Humanities & Social Sciences Reviews
eISSN: 2395-6518, Vol 7, No 3, 2019, pp 38-44
https://doi.org/10.18510/hssr.2019.736

ANALYSIST OF CYBER ESPIONAGE IN INTERNATIONAL LAW AND INDONESIAN LAW

Satria Unggul Wicaksana Prakasa[1], Noviandi Nur P.E.[2]
[1]Faculty of Law Universitas Muhammadiyah Surabaya, Lecture at Departement of International Law, Surabaya, Indonesia, [2]Undergraduate Student at Faculty of Law Universitas Muhammadiyah Surabaya, Surabaya, Indonesia
E-mail: satria@fh.um-surabaya.ac.id

Article History: Received on 3rd February 2019, Revised on 25th March 2019, Published on 2nd April 2019

Abstract

Purpose of Study: A conception of cyber espionage today is extremely vulnerable since the crime has evolved from conventional wiretapping into cyber-based spy activities. This issue becomes complicated when faced with the principle of sovereignty and how the challenge of countries around the world to respond in maintaining the honor, security, and peace of their own countries. The legal issues raised in this legal research are: (1) cyber espionage is one kind of cybercrime (2) Legal mechanisms to crack down on the international legal system and national law again Cyber espionagecrime.

Methodology: Research methods used statute approach and conceptual approach.

Results: The result of this research showed that it could use computing devices and internet network by means of spies, destroying computer system in order to securely obtain state confidential data or by spreading internet virus which is sporadic to government-owned domains and corporation it is clear that cyber espionage id either part of the cybercrime.

Implications/Applications: The lack of legal regulation, both international and national which directly refers to cyber espionage because they alluded to illegal access and illegal interception related only.

Keywords: *Cyber Crime, Cyber espionage, Legal Regulation, Indonesia, international law*

INTRODUCTION

The era of globalization which be signed by all things related to internet activity is quite complicated, namely the emergence of types of crime. At least there are some cases conducted by Hackers has been done activities of chaos of the state systems with the intent and purpose to disrupt the political stability and security of a State or more extreme the crime of cyber aims to overthrow a system of government, from such developments that the new modus operandi was born from the Espionage in the IT world, which could be called Cyber-espionage.

As we know, what happened to Jullian Assange, an Australian journalist who was found hacked important documents of the United States (US) that can be classified as violating the crime of Cyber espionage, because unlawfully, the chairman who is also spokesman of WikiLeaks Has been spreading virally against the international community, in this context the sovereignty of US law is being threatened, and in the end, even if he got another type of crime, that is sexual harassment, Julian Assange is arrested by US law authorities for violating the provisions of the 1917 Espionage Act. Many argue that the US has violated the freedom of expression of Julian Assange because in the US Espionage Act 1917 it is not clearly regulated whether Cyber espionage is one of its regulatory territories, if it is not a regulatory competence, The charge against Julian Assange is considered legally flawed. Not only that, the State of Indonesia is also affected by blow-ups issued by WikiLeaks, cyber espionage events have also been experienced by the family of President SBY in 2013, that befell the First Lady Ani Yudhoyono who her cell phone being tapped and conducted by the Australian Government and sent to the representative CIA in Canberra, it is related to the discourse of succession Ani Yudhoyono who will advance in the Presidential Election 2014 and preparing Harimurti Yudhoyono as the Presidential Candidate in the 2019 General Election. (http://www.merdeka.com/peristiwa/the-australian-ungkap-alasan penyadapan-sby-dan-ani-yudhoyono.htm, (Accsess 16 April 2017)) The issue concerning Julian Assange and WikiLeaks is enough to attract the attention of the international community.

Not long ago, after Julian Assange appeared another name of cyber espionage where this time the culprit was an "insider" of the US secrecy system, he was Edward Snowden, who was mentioned as the most wanted fugitive by the US State because besides he is a former member of the National Security Agency (NSA), also because Snowden exposed many secret intelligence data and even wiretapping results from the US State to other States, He is now a fugitive, faced with extradition and face jurisdiction of US State law, problems arise When Snowden gained political asylum and always managed to escape

from his fugitive, starting from Brazil, Hong Kong (http://www.theguardian.com/world/2013/jun/11/edward-snowden-nsa-whistleblower-profile, (Accsess 16 April 2017), a) and currently receiving asylum from the State of Russia. Snowden is considered to be a party to other countries as a whistleblower for spying that is deemed to have contradicted the manners of international affairs which the United States has slammed, torn into a "hard slap" for US national honor in the international eyes, and one of the people which must be held accountable is Edward Snowden himself.

One of the many cyber espionage patterns and crimes committed by both Julian Assange and Edward Snowden or that befell the former President of Indonesia in 2014 is actually the same, that is hacking the system of data and confidential information of a State in order to create instability of government good state Who became the spy agency and the state being spied on. The conception of cyber espionage today is extremely vulnerable since the crime has evolved from conventional wiretapping into cyber-based spy activities. This issue becomes complicated when faced with the principle of sovereignty and how the challenge of countries around the world to respond to in maintaining the honor, security, and peace of their own countries.

LEGAL ISSUE

Looking at the facts and backgrounds above, the legal issues raised in this legal research are:

1. *Cyber espionage* as one part of Cybercrime.
2. Mechanism of the international legal system and a national law against Cyber-espionage Crime.

RESEARCH METHODS

Legal writing using statute approach. An approach in legal research as a process of finding the rule of law, doctrinal legal principles to address the issue of the law being raised. This approach goes from legal regulation in both the international and national law aspects, both vertical and horizontal, to study the rules of law that are parallel or hierarchical. (http://www.theguardian.com/world/2013/jun/11/edward-snowden-nsa-whistleblower-profile, (Accsess 16 April 2017), b)

Through a conceptual approach by analyzing the analysis of cyber-espionage crime in the mechanisms of international law and Indonesian law based on doctrine and the views of experts and conceptual and theoretical views, it aims to solve legal issues proposed not only by the approach of legislation Solely that is limited (Wjiayanti, 2011).

RESULTS AND DISCUSSION

History of Cyber Crime and Cyber Espionage

The era of globalization has been favored, with the presence of the Internet and the World Wide Web, human connectivity around the globe increasingly unlimited, it is also coupled with the complexity of the issues that overshadow it, in addition to security issues, other issues such as new modus operandi of crime, especially in the cyber world emerging, The problems of cybercrime into Pandora boxes that we can not avoid, but we can not ignore too. (Gragido and Pirg, 2011) History records, in 1960-1970 providing reporting on computer manipulation, computer sabotage, computer espionage and illegal systems known by the world community, from conventionally known crimes at that time changed the pattern so that the form of the crime changed. (Clough, 2010)

Furthermore, the term Hacker was first raised in 1985 when some people tried to steal data and could break the computer defense mechanism through the mechanism of the computer itself, the term is derived from the Yiddish language which means the furniture maker is not important, the term has experienced a significant development And there has been an extension of meaning different from that terminology.

In the modern era is precisely posted 2000s, all the process of human relationships increasingly borderless, not looking at him from where the pattern of interaction is unlimited, even all things have been connected without any obstacles with the Internet itself, there is even a term that states " Our lives, our entertainment, our finances, and our identities, like it or not, are interwoven in a web of 1s and 0s, which exist in a virtual plane of our creation. " (Gragido and Pirg, 2011), in such a deterministic era to the internet, the problem of the security of access to the Internet is also more prone, especially regarding the confidentiality of the State and other state documents, the emergence of one form of modification of new crime in the cyber world of cyber espionage, then There should be an attitude that the crime does not cause more destructive effects.

Understanding Cyber Crime

By definition, Cybercrime according to Bernadette H. Schell and Clemens Martin call it is a crime related to technology, computers, and the Internet. The majority of publicized cyber crimes that concern governments, industry officials, and citizens worldwide include. (Bernadette H. 2004; Selomo and Govender, 2016)

Furthermore, Wall in his book Crime and internet, gives the definition of cybercrime as a due to the legal vacuum that regulates the universal cybercrime has created a variety of interpretations and arises uncertainty of understanding because between the parties both policymakers, academics, and the digital community does not have the same understanding and perspective and set forth in the rule of law is clear. The impact is how the law of the cyber criminals will be difficult to touch. (Wall. 2001 n.d.)

Meanwhile, according to Elliot Turrini and Simon Ghros, who gave the definition of cybercrime and its technical description the cybercrime process is a process of breaking the computational system that is arithmetically arranged and logical reasoning, therefore in the element of cybercrime is who can control the computing and managed to control the function of the computer itself then he can be categorized successfully launched the crime cyber. The analysis of Elliot Turrini and Simon Ghros is very technical and related to the mechanism of computational work, not in the aspect of the modus operandi and what motives the background of a hacker perpetuates the cybercrime. (Ghros and Turrini, 2010; Merkibayev et al., 2018)

Of the three definitions, the definition of cybercrime is not restricted by the rules of international law that applies universally, but we can know that the scope of cybercrime is from the means of infrastructure to commit such crimes through computer equipment, the Internet and the target is to damage the computing system and Disseminating data obtained or even damage an internet domain with the purpose of both profitable and non-profitable.

Understanding Cyber espionage

If previously discussing about cybercrime, then this time the discussion is about Cyber espionage, two intersection themes that is cyber and espionage, then in what aspect becomes the difference between conventional espionage with espionage in cyber aspect.

In terminology, according to the Oxford Dictionary, Cyber espionage means: the use of computers networks to gain illicit access to confidential information, typically that held by a government or other organization: 'improving cybersecurity across government agencies is crucial given the increase in cyber espionage'. (http://www.oxforddictionaries.com/definition/english/cyber espionage, (Accsess 16 April 2017) n.d.) In that sense, it can be understood that cyber espionage is the use of computer networks to gain access to confidential data information held by the government or an organization by destroying the network.

In his work, Will Gragido & John Pirg, tried to reflect on the cyber espionage phenomenon that caused the disability in those countries, that the attacks of cyber espionage were targeted to the State and also the credibility in order to create a national commotion. The reflection, mostly from Government and corporations, does not feel directly or even indifferently to the losses caused, it is related to the avoidance effort to get gaining, branding, & positioning of cyber espionage actors is not high and national stability is not disturbed. Gragido and Pirg (2011) In this context, Will Gragido & John Pick provides restrictions and descriptions of cyber espionage and is associated with the effects.

In retrospect, the notion of espionage that we consider to be the most convenient method is implied with the understanding- ing in the US State of espionage by Glen Peter Hastedth in his book Spionase; Contemporary World Issues as follows: espionage is not an activity that is directed solely at military targets. Espionage is a means of acquiring information that would otherwise be unavailable. Espionage is the act of secretly collecting information. Americans more commonly refer to it as spying. Though in the United States people tend to associate spying with the Cold War, it is an age-old activity. By necessity espionage occurs out of sight; only occasionally does it burst out of the shadows and into the open. However, even then a full picture rarely emerges. People find bits and pieces of evidence that point to an explanation for why an act of espionage occurred or how it was discovered, but important questions frequently remain unanswered long after the fact. (Glen Peter Hastedth Espionage; 2003 n.d.)

The term espionage is concerned with the tacit collection of information, and the US is more likely to say that espionage is related to spying. This term shifted especially after the end of the Cold War, that the term espionage is not understood as an activity of militarism in wartime, but more than that, espionage sought out secret data that should not be available, and in this aspect, one of the most relevant tools for Used is the IT component.

Types and Elements of Crime

The types and elements of the crime of cyber espionage need to be discussed further in this sub-discussion so that further categorization of the crime into one part among cybercrime can we analyze easily. Cyber espionage which is the development of espionage itself on the substance is the same, the main target of this crime is to the defense and security of the State both in the aspect of government and multinational corporation by leaking confidential data or destroying networks and information systems and data of confidentiality of a country with the aim Creating instability in the condition of the State being attacked, with technological developments, espionage attacks irrelevant as they used to be, meaning that with the help of these technological developments it is difficult to anticipate these crimes. As for the evil elements of cyber espionage is no other than the penetration of access to the central sites of the State both in order to steal confidential documents, destructive computing system, even damage it with cyber-attack through computer viruses to State agencies or corporate destinations directed by The Hackers.

Freddy Haris gives a description of cybercrime with its characteristics that are: (1) Unauthorized access: it aims as a means of launching its crime. (2). Unauthorized alteration or destruction of data. (3). Destructive nature of a network and computing system. (4). Perform weakening and create an error of access to computer networks. (Didik M. 2009 n.d.)

Cyber espionage One Part of Cybercrime

By using computer devices and Internet networks by means of spying, destroying computing systems in order to securely obtain state confidential data or by sporadically spreading Internet viruses to government-owned domains and corporations it is clear that cyber espionage is either part of the Cyber Crime law, there needs to be a legal mechanism that can combat such cyber crimes so that the honor and sovereignty and stability of the State can be protected.

International and National Law Regulations Regarding Cyber Crime And Cyber Espionage

International Law Regulations Regarding Cybercrime and Cyber espionage (The Hague Convention 1907 respecting the Laws and Customs of War on Land and its annex: Regulations concerning the Laws and Customs of War on Land)

Long before the international community became aware of cyber espionage, in 1907 in one section under the provisions of international humanitarian law discussing the conventional espionage which can also be associated as spy activities during the war period, the provision is in Article 29, Article 30, Article 31 The Hague Convention 1907 respecting the Laws and Customs of War on Land and its annex: Regulations concerning the Laws and Customs of War on Land or abbreviated to The Hague Convention 1907.

In Article 31 of the Hague Convention of 1907 explains the linkage of spy and espionage: A spy who, after rejoining the army to which he belongs, is subsequently captured by the enemy, is treated as a prisoner of war, and incurs no responsibility for his previous act of espionage. In the provision in question is a spy can be forgiven when doing espionage when he has captured the enemy and doing it as a prisoner of war. Means a spy and espionage activities can be allowed during the war as their way (measures) of attacking the enemy.

In the Protocol addition to the Geneva Conventions of 12 August 1949, and relating to the protection of victims of international armed conflicts (Protocol I) provides an illustration of what is meant by the Hague Convention of 1907 on humanitarian law, which contains the following that espionage activities are prohibited and different perceptions with what is contained in the provisions of the Hague Convention of 1907, wherein the provision that when a combat falls into the power of the disadvantaged and actually performs espionage then the punishment is given as a spy. That is one point among the other provisions in this article which deal with espionage conventionally and is considered to be a part of humanitarian law, its current development of espionage activities is not only done by combatant or not the ancient wiretapping methods, with the development of cyber espionage it can be said espionage in The Hague convention 1907 and the Additional Protocol I of 1977 was less relevant and did not accommodate how to crack down on the crime.

Budapest Convention on Cybercrime, Council of Europe (Europe Treaty Series No.185)

In 2001 in Budapest, Hungary was agreed between the EU Member States through the Council of Europe to make an agreement is Convention on Cyber Crime, although limited to the applicable Member States of the European Union only, but the value of this Convention shall be universal, Because we realize that there is no legal vacuum related to the discussion of cybercrime in international law, if we know that the rules of international criminal law can be found in Rome Statue 1998, but we can not find the latest types of crime one of the cybercrime in umbrella big convention Regarding the international criminal law.

The provisions are not explicitly stated about cyber espionage, but there are several provisions that directly address the issue of illegal access and illegal interception set forth in Articles 2 and 3 of this Convention, the provisions of the law stated that for crimes including illegal access and illegal interception, States parties must act with the provisions of national law for those who do so, unintentionally, without the relevant rights and permission and use the computer system by dishonest entry. In this context, it requires the commitment of the participating countries of the convention to impose national law on two crimes that are actually closely related to the cyber espionage.

ITU Understanding Cybercrime: A Guide for Developing Countries

Cannot be categorized as a legally binding agreement, but the position of International Telecommunication Union (ITU) Understanding of cybercrime: A Guide for Developing Countries is essential in the framework of providing an understanding of cybercrime. Because the principle of this assessment has been given clues about the hunt for cyber espionage so that in this provision can be a reference even if only soft law.

In chapter 2.4.2. from the ITU Understanding Cybercrime explained that the background of the regulation of cyber espionage occurred in the 1980s where a number of German State hackers managed to enter the military computer system of the United States and obtain confidential information and use unlawful means and hack the official website of the State , Or "Phishing" sensitive information relating to trade secrets of the business system. This includes illegal interception via email and other confidential information as well as destruction and removal of data through virus mechanisms and systems.

The unanswered issue in the ITU Understanding Cybercrime provision is how espionage is performed by persons who have access legality to the state websites and then use the data for personal benefit as described above. So in guide principle is trying to give guidance for such case need to be categorized and can be punished like cyber espionage. (ITU, Understanding Cybercrime: A Guide for Developing Countries, 24,28,118,119,120,121. n.d.)

Challenges of Enforcing Cyber Espionage In International Law Mechanisms

With regard to the crime of cyber espionage always related to the cyber warfare crimes committed by countries in the world for the mission of dominance of global power, the US has been a victim of China for cyber espionage activities conducted by People China Liberation (PLA) which is part of the military Republic Chinese People (PRC) led by President Xi Jinping. PLA Unit 61398 has been done cyber espionage activities from 2006-2013 to commit theft of secret data of 100 Terabytes in 14 companies and 20 industries under the responsibility of the US Government which became the motive of the dominance of the global economy. In addition, the PLA by the US is considered responsible for data theft from the government, defense, research, and technology also from the US government. (Benjamin F. 2005; Nazoktabar and Tohidi (2014))

The settlement of the case, the parties prosecuted namely Wang, a company backed by the PLA in cyber espionage activities was convicted by a federal court panel of judges as a cyber espionage act of US trade secrets. Evasion from Wang for being irresponsible as it relates to jurisdiction, but in fact, the US legal authorities claim that cyber espionage committed by Wang and supported by the PLA is not just a mere motive of business competition but with regard to the national security disorder of the United States. Where in the end the publication of the ruling is voiced by US President Barack Obama to PLA and Wang to comply with the legal decision established by the US Federal. Banks (2017)

The US vs China case is one of the few cyber espionage cases that challenge the enforcement of cyber espionage in international legal mechanisms, as the issue of international law enforcement lies in two aspects: (a). Unaccountable jurisdiction and sovereignty to prosecute cyber espionage cases, including those committing crimes being inter-states, which tribunal has the competence to adjudicate; (b). The recognition of cyber espionage crimes as part of an international legal mechanism is also a problem, as there is no international treaty that lawmaking treaties to govern this type of crime; (c). The form of legal liability for cyber espionage crimes is also not regulated, how the mechanism of responsibility and accountability when at the jurisdiction and sovereign points of this crime is recognized by the international tribunal, since the object of the crime committed is in the cyberspace.

Indonesian Law Regulation Regarding Cybercrime and Cyber espionage

The Criminal Code (KUHP)

The provisions on the conventional espionage of the state of Indonesia have been regulated in Law Number 1 Year 1946 concerning the ratification of Wetboek van Straftrecht or commonly known as the Criminal Code (KUHP). In the provisions stipulated in Article 122-Article 125 of the Criminal Code. In that provision has given information about how the espionage

activity is done by someone to the Indonesian military system during wartime with the aim of divulging military secrets (maps, images, and strategy of war) of a State with destructive purpose and creating national noise, hence on It can be punished. The issue in the Criminal Code has not been regulated on cyber espionage, and the limited crime is in the legal aspects of war only. (Banks, 2017; Vlasova et al., 2016)

Law Number 11 Year 2008 regarding ITE and Related Legislation

In 2008, Indonesia has had laws governing cybercrime in the national aspect as well as any regulations relating to such cyber activities. This is stated in Law Number 11 Year 2008 on Information and Electronic Transactions (UU ITE). Article 31 Paragraph (1) provides for unlawful interception: "Every person intentionally and without rights or against the law intercepts or intercepts the Electronic Information and/or Electronic Documents in a particular Computer and/or Electronic System certain belongs to someone else." Interception and tapping in this context not only in the conventional intercepts aspect, but also the tapping of electronic systems.

The exceptions are that wiretapping is allowed when such matter is in the course of a series of legal proceedings and discloses a crime, as mentioned in Article 31 paragraph 3 of the UU ITE, namely: "Except for interception as referred to in paragraphs (1) and (2), interception Shall be carried out in the context of law enforcement at the request of the police, prosecutors, and/or other law enforcement institutions established by law. "

In certain crimes, it is also permissible to intercept and wiretapping itself and be legally permitted by the rule of law of the State of Indonesia. As Law No. 35 of 2009 on narcotics, Law No. 30 of 2002 on the Corruption Eradication Commission, Law Number 21 of 2007 on the Crime of Trafficking in Persons, and Law No. 17 of 2011 on the State Intelligence. For example, in Article 31 of Law No. 17 of 2011 on State Intelligence explains that the provision clearly explains the potential for terrorism, separatism, espionage and sabotage activities that threaten national safety, security and sovereignty, including those undergoing legal process. State Intelligence Agency (BIN) is allowed in order to obtain preliminary information from the provisions.

Lack of regulation of national law that directly refers to cyber espionage because that is only related to illegal access and illegal interception. The intersection between intelligence interests and enormous potential for abuse of cyber espionage in order to create national instability and national defense and security. With these consequences, it is necessary to have clear rules and bindings on the rules of the national law concerning cyber espionage.

CONCLUSIONS AND POLICY RECOMMENDATIONS

1. By using computer devices and Internet networks by means of spying, destroying computing systems in order to securely obtain state confidential data or by sporadic Internet viruses to government-owned domains and corporations it is clear that cyber espionage is either a part of from cybercrime.
2. Lack of legal regulation both International and national that directly refers to cyber espionage because of the only perturbation related to illegal access and illegal interception only, meaning there is the legal vacuum. The intersection of intelligence interests with enormous potential for abuse of cyber espionage in order to create national instability and national defense and security. With these consequences, it is necessary to have clear rules and bindings of both the rules of international law and the rules of national law that become lex specialist regarding cyber espionage.
3. So there needs to be an extension of the meaning of cyber espionage crime, whether it concerns the hacking of secret state data, destructive of secret state sites, and even disturbing public order due to the destruction of the internet network and various other hacking attempts made By the perpetrators of cyber-espionage crimes into international treaties, as well as Indonesian legal mechanisms, so that perpetrators of cyber-espionage crimes may be prosecuted following existing legal jurisdictions.

REFERENCES

Banks, W. C. (2017). Cyber Espionage and Electronic Surveillance: Beyond the Media Coverage. *Emory Journal*, 66(3,3,4).

Clough, J. (2010). Principes of Cyber crime. volume 3 of 4. Cambridge University Press.

Ghros, S. and Turrini, E. (2010). Cyber crime: a multidisiplinary analysis. volume 9 of 10. Springer.

Gragido, W. and Pirg, J. (2011). Cyber crime and espionage; an analysis of subversive multivector threats. *Elsevier Press*,

6(7).

http://www.merdeka.com/peristiwa/the-australian-ungkap-alasan penyadapan-sby-dan-ani-yudhoyono.htm, (Accsess 16 April 2017).

http://www.theguardian.com/world/2013/jun/11/edward-snowden-nsa-whistleblower-profile, (Accsess 16 April 2017).

http://www.theguardian.com/world/2013/jun/11/edward-snowden-nsa-whistleblower-profile, (Accsess 16 April 2017).

Merkibayev, T., Seisenbayeva, Z., Bekkozhanova, G., Koblanova, A., and Alikhankyzy, G. (2018). Oppositions in the conceptual and linguistic category of time. *Opción*, 34(85-2):116–148.

Nazoktabar, H. and Tohidi, G. (2014). Shanty Town and Socio–Cultural Problems in Sari City, Iran. *UCT Journal of Social Sciences and Humanities Research*, 2(2):29–31.

Vlasova, V. K., Kirilova, G. I., and Curteva, O. V. (2016). Matrix Classification of Information Environment Algorithms Application in the Educational Process. *International Electronic Journal of Mathematics Education*, 11(1):165–171.

Wjiayanti, A. (2011). Strategi Penulisan Hukum Normatif. *Lubuk Agung*, 7(8):137–140.