Advances in Social Science, Education and Humanities Research, volume 436
1st Borobudur International Symposium on Humanities, Economics and Social Sciences (BIS-HESS 2019)

International Regulatory Vacuum of Cyber Espionage

Dodik Setiawan Nur Heriyanto[1*]

[1] *Department of International Law, Faculty of Law, Universitas Islam Indonesia, Yogyakarta, Indonesia*
[*] *Corresponding author. Email: dodiksetiawan@uii.ac.id*

ABSTRACT
Cyber espionage employs computer network to gather illegal access to confidential information from government or certain organization. The advance development of technology acknowledges the sophisticated and illegal means of receiving highly confidential data or information for certain purposes that risk the national security of a state. However, international law is still silent to define and regulate cyber espionage especially at the time of peace. By applying the normative legal methodology, this study analyzes the current practices of cyber espionage in the 21st century and how far the international law could reach these illegal activities. This study concludes that the basic diplomatic norms shall be applied to cyber espionage. It strictly in contravention with the principle of non-intervention and sovereignty of a state. Moreover, this study proposed the international legal framework to regulate cyber espionage.
Keywords: *cyber espionage, diplomatic law, sovereignty, non-intervention*

1. INTRODUCTION

Spy action has been practiced since time immemorial. In fact, this activity is the second oldest profession in the world. According to ancient Greek history, three spies from Greece were captured by Persian soldiers in the Sardes region who were looking for secret information about the power of the Persian army [1]. This indicates that espionage have been carried out since time immemorial even when the technological and information equipment is far from the touch of modernity. Spy services also continue to this day where many intelligence organizations or agents are formed both independently and formed by the state with the aim of finding specific information obtained from other countries for certain interest [2].

Indonesia was a victim of espionage, although it is unclear whether this action is included in cyber espionage or not, but in terms of its characteristics, it is included in a cyber espionage practice. Namely the espionage act carried out using the telephone tapping method against a number of Indonesian officials including the telephone of the current president Joko Widodo and his wife and the Republic's top officials, carried out by Australia. The wiretapping case was revealed after one of the CIA agents who had left, Edward Snowden, revealed to the public the confidential information. The same thing actually happened in the reign of the previous President of Indonesia Susilo Bambang Yudhoyono. Snowden in his document also stated that New Zealand also spied on Indonesia and a number of islands along the Pacific Ocean in 2009 [3].

International law also specifically regulates spying activities carried out during war which under the 1907 Hague Regulations, Geneva Conventions, and the Geneva Additional Protocol clearly stipulates that spy activities carried out by part of the armed forces can be captured and obtain status as a prisoner of war [4]. Meanwhile, the regulation related to spying in a peaceful situation is not specifically regulated in international law. Even the literature related to the legal status and whether or not spying in a peaceful situation under international law is still less.

In its current development, spy activities are carried out using the latest technology so that they can obtain confidential information easily, quickly, and without being known from the destination country. Currently, espionage practices are mostly carried out by using spy experts who are reliable computer hackers who can break into the target computer's internet network in order to obtain information illegally. This modern spy activity, of course, requires regulation in international law, bearing in mind that both the Hague and Geneva rules only regulate traditional spy activities [5].

According to the NATO report, almost every day there are one hundred attacks or cyber disturbances directed at NATO headquarters and there are more than one thousand attacks directed at the United States military information system network [6]. This cyber-attack is a bit complicated because it does not only originate from one particular country but is carried out by cyber spy agents originating from more than one hundred different countries. If this is left without rules, it will be dangerous and threaten the country's sovereignty and security. As happened in the United States, spy activities from Russia who tried to be able to access the 2016 presidential election information system violated the principle of non-intervention and caused unrest for the people of the United States.

The absence of rules in international law related to the existence of spy agencies or organizations as well as spy activities that seek information illegally both traditional and cyber means causes legal uncertainty. This has become the focus of research for conducting normative research activities related to the legality of cyber spy activities, their implications for diplomatic relations, and the responsibility of the state conducting cyber spy activities.

2. THE SCOPE OF CYBER ESPIONAGE

The practice of spying is commonly known as espionage or espionage or spying. This activity is a criminal offense with the aim of collecting, transferring or eliminating information relating to national defense with the intention that the information can be used to harm the country or for the benefit of other nations [7]. Espionage can be defined as "attempts to penetrate enemy systems with the aim of extracting sensitive or protected information" [8].

There are also several other terms that are commonly used to describe someone's activities as a spy, including:

a. Spies is a person because of his work sent to the enemy camp to ensure the strength, will, and movements of the enemy, to then convey that information in secret to the authorities, then under international law, the person can be sentenced to death.
b. Clandestine is an activity carried out in secret and hidden in order to achieve an unauthorized goal.
c. Intelligence is intelligence activities that can be interpreted as activities to obtain news or information about important matters or confidential information.

The aim of the cyber espionage is to get important information about the movement and development of targets and other military-related matters or retrieve information about opponents' policies and plans. So now, countries in the world use cyber espionage for further national interests. There are several reasons why a country chooses to engage in cyber espionage such as for military strategy, to know the development of a country, and for the commercial benefit of the country.

Cyber espionage can be used to gain strategic military advantage against enemies. The way is by command or command and control system (C4i system), all military planning can be obtained and followed up to fight the enemy [9]. It can be used as cyber espionage as a tool used to spy on the development of a country and take important documents from a country to be investigated or for certain interests.

A country that supports cyber espionage to gain the commercial interests of enemy countries. This is used to get Research & Development (R&D) from other countries to improve the national economy. The most recent example involving network device manufacturers Cisco and Chinese company Huawei Technologies Co., Ltd. 2003, Cisco filed a lawsuit against Huawei on the grounds that they had violated copyright and directly copied information in the form of source code relating to the most prominent Cisco market, IOS system operations used on routers [10].

3. THE ABSENCE OF INTERNATIONAL LEGAL FRAMEWORK

Cyber espionage also has not received special arrangements and discussion in international law. However, there have been arrangements for cyber-crime through the Hard Law Convention on Cybercrime. The Convention on Cybercrime was created and signed in Budapest, the member countries of the Council of Europe since November 23, 2001, but only came into force in 2004. Until now there are forty-three-member countries of the Council of Europe who signed this convention, thirty-two countries have ratified it. There are also non-European countries that have signed this convention. This convention aims to harmonize the law of the member states, both material law and procedural law, including arrangements regarding international cooperation in dealing with cyber-crimes [11].

The provision of the Convention on Cyber Crimes provides an authority of each member state to adopt the provisions of the Convention into its domestic rules to provide guidelines or sanctions if there is a crime in the form of obtaining access to information illegally and without seizing from the country concerned. In the context of cracking down on the perpetrators of these crimes, this Convention provides access to extradition and legal assistance to resolve the crime of illegal information retrieval [12].

4. DIPLOMATIC LAW APPROACH

4.1. Gathering information under Vienna Convention 1961

The function of diplomacy in Elme Plischke's view is: "Representation, reporting, communication, negotiation, maneuvering, besides caring for national interests abroad" [13]. This means that diplomatic functions are also as representatives of state interests, symbolic representatives, obtaining information, advancing and protecting national interests, and decision making by diplomats.

In foreign relations, information is the main capital in the practice of diplomacy. Collecting information in a country by all legal means and conducting analysis and reporting information to sending countries, is not an activity that violates international law. Article 3 (1) (d) of the Vienna Convention 1961 states that, "Ascertaining, by all lawful means, conditions and developments in the receiving state and reporting there to the government of the sending state". Obviously, the envoys referred to this provision are diplomatic representatives or ambassadors of sending countries to the recipient country as a form of opening diplomatic relations, as well as a form of seeking legitimate information on the development and conditions of the recipient country [14].

Then there are several articles in the 1961 Vienna Convention concerning how a diplomatic relationship between countries through diplomatic representatives / missions should go well, without harming or disturbing the sovereignty of a country. Article 41 (1) of the Convention mentioned that without prejudice to their privileges and impunity, it is the duty of all those who enjoy those privileges and impunity to respect the laws and regulations of the recipient country. They are also obliged not to interfere in the country's internal problems. The same article also regulates at the second section: the diplomatic premises may not be used in a way that is not consistent with the mission function as set out in this Convention or by general rules of international law or special agreements that apply between the sending and receiving countries [14].

From those provisions, it can be concluded that the acquisition of information related to the situation and conditions in the recipient country can be carried out as long as it does not conflict with the recipient's domestic law and international law in particular as stipulated in the 1961 Vienna Convention. Then diplomatic features guaranteed by the Convention Vienna 1961 was only given as long as the diplomatic agent carried out according to the functions and missions given. They are also obliged not to interfere in the internal affairs of the recipient country.

Cyber espionage which is basically an illegitimate search for information in an international diplomatic relationship, because it is clandestine without the target's knowledge in search of information be it political, economic, military and other information (spying), and hacking a network the computer even to the form of theft of important data targets. Cyber espionage committed by one country against another country can be said to violate the provisions in international diplomatic law, because the practice of cyber espionage is not in accordance with the provision of the Vienna Convention 1961. Illegal means of gathering information violates three basic foundations of the treaty, such as: the search information must be carried out in legal ways (article 3 (1) (d), any activities done by a state must in line with the promotion of friendly relations" between sending and receiving countries (article 3 (1) (e), and most importantly mutual agreement shall also be honored (article 2).

Obtaining information from the other states by employing the methods of cyber espionage is a violation to the Vienna Convention 1961. The information includes about a country's economy, circumstances of a country, and can also monitor troop movements in this matter relating to the military or taking data / information about the opponent's government policies and plans in secret as well as other objectives that are clearly detrimental to a country.

Even though Vienna Convention 1961 has regulated how to search for information by all legal means through diplomatic missions / representatives and explained that diplomats and their staff have privileges and impunity does not mean the search for legitimate information through diplomatic missions to a country has no limitations in it. Their activities shall not in contradiction with the function of the mission and promoting the non-intervention principle.

4.2. Effect of Cyber Espionage to the State Diplomatic Relations

Cyber Espionage, which is a violation of international diplomatic law, certainly has its own impacts on the diplomatic relations of a country, especially on countries that are objects of cyber espionage and on the countries of cyber espionage actors themselves, both small impacts and large impacts on a relationship international diplomatic among these countries. What is clear, a cyber espionage practice carried out by the state against other countries has its own impact and consequences because basically cyber espionage is an act that is considered illegal and is not good in a diplomatic relationship.

One impact experienced by cyber espionage object countries as in the case of cyber espionage in general is the loss of documents, data or even important information held by a country, which basically these important documents or data are usually associated with important documents, data or information about the military, economic, political and information policies of a country's government and the activities of the country's top brass. Of course, documents, data or important information hacked by cyber espionage countries against their object country should be part of the privacy of a country itself. Because documents, data and important information of a country should be a consumption and confidential that must be maintained by the country itself, without intervention or spying from other countries who are trying to find benefits from the practice of cyber espionage. Losses obtained by the cyber espionage object state can be said to be a material loss that is important information or important data that is confidential, because of the impact that causes the loss or theft of documents, important data and information that should not be consumed by the state other. Another disadvantage that may be suffered is the damage to the object's state computer system due to viruses left by cyber espionage actors, this is indeed rare because in most cases cyber espionage the perpetrators only spy, retrieve and steal important data of the object state and as much as possible leaving the target computer and internet network without a trace so it is difficult to track by the espionage cyber object's state.

The impact then is that the espionage cyber object state becomes uncomfortable and disturbed by the cyber espionage practice carried out by the offending country so that it will lead to heated diplomatic relations between the two countries and can even cause damage or a break in diplomatic relations between the espionage cyber object state and the offending state cyber espionage

The impact then is that the espionage cyber object state becomes uncomfortable and disturbed by the cyber espionage practice carried out by the offending country so that it will lead to heated diplomatic relations between the two countries and can even cause damage or a break in diplomatic relations between the espionage cyber object state and the offending state cyber espionage.

This usually begins with the temporary withdrawal of diplomatic representatives from the object countries of countries that practice cyber espionage against their country as carried out by Indonesian President in 2009 Susilo Bambang Yudhoyono who withdrew his diplomatic missions from Australia due to the Australians who tapped him and officials Indonesian high. This is a form of protest against what is done by the espionage cyber perpetrators who spy on and even steal and retrieve important data and information on the espionage cyber object country which is very detrimental to the country. So that the 'temporary withdrawal' of diplomatic missions in the country of cyber espionage is usually done as a form of early warning that cyber espionage of their country is undesirable and violates the norms in conducting good diplomatic relations and is an act that is considered unpleasant by a country.

Withdrawal of mission / diplomatic representation from the recipient country is based on the legacy rights owned by each independent country. Which is the right of legacy being the right / authority of each country to open or not open diplomatic relations with other countries. the right of legacy itself is divided into two, namely the active right of

legacy which is the right of the state to send its representatives to other countries, and the right of passive legacy is the obligation of a country to receive representatives from other countries.

In this case, it is legitimate if the espionage cyber object country makes a temporary withdrawal of its mission / diplomatic representatives from the espionage cyber perpetrators as a form of protest over the actions taken by the cyber espionage perpetrators. As was the case with former Indonesian President Susilo Bambang Yudhoyono of Australia in 2009. The cyber espionage object country in this case as the sending country has the right to decide whether or not the country wants to reopen the diplomatic relations after the cyber espionage case occurs, and whether the cyber espionage object country will send its diplomatic representatives back to the espionage cyber perpetrators. All of that is the right of legacy from the espionage cyber object state. Legation rights themselves are recognized in the Havana Convention of 1928 through Article 1.

Then this is reinforced by the provisions contained in Article 2 of the 1961 Vienna Convention, which in an opening of diplomatic relations must be followed by mutual agreement, or in other words there are agreements that have been agreed in the opening of diplomatic relations between the countries. So that if these agreements are no longer reached, each country has the right at any time to break / end a diplomatic relationship between the countries concerned, and no longer conduct diplomatic relations because there is no more good faith and agreement reached between the two parties. This is generally marked by the withdrawal of mission / diplomatic representatives to their home countries both temporarily and permanently.

In the following cases, if efforts to resolve the problem through negotiations by diplomats or the leaders of the country fail and there is no apology from the perpetrators of the state for the cyber espionage actions, and the cyber espionage activities have not been stopped against the object state, it will make things worse. between the two, then a diplomatic mission can be completely terminated completely by the cyber espionage object state by markedly withdrawing diplomatic representatives to their country of origin permanently and severing diplomatic relations between the two. In accordance with the provisions contained in Article 43 of the 1961 Vienna Convention that there are two reasons for the end of the permanent diplomatic mission function, namely:

a. Upon notification by the sending country to the receiving country that the function of the diplomatic agent has ended.
b. Upon notification by the receiving country to the sending country that, in accordance with paragraph 1 of article 9, the recipient country refuses to recognize the diplomatic agent as a member of the mission.

This is usually followed by the declaring of non grata persona by the cyber espionage object state to the diplomatic missions of the offending country in his country. This is consistent with what is explained in article 9 paragraph 1 of the 1961 Vienna Convention namely: "The recipient country may at any time and by not explaining its decision, notifying the sending country, that the head of mission or a member of the mission staff is a persona non grata, or that a person Other staff member of the mission cannot be accepted. In such a case, the sending country would recall the person concerned or dismiss him from his position on the mission. A person can be declared non grata or not acceptable when he arrives in the area of the recipient country.

It can be concluded that the impact of cyber espionage practices on cyber espionage object countries in addition to the impact in the form of material losses (i.e. the theft of data, information or even important documents through computer hackers and sophisticated internet networks). There is also another impact that can be severed diplomatic relations between the two countries by the object state of the espionage cyber perpetrators countries marked by the withdrawal of diplomatic representation / missions from the participating countries both temporarily and permanently, and in very bad circumstances the cyber espionage object countries can persona non grata diplomatic missions / representatives of the state party from their country. Because a diplomatic relationship has been considered so bad and it is felt there is no more good faith in establishing diplomatic relations from the offending country. This demand could ultimately be a prelude to the beginning of active hostilities because the way of negotiations and good relations between the two through diplomatic missions / representatives is considered a failure.

4.3. State Responsibility

Cyber espionage actors in general have various kinds of intentions and objectives in carrying out this illegal practice, which certainly aims and objectives intended for the benefit of the nation and its own country both in terms of military, economic, political, cultural and so forth. In addition, it is the ownership of computer and network systems and sophisticated technology that makes cyber espionage actors able and courageous to carry out this illegal practice, without high-tech internet and computer network systems making it impossible for a country to carry out this illegal practice. Therefore, developing countries such as Indonesia, whose computer systems and internet networks are still considered weak, will become easy targets for cyber espionage objects. Even though in reality it is not only developing countries that are targeted by cyber espionage, but superpowers and having super sophisticated technology such as the United States often get cyber-attacks like this, due to the large amount of important data and information especially in the military, political and economics that can be a reference for other countries to defeat the United States as a superpower, for example countries that often carry out cyber espionage against the United States are Russia, China and China.

Countries that support or become direct perpetrators of spying activities have clearly violated international law and customs [15]. International law experts such as Quincy Wright also agree that cyber spy activities significantly violate the state's obligation to respect the territorial sovereignty of a country [16]. From this argument it can basically be concluded that cyber spy activities constitute a form of violation in international law and practice, in particular a violation of the principle of non-intervention and state sovereignty that is universally applicable

internationally. If this violation causes a great loss to the country whose information has been stolen then responsibility will arise from the state that perpetrates cyber espionage activities.
An act of the state which can be blamed according to international law will automatically give birth to international responsibility for that country. For this reason, according to the 2014 International Law Commission Draft Articles (hereinafter referred to as the ILC Draft) as a customary international law instrument governing state responsibility determines when a country's actions can be said to be wrong. Referring to Articles 1 and 2 of the ILC Draft of a country's actions can be blamed according to international law if first when the acts can be attributed to the country (attribution of conduct to a state) and second when the actions of that country have violated its international obligations [17]. However, the ILC Draft does not restrict when a country is said to have committed a violation of international law. So, in practice, this is determined through the application of other primary international legal sources.

4.3.1. Actions distributed to the state

In general, the applicable provisions in this matter are that only the actions of state organs, the government and / or its officials (persons or entities that act based on orders / directives, recommendations, or supervision of these organs) can be attributed to the state. These organs include organs of national, regional, and local government and individuals or entities at any level, or any person or entity that holds the status of an organ of government based on the national law of a country. It also includes people who actually act as organs of government even though they are not classified according to the national law of the country concerned. Countries that support an intelligence organization or a spy organization if there is a direct link, this support can be distributed to the state's responsibility if the organization's activities are found to have carried out an activity that is not legal according to international law and is detrimental to other countries.

4.3.2. Violation of an international obligation

Even if an act can be attributed to a country, to bear the existence of state responsibility, the act must be proven to be a violation of an international obligation of the country concerned. To determine whether there is a violation of an international obligation, the ILC Draft provides that it must be determined on a case-by-case basis. Meanwhile, it is also determined that a country's actions are not considered to violate international obligations if they occur before a country's obligations are bound by an international obligation. Particularly for participants of the ratification of the Convention of Cybercrime, whenever there is a state ratification of this Convention, acts of cyber spying which constitute one of the crimes in this Convention, state responsibility will arise.

5. CONCLUSION

Spy activities initially carried out traditionally are still far from the touch of modern technology. Generally, the state conducts spy activities through diplomatic representation. However, in the 21st century, espionage activities have become more sophisticated using internet networks and high-tech computer systems which are often referred to as cyber espionage. A cyber espionage act committed by a country against another country is a violation of the provisions of international diplomatic law, namely violating the provisions contained in the articles of the Vienna Convention of 1961. The related articles are Article 3 paragraph 1 letter d the 1961 Vienna Convention on "one of the functions of the diplomatic mission to search for information on the recipient country was carried out in legal ways". Article 2 concerning an opening of diplomatic relations occurs with a "mutual agreement". And Article 3 paragraph 1 letter e concerns a function of diplomatic missions, namely "promoting friendly relations" between sending and receiving countries, and establishing economic, cultural and scientific relations. Cyber espionage is also considered to violate international customary law not to intervene in other countries, and not to take any form of action that is detrimental to other countries.
The diplomatic missions / representatives who are official representatives for their country in the recipient country, also have their own rules and restrictions in carrying out their duties. As stated in Article 41 paragraph 3 of the 1961 Vienna Convention concerning diplomatic missions / representatives not to abuse the building in this case and all its facilities for an activity that is not in accordance with the function of the diplomatic mission, or general rules of international law / special agreements in force between the sending and receiving country. And Article 41 paragraph 1 of the 1961 Vienna Convention concerning diplomatic missions / representatives to respect the legal rules of the recipient country and not interfere in the internal affairs of the receiving country.
Cyber espionage as an act that violates the provisions in international diplomatic law, has its own impacts on a diplomatic relationship between countries, especially countries that are objects of cyber espionage and countries that engage in cyber espionage. Some of these impacts are Losses obtained by the cyber espionage object state, namely the successful theft, or even loss of some data, documents, and important confidential information due to the practice of cyber espionage by the offending state against its country. Other losses that may be suffered are damage to the object's computer system in the country due to viruses / malware left by cyber espionage actors. Meanwhile, for espionage cyber actors, espionage practices can be a thing that can benefit their country, because with information and data obtained from cyber espionage activities, the information and data can be used to advance the country's military technology, knowing economic strategies and policies that are being carried out even by the object state and other benefits that are rationally impossible to obtain from diplomatic missions in the object state. The perpetrators of these cyber espionage activities can be held to account internationally because they have violated international law and customs, especially in violation of the

principle of non-intervention and sovereignty and if they cause harm in other countries.

REFERENCES

[1] J. A. Richmond, Spies in Ancient Greece, 45 (1) Greece and Rome 1, 1998, pp.15-18.

[2] Mark M. Lowenthal, "Intelligence: From Secrets to Policy", London: Sage Publications, 2015, pp.75-80.

[3] "New Zealand Spying on Pacific Neighbours and Indonesia: Snowden Documents", accessed from https://www.reuters.com/article/us-newzealand-spying-pacific/new-zealand-spying-on-pacific-neighbors-and-indonesia-snowden-documents-idUSKBN0M104R20150305 dated 20 January 2018.

[4] The Hague Convention Respecting the Laws and Customs of War on Land, article. 29. Additional Protocol to the Geneva Conventions of 12 August 1949 and relating to the Protection of Victims of International Armed Conflicts, article 46 (2).

[5] Walter Gary Sharp, "Cyber Space and the Use of Force", The United States: Aegis Research Corp, 1999.

[6] Siobhan Gorman dan Stephen Fidler, "Cyber Attacks Test Pentagon, Allies and Foes", Wall Street Journal, accessed from http://www.wsj.com/articles/SB10001424052748703793804575511961264943300 dated 21st of May 2018.

[7] Arlina Permanasari, "Pengantar Hukum Humaniter", Jakarta: Internasional Comite of The Red Cross, 1999, p. 89.

[8] Thomas Rid, "Cyber War Will Not Take Place", in Karin Kosina, "Wargames in the Fifth Domain", Thesis, Vienna, 2012, p.22.

[9] "Cyber Espionage Otherwise Known as Cyber Spying Information Technology", Essay, 2012, accessed from http://www.ukessays.com/essays/information-technology/cyber-espionage-otherwise-known-as-cyber-spying-information-technology-essay.php 23 June 2018.

[10] Marguerite Reardon, "Light Reading", 2003, accessed from Huawei: Cisco Code Is Gone: http://www.lightreading.com/ethernet-ip/huawei-cisco-code-is-gone/d/d-id/590745?piddl_msgorder=asc#msgs 26 June 2018.

[11] Josua Sitompul, "Cyberspace, Cybercrimes, Cyberlaw: Tinjauan Aspek Hukum Pidana", PT. Tatanusa, Jakarta, 2012, p.107.

[12] Convention on Cybercrime, 2004.

[13] Ambarwati, et. al., "Hukum Humaniter Internasional Dalam Studi Hubungan Internasional", Jakarta: PT. RajaGrafindo Persada, 2009, p. 114.

[14] Vienna Convention 1961, art. 3 (1)

[15] Manuel R. Garcia-Mora, "Treason, Sedition, and Espionage as Political Offenses Under the Law of Extradition", 26 Pittsburgh Law Review 65, 1964, pp.79-80.

[16] Quincy Wright, "Espionage and the Doctrine of Non-Intervention in Internal Affairs", Essays on Espionage and International Law, Ohio State University, 1962, p.12.

[17] Malcolm D. Evans, International Law, Second Edition, Oxford University Press, New York, 2006, p. 459.