. 4, no. 4, (2020), p. 730.
[3]Joko Triyanto, Sunardi, and Imam Riadi, "Analysis of Cyber Espionage Investigations on Facebook Using *the Digital Forensics Research Workshop* (DFRWS)", *TECHNO Journal* , Vol. 23, no. 1, (2022), p. 40

for spying.[4]

This kind of cybercrime has a serious impact, not only on the individual or organization that is the victim, but also on national security and privacy as a whole. Therefore, handling *cyber espionage* requires cooperation between countries, technology companies, as well as strengthening information security systems to deal with this threat effectively. One type of *cyber crime* that is considered very dangerous is cyber espionage, which is often referred to as spying or reconnaissance on other parties' data. [5]Because the internet is a medium that crosses information boundaries, access to data involving other parties is a major concern and can be a serious crime. Before the advancement of information technology and the internet, surveillance was usually carried out conventionally, including wiretapping using voice recording devices. However, with advances in internet networks and widely available software, eavesdropping can now be done digitally, including intercepting voices, images and data as targets, which is known as *cyber espionage* . [6]

Regulation of *cyber espionage* , or wiretapping in the context of digital technology, has become a major concern in Indonesian positive law and international law. In an era where information technology is developing rapidly, *cyber espionage practices* can have a significant impact on individual privacy, national security, and global stability. In Indonesia, regulations regarding *cyber espionage* are reflected in various laws, such as Law Number 36 of 1999 concerning Telecommunications and Law Number 11 of 2008 concerning Information and Electronic Transactions. This regulation regulates various aspects of wiretapping in the context of modern technology, including prohibitions, criminal sanctions, and law enforcement powers. However, the implementation and enforcement of laws related to *cyber espionage* often pose challenges, especially in the face of continually changing technological developments.

On the other hand, at the international level, the issue of cyber espionage has become a complex topic of debate. Various countries and international institutions have tried to develop legal frameworks that regulate *cyber espionage activities* at the global level. However, the challenges faced in achieving consensus and implementing effective rules remain complex. In this article, we will analyze further the regulation of cyber espionage in Indonesian positive law and at the international level.

Research Method

The research method used is normative juridical, and takes the form of a data study conducted by examining library studies (*librarian study*).[7] While the core research data only serves as complementary data. This study uses various methodologies, including a *statute approach,* namely reviewing all laws and regulations

[4]Miftakhur Rokhman Habibi and Isnatul Liviani, "Information Technology Crime (Cyber Crime) and its Management in the Indonesian Legal System", *Al-Q ā n ū n: Journal of Islamic Legal Thought and Reform* , Vol. 23, no. 2, (2020), p. 405
[5]Sutarman, *Cyber Crime, Modus Operandi and Management* . (Yogyakarta: LaksBang PRESSindo, 2007), p. 3.
[6]Shelly Nicko, *Cyber Espionage Crime* . (Surabaya: Airlangga University Press, 2010), p. 16
[7] Rony Hanitiyo Soemitro, *Legal and Jury Research Methods*. (Jakarta: Ghalia Indonesia, 1994), pp. 5.

related to the legal issues being investigated.[8] In addition, it also uses a *Conceptual Approach*, namely by combining practical concepts that can be implemented into a particular point of view and become a solution to the problems that have occurred.[9] Study findings include analytical, descriptive, and prescriptive information. Prescriptive is a solution to the legal problems raised and etymologically means what should be,[10] while analytical descriptive research is limited to efforts to reveal a problem and situation as it is,[11] so that it only reveals or describes an event or fact that exists in detail, systematically, and thoroughly.[12]

Results and Discussion

Regulation of *Cyber Espionage* in Indonesian Positive Law

The rapid development of technology has had a significant impact on the way we communicate and interact. While telecommunications technology makes it easier to exchange information, it also opens up gaps for the emergence of various new forms of crime that require criminal law provisions to be overcome. Sudarto explained that criminal law is part of criminal politics which aims to rationally overcome crime.[13] Currently, there are various regulations governing wiretapping which are scattered in law. Two laws that specifically regulate wiretapping are Law no. 36 of 1999 concerning Telecommunications and Law no. 11 of 2008 concerning Information and Electronic Transactions. This law is the legal basis for regulating and anticipating wiretapping practices in the context of modern communications technology.

Espionage comes from the French word *espionnage* , which is a practice of collecting information about an organization or institution that is considered secret without obtaining legal permission from the owner of the information. *Cyber Espionage* consists of the words *Cyber* and *Espionage. Cyber* is defined as cyberspace or the internet, while *Espionage* is the criminal act of spying or espionage. *Cyber Espionage* is a crime that uses the internet network to carry out spying activities against other parties. by entering the target party's computer network (*computer network system)* . This crime is usually directed against business rivals whose important documents and data are stored in a *computerized system*. Actions *of cyber espionage* over electronic data and/or information by several telematics experts are classified into 2 (two), namely:

1. *Cyber espionage* as a pure crime is an act of spying carried out with the aim of

---

[8] Peter Mahmud Marzuki, *Legal Research*. (Jakarta: Kencana, 2010), p. 93.
[9] Johni Ibrahim, *Theory & Methodology of Normative Legal Research*, cet. III. (Malang: Bayumedia Publishing, 2007), pp. 302
[10]Abraham Ethan Martupa Sahat Marune, "Metamorphosis of legal research methods: navigating dynamic exploration", *Civilia: Journal of Legal Studies and Civic Education*, Vol. 2, No. 4, (2023), pp. 73-81.
[11]Abraham Ethan Martupa Sahat Marune, "Relevance of Legal Research Methodology in Addressing Modern Legal Challenges", *Pena Justisia: Media for Communication and Legal Studies*, Vol. 21, No. 2, (2022), pp. 1-15.
[12] Titon Slamet Kurnia et al, *Legal Education, Legal Science and Legal Research in Indonesia: A Reorientation*. (Yogyakarta: Student Library, 2013), p. 129.
[13]Sudarto, *Criminal Law and Community Development: A Study of Criminal Law Reform* . (Bandung: Switch Baru, 1983), p. 31.

exploiting data or information for criminal acts, for example using the data or information obtained and then processing it so that it can be used to steal data, sabotage and falsify data.

2. *Cyber espionage* as a gray crime, is an act of spying carried out only to gain pleasure for the perpetrator due to the satisfaction of being able to access another party's computer.

The basic basis for imposing criminal penalties on perpetrators *of cyber espionage* in Indonesia is that they must meet the qualifications of a criminal act. Considering that *cyber espionage* is one of the *cyber crime activities* against personal and confidential information of a person, agency or institution, the application of criminal articles must be appropriate, both based on those in the Criminal Code and outside the Criminal Code because this spying activity goes through a coherent process. When it comes to state security, the Criminal Code only regulates espionage against the state which tends to be carried out conventionally during war, namely in Articles 124 paragraph (2) and 126 of the Criminal Code. In Article 124 paragraph (2) it is formulated that:

> "It is punishable by life imprisonment or a maximum period of twenty years if the author:
>
> 1st: Tell or hand over to the enemy maps, plans, drawings, or writings regarding army buildings;
>
> 2nd: Become a spy for the enemy or give him accommodation."

Other provisions relating to the criminal act of *Cyber Espionage,* if a person's actions involve the leaking of data, especially regarding data that must be kept confidential (*data leakage*), then the provisions that can be applied are provisions relating to the act of leaking a secret.

Provisions related to leaking state secrets (including actions using internet facilities) are regulated in Articles 112, 113 of the Criminal Code and Article 114 of the Criminal Code as well as acts that leak company secrets are regulated in Article 322 of the Criminal Code and Article 323 of the Criminal Code. Act no. 36 of 1999 concerning Telecommunications strictly prohibits wiretapping in all its forms, including the use of additional tools or equipment on telecommunications networks to obtain information illegally. Article 40 of the Law emphasizes that individual privacy rights must be protected, so that wiretapping is prohibited because it violates this right. Violation of this rule can be subject to a maximum criminal sanction of 15 years in prison in accordance with Article 56 of Law no. 36 of 1999. In principle, the Law emphasizes strict protection of consumer information and confidentiality, although there are very limited exceptions because it involves violations of other people's personal rights. In addition, this law has a jurisdictional reach that covers actions within and outside the jurisdiction of Indonesia, considering that information technology is cross-territorial.

Act no. 36 of 1999 concerning Telecommunications and Law no. 11 of 2008 concerning Information and Electronic Transactions (UU ITE) is the legal basis for the use of Information Technology. The ITE Law, even though it has undergone

several judicial reviews at the Constitutional Court, is very important because it regulates electronic transactions and measures to protect service users. The Constitutional Court's decision emphasized that wiretapping, as a limitation of human rights, must be regulated appropriately in accordance with the 1945 Constitution of the Republic of Indonesia. Regulations regarding the legality of wiretapping must be in the form of law. The ruling strengthens the protection of citizens' privacy against wiretapping. The Court also emphasized that every interception must be carried out lawfully, especially in the context of law enforcement. Amendments to Article 5 of the ITE Law aim to provide legal certainty regarding the use of Electronic Information and Electronic Documents as evidence. The ITE Law strictly prohibits detrimental actions in the context of electronic transactions.

Act no. 11 of 2008 regulates wiretapping in Article 31, prohibiting wiretapping on documents and electronic transmission of information. This coincides with Article 32 of the ITE Law which specifically regulates the criminal act of wiretapping on the transmission of electronic information/electronic documents. Electronic Information and Electronic Documents are considered as valid evidence in electronic transactions. Amendments to the 2016 Law confirm criminal provisions. Criminal acts in Information Technology are often difficult to detect and overcome because of their virtual nature. Law enforcers experience difficulties in dealing with misuse of Information Technology. Investigation of criminal acts in the field of Information Technology is regulated in Article 42 of the ITE Law, complying with the provisions of the Criminal Procedure Law and the ITE Law.

Article 43 of the ITE Law, which was revised in 2016, gives special authority to Civil Servant Officials in the field of Information Technology and Electronic Transactions as investigators. They are responsible for carrying out criminal investigations in this field by paying attention to protecting privacy and data integrity. Searches and seizures are carried out in accordance with criminal procedural law by safeguarding the interests of public services. This official has powers such as receiving reports, examining witnesses, checking the veracity of reports, inspecting business entities, and sealing and confiscating tools or facilities used for unlawful Information Technology activities. They can also make electronic data inaccessible, request information from electronic system operators, terminate investigations, and notify and convey the results of investigations to the Public Prosecutor through State Police Officials. They can also work with investigators from other countries to share information and evidence.

From the formulation above, there are several important elements in the act of wiretapping that can be emphasized, such as the "intentional" element and the "without right or against the law" element in carrying out the interception. What is interesting about this formulation is the emphasis on the subjective element, namely intentionality as the intention in carrying out the action. This means that the perpetrator deliberately carried out the act and was able to predict the results of his action, so that the requirements for awareness and knowledge were met. Faisal Thayib, as quoted by Go Lisanawati, categorized wiretapping in Article 31 of the ITE Law as a computer-related crime in the form of illegal wiretapping. This is a prohibited criminal act because it is carried out without permission and harms the

interests of other people. The act of wiretapping as regulated in Article 31 of the ITE Law is an act that is strictly prohibited because it has the potential to harm computer system users.[14]

Wiretapping is also clearly regulated in Law no. 1 of 2023 concerning the Criminal Code, especially in Article 322 paragraphs 1 to paragraph 3. This article clearly states that wiretapping in any form is a criminal act that will be subject to criminal sanctions. Wiretapping, although considered a criminal offense, is also permitted in certain contexts by law enforcement officials to uncover certain crimes. Some laws that regulate this include:[15]

a. Dutch Criminal Code Articles 430-434 regulate the prohibition against officials authorized to conduct wiretapping and share the information obtained.[16]
b. Law Number 5 of 1997 concerning Psychotropic Substances: Gives wiretapping authority to the police in the context of criminal investigations related to psychotropic substances.
c. Law Number 31 of 1999 concerning Eradication of Corruption: Places wiretapping authority on investigators to examine corruption cases.
d. Law Number 36 of 1999 concerning Telecommunications: Apart from regulating wiretapping, it gives technology service owners the power to provide communication data as evidence in court.
e. Perppu Number 1 of 2002 concerning Terrorism: Establishes the power of wiretapping in investigations of terrorism crimes with permission from the court.
f. Law Number 18 of 2003 concerning Advocates: Protects communications between advocates and their clients from eavesdropping.
g. Law Number 21 of 2003 concerning Human Trafficking: Grants wiretapping authority to investigators for human trafficking cases with permission from the court.
h. Law Number 11 of 2008 concerning Information and Electronic Transactions: Allows wiretapping in law enforcement with certain permits.
i. Law Number 35 of 2009 concerning Narcotics: Gives authority to the National Narcotics Agency to carry out wiretapping related to narcotics.
j. Law Number 8 of 2019 concerning Money Laundering: PPATK can recommend wiretapping to investigators to prevent money laundering.
k. Law Number 46 of 2009 concerning Corruption Crime Courts: Establishes that wiretapping results can be used as evidence in court if carried out in accordance with specified procedures.

Testing the readiness of Indonesian law enforcement and international law against Cyber Espionage can be done through organizational management principles

[14]Go Lisnawati, "Underlining Law Number 11 of 2008 concerning Information and Electronic Transactions in the Dimensions of Cyber Law Development", *Mika Journal* , Vol. 12, no. 1, (2009), p. 96
[15]Nurazizah, Amirudin, and Ufran, "Criminal Acts of Wiretapping (Cyber Espionage) According to Positive Law in Indonesia", *Wahana Pendidikan Scientific Journal* , Vol. 9, no. 13, (2023), p. 483-485.
[16]R. Soesilo, *The Criminal Code (KUHP) and its Complete Commentary Article by Article* , (Bogor: Politea, 1994), p. 290-293.

using a three legal subsystem approach. Organizations, in this case the Indonesian government, are in an effort to face the threat of Cyber Espionage. One of the principles of organizational management is Planning, Organizing, Actuating, and Controlling (POAC) which was introduced by George R. Terry. The POAC principle contains stages in carrying out organizational functions which consist of planning, organizing, directing and monitoring.

1. Planning

   Planning is a stage for a manager to decide on a vision and mission, determine implementation to achieve goals by dividing responsibility for implementing the plan to someone and measuring indicators of success by comparing goals. The application of planning principles in law enforcement can take the form of searching for and reviewing national legal arrangements, including the results of ratification of international agreements relating to Cyber Espionage and developing plans for law enforcement. In the Criminal Code (KUHP) in Indonesia, there are regulations regarding crimes that utilize computer networks or cybercrime. The provisions in the Criminal Code relating to cyber crime are still conventional. However, cyber crime can be classified based on the level of intensity of the case, namely:

   a) Provisions regarding theft offenses.

   b) Provisions regarding the act of entering or crossing another person's territory. c) Provisions regarding disclosure of secrets.

   The rules in the Criminal Code that regulate the classification of these cases can be found in articles 362 of the Criminal Code, 167 of the Criminal Code, 112-113 of the Criminal Code. In using this article, a legal approach or interpretation must be taken. An example of the application of legal interpretation is the case of electricity theft. What is at issue in this case is whether the flow of electricity can be interpreted as "goods" and whether the action can be said to be "taking". The Dutch Judicial Council has decided that electrical circuits are included in the goods and thus taking action has occurred as regulated in Article 362 of the Criminal Code. The thing that was taken into consideration by the judicial panel was that the purpose of Article 362 was an effort to protect other people's property (Hoge Raad dated 23 May 1921, W 10726, NJ 1921. 564). Then, regarding the provisions regarding entering or crossing other people's territory. In article 167 of the Criminal Code it is stated that attempts to enter a house.

   a closed room or yard, in a way that is not justified by normative values and which poses a threat to the home owner, is punishable by a maximum penalty of nine months and can be increased if it is followed by a threat or there is cooperation in carrying out the action. When related to Cyber Espionage, the place where this crime occurs is cyberspace. Therefore, if you carry out a legal interpretation of this article, what will be recorded is the act or act which is against the law. Another provision related to the act of Cyber Espionage is that this act results in the leaking of data, especially data that must be confidential, so the provisions that can be applied are Article 112, Article 113 and Article 114 of the Criminal Code. Starting from a maximum criminal

threat of one year, namely when a person is negligent in carrying out his duties so that confidential letters or objects can be known by parties who do not have the right to know, up to the most serious criminal threat, namely when someone deliberately provides state secret information to another country, he is threatened with a maximum prison sentence. seven years long. Apart from the Criminal Code, there are other provisions relating to Cyber Espionage, namely Law Number 11 of 2008 concerning Information and Electronic Transactions (UU ITE) and Law Number 36 of 1999 concerning Telecommunications (UU Telkom). This law was formed to provide a legal umbrella for law enforcement officials to arrest and ensnare perpetrators of this crime rather than relying solely on the Criminal Code as a source of law in resolving these criminal offenses. In the ITE Law there is Article 30 Paragraph (2) which regulates Cyber Espionage provisions which state that a person who deliberately accesses a computer or electronic system in an unauthorized way to obtain electronic information or electronic documents is subject to a maximum prison sentence of 7 (seven) years and / or a maximum fine of IDR 700,000,000.00 (seven hundred million rupiah). Subject provisions in Cyber Espionage actions are also specified in this law, which consists of individuals and corporations. Regarding acts of Cyber Espionage carried out by corporations, this will result in a penalty being imposed, this is stated in Article 52 Paragraph (4) which can be understood when a corporation commits an act of Cyber Espionage, it will be punished with the principal penalty plus two-thirds. Regarding evidence in cyber crimes, evidence is added in the form of information or electronic documents. The provisions governing criminal acts in the telecommunications sector are regulated in the Telkom Law. In Article 22 and Article 50, it can be interpreted that every person is prohibited from accessing or manipulating computer or telecommunication networks and service providers. This article does not expressly state that Cyber Espionage is included in the formulation of the article, but regulates the actions of hackers who carry out espionage to spy on or intercept data. To strengthen law enforcement against acts of Cyber Espionage, Indonesia participated in the UN Anti-Espionage Resolution dated November 5 2013 .

2. Organizing

   Organizing is the entire process of grouping people, tools, tasks, as well as authority and responsibility to create an organization that can be moved as a unit in order to achieve predetermined goals. The implementation of this stage is to ensure resources to carry out specific plans and division of tasks to agencies and law enforcement officers. Indonesia has several institutions related to the threat of Cyber Espionage, one of which is the Indonesian National Police (Polri). The National Police is a component of the state whose role is to maintain security and public order, enforce the law, and provide protection, guidance and services to the community in order to maintain domestic security. Military forces, namely the Indonesian National Army (TNI) and intelligence institutions, namely the State Intelligence Agency

(BIN), can face the threat of Cyber Espionage. The State Intelligence Agency (BIN) as a state intelligence agency is tasked with early detection of threats that could disrupt the stability of the country's defense and security and in this case coordinates with the TNI as an effort to defend the country through strictly guarding geographical boundaries from state attacks using its military force. Apart from that, Indonesia has been a member of the International Telecommunication Union (ITU) since 1949. This is based on Presidential Decree Number 10 of 1969 regarding the International Telecommunication Union Convention in Montreux in 1965. ITU is an international organization that operates in the telecommunications sector and is related to the United Nations. Nation (UN).

3. Actuating
   Actuating in organizational management principles is an effort to realize plans by directing and motivating each employee according to their roles, duties and responsibilities. The application of the actuating principle in law enforcement can be that the government directs law enforcement agencies and officers to carry out enforcement in accordance with applicable law. The basis on which the National Police is expected to be able to provide guidance and protection to the community regarding Cyber Espionage is Law Number 2 of 2002 concerning the National Police of the Republic of Indonesia. The military's presence in the defense and security components in Indonesia is based on Article 3 of Law Number 34 of 2004 concerning the Indonesian National Army (TNI) which states that the TNI is under the president's orders in the deployment of military force. BIN has a legal basis in the form of Law Number 17 of 2011 concerning State Intelligence. In article 4, it is stated that BIN plays a role in carrying out early detection and warning efforts to prevent, ward off and overcome the nature of threats that may arise and endanger national interests and security. Regarding the TNI which also coordinates with BIN to maximize the country's defense and security, it is mentioned in Article 9. Then, ITU can collaborate with the National Police, TNI or BIN as a facilitator in developing security to face cyber threats, this is based on the results at the WSIS (World Summit of Information Society) in 2013. (International Telecommunication Union (ITU), 2015)
4. Controlling
   Controlling is the final stage of every plan implementation which ensures that each task has gone according to plan and determines the next plan after seeing the results of the implementation. The efforts of the National Police, TNI, BIN, and ITU in enforcing the law against Cyber Espionage need to be supervised by each supervisory function unit from each institution such as the National Police General Supervision Inspectorate, the TNI Inspectorate General, the BIN Main Inspectorate, and for the ITU Institution, supervision can be carried out by the UN. or any member country. In this way, Indonesia can carry out law enforcement against Cyber Espionage by using laws that are still in force and running the institutions of the National Police, TNI, BIN and inviting ITU cooperation.

Cyber Espionage Regulations in International Law

In the realm of international law, *cyber espionage* is still a topic that is rarely discussed because there are no specific regulations governing this matter. [17]The term "international law" itself was first introduced by Jeremy Bentham, a philosopher who is also a scholar from England, who introduced the concept of utilitarianism. [18]JL Brierly, an international law expert, defines International Law as the legal framework and principles that bind countries in their relationships with each other. [19]John Perkins has observed that international law developed based on the inexorable logic of international cooperation, applied in the context of foreign policy. The roots of law and its legitimacy lie in the dynamics experienced by these countries.

The Statute of the International Court of Justice, regulated in Article 38 paragraph (1), stipulates that the court will consider four sources to decide a case, including:[20]

a. International treaties, both general and specific, which establish rules that are expressly recognized by the countries participating in the treaty;
b. International customs, including opinions juris and general customs, which have become legal norms due to recognition by the international community;
c. General principles of Law recognized by civilized nations;
d. Court decisions and views of leading legal experts from various countries, as additional sources for establishing legal rules.

With various legal sources mentioned in Article 38 paragraph (1), *cyber espionage activities* will be assessed based on several sources of international law. This involves a review of international treaties and conventions that may regulate the issue of *cyber espionage* , as well as an examination of the substance of international court decisions that may impact *cyber espionage* and various relevant principles. [21]However, currently there are still no specific regulations that directly regulate *cyber espionage* , and there are even inconsistencies in the perception of traditional *espionage or Human Intelligence* . [22] Due to the legal vacuum regarding peacetime *espionage* in international law, individual countries have long criminalized acts of espionage through their domestic laws.

Several multilateral conventions indirectly touch on the issue of *espionage* in peacetime. For example, Article 7(3) *of the 1959 Antarctic Treaty* gives representative observers the right to carry out "inspections" of stations, installations, equipment and

---

[17]David Wallace, "Peeling Back the Onion of Cyber Espionage after Tallin 2.0", *Maryland Review* , Vol. 78, no. 2, (2019), p. 17.
[18]Gerald Postema, *Utilitarian International Order: Bentham on International Law and International Order* , (United Kingdom: Oxford University Press, 2019), p. 1.
[19]JL Brierly, *The Law of Nations: An Introduction to International Law* . (Jakarta: Bhratara 1963), p. 56
[20]JG Starke, *Introduction to International Law* . (Jakarta: Sinar Graphics 2008), p. 78.
[21]Michael N. Schmitt, *Tallin Manual on the International Law Applicable to Cyber Warfare* . (London: Cambridge University Press, 2013), p. 45.
[22] Veronika Prochko, "The International Legal View of Espionage", E-International Relations, available at https://www.e-ir.info/2018/03/30/the-international-legal-view-of-espionage/ , accessed on April 27, 2024.

aircraft of countries that have ratified the convention. Acts of surveillance, investigation, or review may be considered espionage activities. Article 19 paragraph (2) c UNCLOS (*United Nations Conventions on the Law of the Sea*) states that actions aimed at collecting information that is detrimental to the defense or security of coastal states are prohibited. However, this article only applies to ships that wish to cross or sail in the territorial waters of a country, so it does not cover *cyber espionage* carried out remotely.[23]

Espionage is often discussed in several articles in *the Vienna Convention on Diplomatic Relations* , *the Vienna Convention on Consular Relations* , and *the Convention on Special Missions* , such as Article 41 VCDR, Article 55 VCCR, and Articles 47(1) and (2) CSM. These conventions emphasize that diplomatic officials must comply with the laws of the receiving country and must not use diplomatic facilities for activities that violate their duties as diplomatic officials. Regulations regarding espionage in the context of wartime are often mentioned in *Convention* (IV) *Respecting the Laws and Customs of War on Land* , especially in Articles 29, 30 and 31. [24]In these treaties, it is not mentioned that acts of espionage and sending intelligence to countries enemy is considered an international offense. Espionage activities between countries, both in times of peace and war, have become common activities and are accepted by the international community. Although not explicitly declared war crimes, they are still generally considered criminal acts by states.[25]

However, *cyber espionage,* as an evolutionary form of conventional espionage, has not been specifically regulated in international agreements as a violation of international law. There are exceptions if the activity violates existing norms and principles of International Law. Although there is no international agreement that specifically regulates *cyber espionage* , various countries have regulated this issue in their national legislation. For example, Indonesia has regulated it in Article 7 of Law no. 3 of 2002 concerning National Defense and Article 30 of Law No. 11 of 2008 concerning Electronic Transaction Information. Other countries, such as the United States, have had *cyber* security laws since 2012. The European Union, as a supranational organization, has *a Convention on Cybercrime* which regulates various obligations for member states to prohibit acts *of cybercrime* , including *cyber espionage* in their territory. [26]

The implications of international customs and opinions juris in the context of the legality *of cyber espionage* have not yet been fully established. There is no legal view that firmly supports that *cyber espionage acts* are in accordance with International Law. [27] Article 38 of the Statute of the International Court of Justice explains that

---

[23]Katharina Ziolkowski, *Peacetime Regime for State Activities in Cyberspace: International Law, International Relations and Diplomacy* . (Tallin: NATO CCD OE, 2013), p. 228
[24]Vienna Convention on Diplomatic Relations 1963.
[25]Christopher D. Baker, "Tolerance of International Espionage: A Functional Approach", *American University International Law Review* , Vol. 19, no. 5, (2003), p. 1092.
[26]Aldo Rahmandana, "Judicial Review of Cyber Espionage Based on International Law", *Jurist-Diction* , Vol. 4, no. 6, (2021), p. 2149
[27]Aaron Shull, *Cyber Espionage and International Law* , GigaNet: Global Internet Governance Academic Network, Annual Symposium 2013, p. 2.

international custom is one of the sources of International Law, which includes two main elements: State Practice and *Opinio Juris Necessitatis* . [28]Even though there have been many *cyber espionage incidents* that meet the first element, namely state practice, there is not yet clear enough evidence to justify these actions as applicable law. Therefore, *opinions juris* cannot be a justification for *cyber espionage activities* between countries.

Furthermore, after reviewing the two sources of international law on *cyber espionage* , it is also necessary to consider the implications of the principles and various related decisions to support arguments regarding the legality *of cyber espionage* . One of the guidelines published by an organization under NATO, namely CCDCOE (*Cooperative Cyber Defense Center of Excellence*), is *the Tallin Manual* . This guide was prepared by 20 international experts and practitioners with the aim of explaining how international law is applied in cyberspace. This guide discusses *cyber operations* carried out by countries and individuals. The contents of this guide try to reflect *international customs* international *law* or custom, as well as its consistency with other sources of international law, such as "the teachings of the most qualified publicists". Some of the statements in the guide, such as the views of the US government, may be considered a basis for the formation of *an opinions juris* relating to *cyber espionage* .[29]

Conclusion

Based on the research results and discussion above, the author concludes that: Regulations regarding *cyber espionage* in Indonesia, especially regarding the practice of wiretapping, are regulated in several laws, such as the Telecommunications Law and the ITE Law. Violation of this rule can result in serious criminal sanctions, up to 15 years in prison. Wiretapping in the context of modern communication technology is strictly regulated and has a broad jurisdictional reach. The ITE Law has an important role in regulating electronic transactions and protecting the privacy of service users. The Constitutional Court's ruling strengthens the protection of citizens' privacy against wiretapping, emphasizing that every interception must be carried out legally and in accordance with the law. In addition, there are other laws that regulate wiretapping in the context of investigating certain crimes, such as human trafficking, corruption, terrorism, narcotics, money laundering, and others. Although considered a criminal offense, wiretapping is also permitted in certain contexts to uncover crimes.

The regulation of cyber espionage in international law remains underexplored, as there are currently no specific regulations directly governing it. International law, which binds states in their interactions, has evolved based on the necessity of international cooperation, reflected in state foreign policies. However, there continues to be a lack of explicit regulations addressing cyber espionage, whether in peacetime or wartime contexts. Given the increasing frequency and sophistication of cyber threats, it is crucial for international stakeholders to consider drafting

[28]Tamas Hoffmann, "Dr. Opinion Juris and Mr. State Practice: The Strange Case of Customary International Humanitarian Law", *Annales Universitatis Scientiarium Budapestinensis de Rolando Eötvös Nominatae Sectio Iuridica* , Vol. 46, no. 1, (2006), p. 374
[29]Michael N. Schmitt, "International Law in Cyberspace: The Koh Speech and Tallin Manual Juxtaposed", *Harvard International Law Journal* , Vol. 54, no. 1, (2012), p. 16.

comprehensive legislation, such as cyber laws, to establish clear norms and guidelines. Such laws could provide much-needed clarity on permissible and impermissible activities in cyberspace, enhance global cybersecurity, and deter malicious state-sponsored cyber operations.

Bibliography

Arief, Barda Nawawi. Mayantara Crime: Development of Cyber Crime Studies in Indonesia. Jakarta: Rajawali Press, 2005.

Baker, Christopher D. "Tolerance of International Espionage: A Functional Approach", *American University International Law Review* , Vol. 19, no. 5, (2003).

Brierly, JL *The Law of Nations: An Introduction to International Law* . Jakarta: Bhratara 1963.

Go Lisnawati, "Underlining Law Number 11 of 2008 concerning Information and Electronic Transactions in the Dimensions of Cyber Law Development", *Mika Journal* , Vol. 12, no. 1, (2009),

Hoffmann, Tamas. "Dr. Opinion Juris and Mr. State Practice: The Strange Case of Customary International Humanitarian Law", *Annales Universitatis Scientiarium Budapestinensis de Rolando Eötvös Nominatae Sectio Iuridica* , Vol. 46, no. 1, (2006).

Imam Riadi, Sunardi, and Widiandana, Panggah. "Investigation of Cyberbullying on WhatsApp Using Digital Forensics Research Workshop", *RESTI (Information Systems and Technology Engineering) Journal* , Vol. 4, no. 4, (2020).

Joko Triyanto, Sunardi, and Riadi, Imam. "Analysis of Cyber Espionage Investigation on Facebook Using *the Digital Forensics Research Workshop* (DFRWS)", *TECHNO Journal* , Vol. 23, no. 1, (2022).

Marune, Abraham Ethan Martupa Sahat, "Metamorphosis of legal research methods: navigating dynamic exploration", *Civilia: Journal of Legal Studies and Civic Education*, Vol. 2, No. 4, (2023): 73-81.

Marune, Abraham Ethan Martupa Sahat, "Relevance of Legal Research Methodology in Addressing Modern Legal Challenges", *Pena Justisia: Media for Communication and Legal Studies*, Vol. 21, No. 2, (2022): 1-15.

Marune, Abraham Ethan Martupa Sahat, and Brandon Hartanto. "Strengthening personal data protection, cyber security, and improving public awareness in Indonesia: Progressive legal perspective." *International Journal of Business, Economics, and Social Development* 2, no. 4 (2021): 143-152.

Miftakhur Rokhman Habibi and Isnatul Liviani, "Information Technology Crime (Cyber Crime) and its Management in the Indonesian Legal System", *Al-Q ā n ū n: Journal of Islamic Legal Thought and Reform* , Vol. 23, no. 2, (2020).

Nicko, Shelly. *Cyber Espionage Crime* . Surabaya: Airlangga University Press, 2010.

Nurazizah, Amirudin, and Ufran, "Criminal Acts of Wiretapping (Cyber Espionage) According to Positive Law in Indonesia", *Wahana Pendidikan Scientific Journal* , Vol. 9, no. 13, (2023).

Postema, Gerald. *Utilitarian International Order: Bentham on International Law and*

International Order . United Kingdom: Oxford University Press, 2019.
Rahmandana, Aldo. "Judicial Review of Cyber Espionage Based on International Law", *Jurist-Diction* , Vol. 4, no. 6, (2021).
Schmitt, Michael N. "International Law in Cyberspace: The Koh Speech and Tallin Manual Juxtaposed", *Harvard International Law Journal* , Vol. 54, no. 1, (2012).
Schmitt, Michael N. *Tallin Manual on the International Law Applicable to Cyber Warfare* . London: Cambridge University Press, 2013.
Shull, Aaron . *Cyber Espionage and International Law* , GigaNet: Global Internet Governance Academic Network, Annual Symposium 2013.
Soesilo, R. *The Criminal Code (KUHP) and its Complete Comments Article by Article* . Bogor: Politea, 1994.
Starke, JG *Introduction to International Law* . Jakarta: Sinar Graphics 2008.
Sudarto. *Criminal Law and Community Development: A Study of Criminal Law Reform* . Bandung: New Switch, 1983.
Sutarman. *Cyber Crime, Modus Operandi and Management* . Yogyakarta: LaksBang PRESSindo, 2007.
Veronika Prochko, "The International Legal View of Espionage", E-International Relations, available at https://www.e-ir.info/2018/03/30/the-international-legal-view-of-espionage/ , accessed on April 27, 2024.
Vienna Convention on Diplomatic Relations 1963.
Wallace, David. "Peeling Back the Onion of Cyber Espionage after Tallin 2.0", *Maryland Review* , Vol. 78, no. 2, (2019).
Ziolkowski, Katharina. *Peacetime Regime for State Activities in Cyberspace: International Law, International Relations and Diplomacy* . Tallin: NATO CCD OE, 2013.