CHAPTER I

INTRODUCTION

1.1 Background

We live in our own virtual world, where we have truly crossed the threshold from humanity to technologically augmented humanity as a result of the rapid development of technology. Along with the human development from time to time, the human need for information and communication encourage them to invent and develop new cutting-edge communication media which gives human the possibility to communicate and disseminate information quickly and precisely. With the process of discovery and development of communication and information media then human invent a technology that can facilitate their communication and information distribution without being hindered by space, boundaries, distance, and time. Information and communication technology have brought people to a new civilization with a social structure and regulated values in such a way that in its development, computers have been invented as a product of information and communication technology.

Computer, based on Law No. 11 of 2008 concerning Information and Electronic Transactions in Article 1 point 14: "a tool that is useful for processing electronic, magnetic, optical, or system data that performs logic, arithmetic, and storage functions."[1]

[1] Pasal 1 poin 14 UU No. 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik "Komputer adalah alat untuk memproses data elektronik, magnetic, optik, atau sistem yang melaksanakan fungsi logika, aritmatika, dan penyimpanan."

The convergence between telecommunications, media, and information technology presents a new tool called the internet. An internet is defined as a globally connected network system that allows for global communication and access to data resources via a vast network of private, public, academic, business, as well as government networks[2].

In 1969 the US Department of Defense, U.S. Defense Advanced Research Projects Agency (DARPA) decided to do a research about how to connect multiple computers until the first computers were connected in the same year. The Network Control Program was then implemented in 1970 alongside with the declaration that the network was operational in 1971[3]. The ARPANET was then divided into two; ARPANET and MILNET that is used for military purposes[4] and that process brings us to the Internet that we know today[5].

By the advancement of technology and the invention of internet itself, it enables us humans to do various activities ranging from communicating, online business transaction, online shopping, and many others so that the existence of internet inadvertently separated real life and virtual life. In addition, the consumption of internet can cause both positive and negative impacts. The positive impacts of the internet include; effective communication using instant messaging services without being hindered by geographical boundaries, improved business interactions, less complicated banking and shopping method, the widespread and easy access for news, the existence of online books and journals for education

[2] Technopedia, "What Is the Internet? – Definition from Technopedia". https://www.techopedia.com/definition/2419/internet. Accessed 16 July, 2022.
[3] Bidgoli Hossein. *The Internet Encyclopedia.* (Hoboken: John Wiley & Sons, 2004)
[4]Science Node, "A Brief History of the Internet". https://sciencenode.org/feature/a-brief-history-of-the-internet-2018.php. Accessed 16 July, 2022.
[5] Stein Scholberg, *The History of Cybercrime: 1976-2014,* (Norderstedt: Books on Demand, 2014).

purposes, easier job application, and enhancing research in general. Alongside the negative impacts of internet usage include; easy availability of illegal and inappropriate digital material, addiction to social networks, hacking and cracking activities including stealing data and/or banking information, and lastly the misuse of internet for spreading hate speech and terrorism[6].

The rapid development of internet results in new concept and theories – one of the most common one is cyberspace. Cyberspace was first introduced by the American-Canadian author William Gibson in the year of 1982 in his book titled *Neuromancer*. In his book, Gibson described cyberspace as the creation of computer network in a world full of artificial intelligence. Initially, the term cyberspace is used to describe the location in which people interacted with one another through the internet – the location of internet consumer is said to exist in the cyberspace. Until the 21st century, more businesses and governmental institutions used web-based discussions for more professional matters and it seem to offer opportunity for public discussion that is not available in real world[7].

Despite the functionality of the internet as a medium for information delivery there are also disadvantages of internet especially in the case of its security. Even though many programs have been developed to protect important data on the internet, many people continue to use it as a means of crime, this act is known as cybercrime.

Cybercrime is any criminal activity that involves a networked device or a network. Most cybercrimes are intended to generate profit for the cybercriminals

[6] Asianet Broadband, "Internet Effects on Society: Positive and Negative Impact of Internet". https://asianetbroadband.in/effects-of-the-internet-on-society/. Accessed 16 July, 2022.
[7] Encyclopedia Britannica, "Cyberspace". https://www.britannica.com/topic/cyberspace Accessed 16 July, 2022.

but some are carried out to directly damage or disable a computer. Illegal cyber activities are executed by spreading malware, illegal information and other digital materials to infect targeted computers with virus[8]. A cybercrime is very hard to detect because it can be plotted in complete privacy, executed from a predetermined location, and leaves a hard to detect footprint; tracking the cybercriminals will necessitate technical expertise given due consideration that a cybercrime leaves almost no trace in the real world making it extremely difficult to gather evidence[9].

Cybercriminals are also known as hackers and crackers. A hacker is someone who is interested in the arcane and convoluted workings of any computer and operating network system – hackers are knowledgeable about operating systems and various programming languages and never have the desire to intentionally damage or steal another person's data. While a cracker is someone who maliciously breaks into a system or otherwise violates the system integrity of remote machines. Crackers destroy data on purpose and cause problems for their targets in general[10].

To prevent crimes committed by hackers or crackers, everyone who uses the internet needs a firm and binding law, but the issue is one of state jurisdiction. Do each country has the authority to prosecute cybercriminals from other countries? So many countries are attempting to have a discussion about the issue. One of the most visible is the Council of Europe's efforts to address cybercrime. The Council

[8] TechTarget, "What Is Cybercrime? Definition from Searchsecurity" https://www.techtarget.com/searchsecurity/definition/cybercrime. Accessed 15 July, 2022.
[9] Deccan Herald, "Cybercrimes Are Hard to Detect". https://www.deccanherald.com/content/634262/cybercrimes-hard-detect.html. Accessed 15 July, 2022.
[10] InformIT, "Hackers and Crackers". https://www.informit.com/articles/article.aspx?p=30048 Accessed 15 July, 2022.

of Europe produced The Council of Europe Convention on Cybercrime, an international convention on cybercrime. On November 23, 2001, this convention was signed in Budapest, Hungary. The convention deals with issues of state interest, such as jurisdiction[11]. As of today, a total of 66 countries have ratified the Convention of Cybercrime – those countries include France, Belgium, Germany as a member of the Council of Europe and Japan, The United States, Philippines as non-members of the Council of Europe to name a few[12].

The concern on multilateral agreement arises ever since this convention was signed and ratified. Take the agreement between Japan and France as an example, on June 10 2008 Japan and France government minister agreed to work together on cybercrime. Japan's Minister of State and head of its National Public Safety Commission, and France's Minister of State, reaffirmed the importance of direct information exchange between the two governments during a bilateral meeting on the sidelines of the G8 Justice and Home Affairs Ministerial Meeting in Tokyo. According to a statement from Japan's National Police Agency, both parties have also committed to strengthening cooperation in combating the complex problem of cybercrime[13].

The regulation on cybercrime in Indonesia existed since 1999 with the enactment of Law No.36 of 1999 concerning Telecommunication. This law did not explicitly regulate about cybercrime as it only touches upon illegal access[14]. Law

[11]"Cybercime: The Council of Europe Convention", Congressional Research Service, Vol. 7, (2006), pg. 4.
[12] Council of Europe Portal, "Chart of signatures and ratifications of Treaty". https://www.coe.int/en/web/conventions/full-list?module=signatures-by-treaty&treatynum=185. Accessed 16 July, 2022.
[13] Computer Crime Research, "Closer Ties on Cybercrime: Japan and France Agreement". https://www.crime-research.org/news/26.06.2008/3428/ Accessed 26 July, 2022.
[14] Law Number 36 of 1999 concerning Telecommunication

No.11 of 2008 concerning Information and Electronic Transactions furthermore outline about cybercrime and cybercriminals – specifically Chapter 7 of the Law concerning Prohibited Acts regulates about illegal cyber matters including the production and distribution of digital information in any form, blackmailing and threats, hate speech, illegal computer access, stealing data and confidential electronic information, breaking through bypass, and breaking into security system until cyberattack that causes loss for other parties[15].

As explained above, all sorts of criminal offenses performed by utilizing the internet is known as cybercrime. Due to the world that continues to evolve, appears a phenomenon of globalization with borderless communication networks and relation between countries are much more borderless than before which makes a country can experience disputes with other countries that are considered to be a friendly country. Moreover, as government and influential actors all over the world always thrives to maintain the standard of living by improving productivity and economic security, the interest in economic espionage escalates in number and becomes one of the most concerning and disadvantaging cyber offense. Economic espionage is the act of illegally gaining ownership over an institution or a company's trade secret to benefit one party, in this case a foreign government which may give impact to a nation's national security. The Canadian Security Intelligence Service herein after referred to as ("CSIS") presented a very comprehensive and very spot on definition of cyber economic espionage[16].;

> "illegal, clandestine, coercive, or deceptive activity engaged in or facilitated by a foreign government designed to gain unauthorized

[15] Law Number 11 of 2008 concerning Information and Electronic Transactions as amended by Law Number 19 of 2016
[16] Canadian Security Intelligence Service Act (R.S.C., 1985, c. C-23)

> access to economic intelligence, such as proprietary information or technology, for economic advantages."

Directly quoting from the United States' Economic Espionage Act of 1996,

> "(a) In general – whoever, intending or knowing that the offense will benefit any foreign government, foreign instrumentality or foreign agent, knowingly – (1) steals, or without authorization appropriates, takes, carries away, or conceals, or by fraud, artifice, or deception obtains a trade secret; (2) without authorization copies, duplicates, sketches, draws, photographs, downloads, uploads, alters, destroys, photocopies, replicated, transmits, delivers, sends, mails, communicates, or conveys a trade secret; (3) receives, buys, or possesses a trade secret, knowing the same to have been stolen or appropriated, obtained, or converted without authorization; (4) attempts to commit any offense described in any of paragraphs (1) through (3); or (5) conspires with one or more other persons to commit any offense described in any of paragraphs (1) through (3), and one or more of such persons do any act to effect the object of the conspiracy shall, except as provided in subsection (b), be fined not more than $500,000 or imprisoned not more than 15 years, or both.[17]"

Nowadays, many countries are accused of conducting economic espionage and cyberspace becomes a preferred operational domain for these kinds of criminal offense[18] that are carried out by various economic espionage actors ranging from antagonistic nation-states, state-controlled businesses, and sponsored operations carried out by hacker groups which results in larger threats to worldwide economic and trade. China, Russia, and Iran are a few of the most capable countries to conduct cyber economic espionage and they are proven to have the capability of stealing the United States' trade secret and confidential information. The United States cyber securities is aware that these three countries will continue to collect sensitive US economic information through the cyberspace and the US has also announced that

[17] Economic Espionage Act of 1996, 18 U.S.C, 1831-1839 (1997)

[18] The Anticorruption Blog, "Series: Economic Espionage and Theft of Trade Secrets". https://www.anticorruptionblog.com/corruption/series-economic-espionage-and-theft-of-trade-secrets/ Accessed 30 July, 2022.

they will keep improving technologies to protect their intellectual property and confidential information.

Supporting the above statement, an economic espionage is typically performed to steal valuable proprietary information such as information in regards to finance, government policy, and technological matters. Economic espionage gives the offender a cheap access to an information and cause severe economic losses for the victims. Economic espionage is very common in the United States and the United States have ratified the Espionage Act but economic espionage keeps on becoming a serious threat in the country. Until now, the United States is still improving their security and technology to overcome and avoid economic espionage. In fact, a strong and developing country like the United States is still facing a major threat of economic espionage, it is safe to say that the Espionage Act does not perfectly close the possibility of economic espionage in the United States. Imagine a developing country like Indonesia, which is also a target of economic espionage yet we have no binding law or regulation as an act of prevention and punishment for economic espionage that might happen. Economic espionage activities will continue to develop especially since entering the industrial revolution phase which makes the invention of transportation and communication technology to conduct espionage becomes more modern and sophisticated.

As we all know, there are ranges of methods of economic espionage and the most used method is through cyber-attacks. Cyber-attacks are meant to steal or destroy information illegally from an organization's computer system which opens their access to sensitive data and those data will be exploited. The most common cyber-attack methods include hacking, phishing, eavesdropping, man-in-the-

middle attack, SQL injection, and exploiting poor security. Hacking is breaking into a software that includes confidential information, phishing is sending email to trick someone with a malicious link, eavesdropping is tracking valuable information through a network, man-in-the-middle attack is postponing a network between users, SQL injection is inserting malicious code into an application to exploit a database, and exploiting poor security practices is making use of a network's security weakness to access a data.

There are also some characteristics to identify economic espionages. Economic espionages are hard to identify because it is almost indistinguishable with normal daily activities since economic espionages can be performed by a highly integrated employee, it is hard to point a perpetrator who is responsible because they are often smart and they are capable of prolonging the legal procedures until it is no longer feasible to continue with the case, economic espionage may also harm the price of stocks since it makes the value of a company falls and no one will be interested to invest in a company where its data has been breached, and lastly it can be seen as a violation of IT requirements, since a company is a hundred percent responsible for its user's personal data sometime the leakage of personal data drags a company to become the one who is in fault where actually this is an act of cyber economic espionage where an offender is trying to acquire personal data information through hacking methods[19].

Aside from the methods and characteristics of cyber economic espionage, it is also important to understand dominant effect of acts such as cyber espionage to the

[19] Ekran, "How to Detect and Prevent Industrial Espionage". https://www.ekransystem.com/en/blog/prevent-industrial-espionage Accessed 1 August, 2022.

economy. Researchers have suggested that the upper limit of cost of cyber espionage is only between 0.5% and 1% of a country's income.

Figure 1.1 Global Estimation Cost for Malicious Cyber Activity

Putting Malicious Cyber Activity in Context			
CRIMINAL ACTION	ESTIMATED COST	PERCENT OF GDP	SOURCE
GLOBAL			
Piracy	$1 billion to $16 billion	0.008% to 0.02%	IMB
Drug Trafficking	$600 billion	5%	UNODC
Global cyber activity	$300 billion to $1 trillion	0.4% to 1.4%	Various

As discussed before, one of the causes of cyber economic espionage is the increase of internet and technology users all around the world, though we need to keep in mind that not all transfer of technology can lead to cyber economic espionage because it is normal for foreign investment. It is wrong to ascribe that all technology transfer leads to cyber economic espionage but we should not ignore the possibility that cyber economic espionage could affect economic growth. Most companies in the world thought that they have everything under control when they become a victim of cyber economic espionage, in a world that has fast growing markets, they can run faster to create new technologies to minimize the loss of espionage. In fact, because of this act cyber economic espionage offenders can absorb the stolen information and produce competitive products, many companies did not realize that they lost in strategic advantages, intellectual property, sales data, customer list, and competitive analysis[20].

1.2 Formulation of Issues

[20] "The Economic Impact of Cybercrime and Cyber Espionage", McAfee, (2013), pg. 16.

This paper addresses the issue of state jurisdiction in dealing with cross-border cyber economic espionage cases in Indonesia since Indonesia has not ratified a law regarding economic espionages, in some measures a solid regulation of jurisdiction towards this crime is strictly needed as effective punishments. Cybercrime is a complex crime that occurs in the borderless realm of cyberspace and is compounded by highly skilled crime groups. Cybercriminals can be found in various regions, and their impact can be felt by societies all over the world, making this an urgent issue that requires immediate international attention.

To narrow the discussion, researcher will limit the problems to be discussed, namely:

1. Is Law No. 11 of 2008 concerning Electronic Information and Transaction significant enough to tackle economic espionage and how is the jurisdictional arrangements in handling cyber cases that occur between countries?
2. How should Indonesia as a non-EU member country adopt the 2001 European Union Convention on Cybercrime determine jurisdiction and give deterrent effect to economic espionage offenders?

1.3 Purposes of Research

The goal of this study is to provide an overview of the regulation regarding cybercrime jurisdiction in Indonesia as well as international legal instruments, in this case The Europe Council Convention on Cybercrime, concerning overcoming the problem of a country's jurisdiction in dealing with cybercrime cases. Aside from

that, the goal of this writing is to solve legal problems, make legal discoveries, and develop legal knowledge in the future.

1.4 Benefits of Research

This research was conducted with the hope that it will provide benefits, both objective benefits and subjective benefits, as follows:

a. Objective Benefit

   The objective benefits of this research are to grasp the knowledge about the application and adoption of the Convention on Cybercrime in countries outside the European Union, such as Indonesia, and the significance of Law No. 11 of 2008 in determining jurisdiction to tackle transnational cyber economic espionage cases.

b. Subjective Benefit

   The subjective benefit of this research is additional knowledge and insight for writers about business law and criminal law, particularly cybercrime, as well as fulfilling the requirements for a bachelor's degree at Faculty of Law Universitas Pelita Harapan. Moreover, this thesis will be beneficial if the House of Representatives will make a law regarding cyber economic espionage and this thesis would also serve as a reference for students and researchers for academic purposes.

1.5 Systematics of Writing

Systematics are provided to help readers understand the material that will be discussed later in this thesis. It is hoped that the reader will be able to understand

the outline of this thesis after reading this systematic. This paper is divided into five chapters, as follows:

The **first chapter** consists of the background that outlines about the history of computer, internet and the latest development of technology. To avoid broad discussions, the author explains about the gap that occurs between cybercrimes and its jurisdiction and will be furthermore discussed in this paper. Moreover, this chapter also contains the research objectives and the systematic of writing which is intended to guide the reader in following the author's way of thinking on this topic. The **second chapter** Contains theoretical and conceptual framework which specifically discuss about cyberspace and economic espionages along with the US Law on Economic Espionage, threat of cyber espionage in Indonesia, cybercrime jurisdiction under international law, jurisdiction based on the Cybercrime Convention, and jurisdiction based on the Indonesian law.

The **third chapter** contains the method of research including the type of legal research used in this thesis is normative legal research to examine positive law to find the best legal formulation to eradicate the issue discussed, followed with the type of data, data collection method, and data analysis.

The **fourth chapter** Contains the core of all issues that are already specific, this chapter contains a discussion of jurisdictional arrangement in handling cybercrime cases in Indonesia and transnational cyber economic espionages. This chapter will examine how is Indonesia's role in ratifying the Cybercrime Convention as a non-EU member country, the US Law on Economic Espionage as a way to tackle economic espionage cases as well as the validity of the IT Law.

The **fifth chapter** contains conclusions from all the discussions that have been described in previous chapters, this conclusion is an answer to the main problems that the author proposes in the first chapter. In addition, this chapter also contains suggestions for the problems discussed.