CHAPTER I

INTRODUCTION

1.1 Background

The rapid development of technology and the internet allows for the movement of data around the world. A conspicuous feature of information technology has an impact on the evolution of telecommunications technology. The ease of accessibility and searchability of information results in the transborder flow of personal information across national borders. It also has given rise to social changes including the negative side: the emergence of new types of crime using new technology.[1] Technology can be used in the commission or facilitation of crime; often refer as 'cybercrimes.[2] Cybercrime is quick to occur and difficult to prosecute due to the complete anonymity and often far beyond the reach of a nation's laws. Criminals have increasingly located in places other than their acts produce their effects. Nonetheless, domestic laws are generally confined to a specific territory and the solutions to the problems posed must be addressed by international law.[3]

[1] S. Juneidi, *Council of Europe Convention on Cybercrime*, Fifth European Intensive Programme on Information and Communication Technologies Security (IPICS 2002), University of the Aegean (2002), p.2

[2] Several terms are used synonymously and often interchangeably including 'computer crime', 'high-tech crime', 'digital crime', 'electronic crime', and 'technology-enabled' crime.

[3] Juneidi, 2002, *op. cit.*, p.2

Predominantly, there is no single state, or international body formally address a regulation to govern the internet including cybercrime.[4] The transnational progression of the data flow along with the crime rise in cyberspace brings to the fore importance of creating a regulatory framework over cybercrime. Although there have been various efforts, the fast and unpredictable movement of data transfers imposes difficulty to determine which laws will apply as it is subject to state jurisdiction.[5]

There are other important issues such as criminalization as it conducts is not criminalized in a specific country, persons in that country may act with impunity in committing offenses that may affect other jurisdictions. Aside from there are no ability to prosecute in the home jurisdiction, efforts at evidence gathering and extradition pose challenges in the absence of dual criminality.[6] It also needs to be noted that different countries have different perceptions related to the content of the criminal law which often depends on socio-cultural facts.[7] As there are different standards, gaps, and exemptions in criminal law frameworks both substantive and procedural among countries, there is a need for international cooperation for cybercrime legislation. The enactment of cybercrime law provides rules of conduct and standards of behavior for the use of the internet, computers, and related digital

[4] Council of Europe Commissioner for Human Rights, The Rule of Law on the Internet and in the Wider Digital World' (2014), p. 36.

[5] M. Corley, *The Need for an International Convention on Data Privacy: Taking a Cue from the CISG*, 41 Brook J. Int'l L. (2016), https://brooklynworks.brooklaw.edu/cgi/viewcontent.cgi?article=1425&context=bjil, accessed on 24 April 2020, p. 722

[6] J. Clough, *A World of Difference: the Budapest Convention on Cybercrime and the Challenges of Harmonization*, Monash University, Monash University Law Review (2014), p. 702

[7] For example, spam, in many developing countries would like to see criminalized but in most developed countries, it sees as a civil or administrative matter.

technologies, and the actions of the public, government, and private organizations; rules of evidence and criminal procedure, and other criminal justice matters in cyberspace; and regulation to reduce risk and/or mitigate the harm done to individuals, organizations, and infrastructure should a cybercrime occur.[8]

In 2001, the Council of Europe (further referred to as "**CoE**") established the Budapest Convention on Cybercrime[9] (further addressed as "**the Budapest Convention**") being as the first multilateral binding instrument to regulate cybercrime. The content of the Budapest Convention layout (i) the criminalization of conduct ranging from illegal access, data, and systems interference to computer-related fraud and child pornography; (ii) procedural law tools to investigate cybercrime and secure electronic evidence concerning any crime; and (iii) efficient international cooperation.[10]

Noting that the issue of international cybercrime poses a challenge in the investigation, prosecution, and adjudication, it is crucial to recourse these issues through international agreement. One of the purposes of the Budapest Convention is enhancing international cooperation[11] making this Convention more than a legal document but a framework which permits hundreds of practitioners from Parties to share experience and make relationships to facilitate cooperation in specific cases.

---

[8] United Nations Office of Drugs and Crime, *Cybercrime Module*, https://www.unodc.org/e4j/en/cybercrime/module-7/key-issues/national-capacity-and-international-cooperation.html, accessed on 20 November 2020, p. .52

[9] Convention Cybercrime, opened for signature 23 November 2001, ETS No 185 (entered into force 1 July 2004)

[10] Cybercrime Convention Committee (T-CY), *The Budapest Convention on Cybercrime: benefits and impact in practice*, T-CY (2020), p. 4

[11] Chapter III of the Budapest Convention on Cybercrime ("**the Budapest Convention**")

Moreover, the Budapest Convention was backed up by "capacity building projects" to assist countries in creating necessary capacities for the investigation, prosecution, and adjudication of cybercrime and other cases involving electronic evidence.[12] According to the recent survey on the global state of cybercrime legislation regarding the impact of the Budapest Convention, there are some 153 members of the UN who had used the convention as a guideline or a source for their legislation.[13]

Indonesia, being a country with the fourth-largest growth in internet users in the world, also facing the impact of technology development including threats. Indonesia cyberlaw is regulated under Undang-Undang No. 11/2008 tentang Informasi dan Transaksi Elektronik or Law No. 11/2008 regarding Information and Electronic Transaction (further addressed as "**UU ITE**")[14] and Undang-Undang No. 19/2016 tentang Amandemen Undang-Undang No.11/2008 tentang Informasi dan Transaksi Elektronik or Law No. 19/2016 regarding Amendment to Law No. 11/2008 regarding Information and Electronic Transaction (further addressed as "**UU 19/2016**") According to Hasyim Gautama, there are several obstacles that Indonesia government has to deal with concerning cybersecurity development such as[15]

[12] Cybercrime Convention Committee (T-CY), *The Budapest Convention on Cybercrime: benefits and impact in practice*, T-CY (2020), p. 4
[13] Cybercrime Program Office of the Council of Europe, *the Global State of Cybercrime Legislation*, Bucharest (2020), https://www.coe.int/en/web/cybercrime/-/global-state-of-cybercrime-legislation-update-, accessed on 22 November 2020
[14] Law No.11/2008 regarding Information Electronic Transaction ("**UU ITE**")
[15] M. Rizal, Y. M. Yani, *Cybersecurity Policy and Its Implementation in* Indonesia, Universitas Padjajaran Indonesia (2013), p. 70

1. State administrators that have a weak understanding of cybersecurity issues,

2. Some internet services that have servers located abroad,

3. Lack of a secure system in Indonesia cyber facilities,

4. The absence of a law that specifically addresses and regulate attacks in the cyber world,

5. The frequent happenings of cybercrime that render it hard to handle,

6.Weak awareness of international threats of cyber-attacks that can paralyze a state's vital infrastructures.

As cybercrime has a transborder characteristic, Indonesia government needs a policy that regulates all elements related to cybersecurity. Such regulation has to meet the international standard to face an international cyber-attack. UU ITE gives mandates for the Indonesian Ministry of Defense and the Ministry of Information and Communication to protect the sovereignty and territorial integrity of Indonesia for a safe cyberspace. Both ministries implement the UU ITE through five cybersecurity policy agendas: (1) capacity building, (2) policy and legal framework, (3) organizational structure, (4) technical and operational measures, and (5) international cooperation.[16]

Indonesia's position in the Budapest Convention is not a member country that has participated in compiling the Budapest Convention. Thus far, Indonesia has not participated in ratifying the Budapest Convention, but the substantive

[16] M. Rizal, Y. M. Yani, 2013, *op. cit.*, p.71

provisions in the Budapest Convention were adopted and harmonized in UU ITE and UU 19/2016.[17] In handling international cybercrime, there are hindrances faced by Indonesia. First, state boundaries and jurisdiction. Although UU ITE has been formed in Indonesia, in practice, the cyber world remains difficult to tame because cyberspace is a virtual world that is difficult to find in real terms but can be visited by millions of users around the world at any time. These characteristics that influence the UU ITE influence its application because cybercrime is often cross-border in nature. This raises questions about the jurisdiction that applies to acts or consequences of criminal acts and the perpetrators. It is realized by Indonesia that the limitations of its conventional laws are difficult to answer this problem.[18] Regarding the organizational structure, previously, the implementation of cyber defense in Indonesia government has not been a coordinated national initiative. The implementation steps are sectoral, and it highly relies on each of the sectors' interests and capability. The capability, deterrence, and countermeasures of cyber defense are weak and vulnerable to massive attacks. As domestic anticipation still not sufficient for a sophisticated cyber defense implementation, the role of international cooperation as mentioned within the policy agendas is indispensable. The implementation of international cooperation is done by joining international associations and conducting the Mutual Legal Assistance Agreement (further addressed as "**MLA**") through bilateral, regional, or multilateral agreements. Indonesia currently has conducted MLA with the Association of South East Asian

[17] D. Bunga, *Legal Response to Cybercrime in Global and National Dimensions*, Padjajaran Journal of Law Volume 6 Number 1 [ISSN 2460-1543] [e-ISSN 2442-9325] (2019), p. 84
[18] R. Setiawan, *Efektivitas Undang-Undang Informasi dan Transaksi Elektronik di Indonesia Dalam Aspek Hukum Pidana*, Recidive Vol 2 No. 2 (2013), p. 141

Nations (further addressed as "**ASEAN**"), Australia, United States, China, and Korea. MLA allowing investigators such as the police to request for evidence located outside Indonesia and prosecution of the perpetrator, not within Indonesia jurisdiction. This still imposes challenges for Indonesia government to deal with case of cybercrime occurred not within those countries. Furthermore, for effective implementation of MLA, domestic law must meet adequacy with international practice.

As the role of international cooperation is indispensable to support successful implementation to mitigate cybercrime, this thesis attempts to address how the Budapest Convention in enhancing Indonesia government enforcement and can serve as a guideline for cybercrime legislation. Additionally, it aims to analyze the mechanism of the Budapest Convention, especially concerning facilitate cooperation in international cybercrime cases. Such findings would then serve as a recommendation for other nations including Indonesia to further improve UU ITE to regulate international cybercrime. As such, this thesis reflects how the Budapest Convention may inspire and influence Indonesia government in reforming and improving their cyber law.

1.2 Formulation of Issue

1. What is Indonesia's enforcement mechanism in tackling international cybercrime?
2. How Indonesia can improve its cybercrime enforcement by considering the Budapest Convention?

1.3 Research Purpose

Responding to the comprehensive questions proposed above, this thesis namely attempts:

1. To analyze the enforcement mechanism in Indonesia in dealing with cybercrime including provisions in UU ITE and relevant institutions.
2. To analyze how Indonesia as a non-member of the Budapest Convention can improve its enforcement by considering the Budapest Convention in tackling international cybercrime.

1.4 Research Benefit

The benefits of this research are, as a whole, to make certain of and improve international privacy and data protection regime in the 1) Theoretical and 2) Practical sense:

1. **Theoretical Benefits**

   This thesis aims to analyze the mechanism of the Budapest Convention in regulating cybercrime. Moreover, it looks into how the Budapest Convention can assist countries including Indonesia to regulate and improve cyberlaw for efficient international cooperation in handing international cybercrime cases. Thus, this thesis seeks to process existing literature to find the possible implementation that current Indonesia cyber-crime law may improve.

2. **Practical Benefits**

In practice, this thesis seeks to prepare Indonesia government to efficiently and effectively tackle future issues arising from transnational cyber-crime. By addressing how the Budapest Convention can assist nations in creating and implementing cybercrime law, this paper aims to provide a possible framework and method for Indonesia government in reforming their cyber law.

This thesis hopes can improve better protection and adjudication towards transnational cyber-crime in Indonesia.

1.5 Framework of Writing

CHAPTER I INTRODUCTION

The first chapter introduces the starting point of this thesis. It informs readers of the issue regarding technology and information-development which results in a crime. This chapter briefly discusses the establishment of the first international agreement regulated cyber-crime, the Budapest Convention. Different jurisdictions, the content of criminal law, and the lack of national legislation pose challenges in prosecuting and adjudicating cyber-crime. Moreover, this chapter discusses the current state of Indonesian cyberlaw and enforcement which need to be improved to regulate transnational cybercrime. The chapter brings up the issues that this research seeks

to comprehend and resolve. This chapter also addresses the benefits of this research along with laying the framework writing of the paper.

CHAPTER II LITERATURE REVIEW

This chapter contains theories that become the basis or reference in compiling this research, and as a reference for the author in compiling this research. This chapter discusses the theoretical background of the writing's paradigm, addressing relevant concepts, terminologies, and legal provisions which will be relevant in the following chapters. This involves bringing forts existing literature on the theory of sources of international law, and the role of the CoE and Indonesian Cyber Law. Additionally, this chapter also introduces international criminal law, cyber-crime law along with its theoretical understanding. Lastly, this chapter discusses the work of the Budapest Convention toward international cooperation for further analysis.

CHAPTER III RESEARCH METHODOLOGY

This chapter contains what method will be used by the author as a reference for compiling this research. This chapter discusses the nature of the research paper in its methods of research and the types of research this paper entails with a descriptive understanding of the

mechanism of obtaining information. Furthermore, the chapter explains the types of information gathered, introduces the techniques and approaches this thesis will use, and equip in tackling the issues addressed.

CHAPTER IV ANALYSIS

In this chapter, the author will discuss the issues raised in this research and the solutions to the issues about the theoretical foundation and the normative analysis to solve the issues. This chapter will be divided into two sub-chapters and each sub-chapter will answer each research question as set out in chapter two of this paper. The first sub-chapter will discuss the Indonesia enforcement mechanism by analyzing the effectiveness of UU ITE in regulating cybercrime, the enforcement of Indonesian institutions, the precedent of Indonesia's enforcement, and room on how Indonesia can improve its enforcement in handling international cybercrime. The second sub-chapter will provide an analysis of the Budapest Convention as a first binding international agreement in cybercrime which serves as the basis of the State adopting domestic cyberlaw. Furthermore, it will provide a comparison between the State party to the Budapest Convention and Indonesia concerning tackling international cybercrime. Lastly, it will cover legal principles within

the Budapest Convention which can be adopted by Indonesia to improve its enforcement.

CHAPTER V CONCLUSION & RECOMMENDATION

In this chapter, this author will summarize and provide a conclusion for the problems explained in chapter four. Aside from providing a conclusion, the author will also provide recommendations on those particular issues to improve Indonesia's enforcement mechanism by considering the Budapest Convention.