Legal Response to Cybercrime in Global and National Dimensions

Dewi Bunga*

DOI: https://doi.org/10.22304/pjih.v6n1.a4

Submitted: Jan 25, 2019 | Accepted: April 23, 2019

Abstract

Cybercrime is a serious crime in the era of globalization. This crime employs sophisticated technology and anonymity. It is fast, crosses states' borders, and has a wide impact. Cybercrime causes both material and immaterial losses. It even threatens world peace and security. The legal issue in this research is to discuss the international response to cybercrime, the substance of the Convention on Cybercrime, Budapest, 23.XI.2001, and Indonesia's position in the Convention on Cybercrime. The international response to cybercrime is done by holding international meetings at the United Nations Congress to discuss efforts to prevent cybercrime. Convention on Cybercrime, is the first provision for regulating cybercrime. The substance of the Convention on Cybercrime consists of material criminal law, procedural law, corporate responsibility, international cooperation and so on. Indonesia's position in the Indonesia Convention on Cybercrime is not to ratify the Convention on Cybercrime, but adopts the provisions of the Convention on Cybercrime on the Law Number 11 of 2008 on Information and Electronic Transactions and the Law Number 19 of 2016 on the Amendment of the Law Number 11 of 2008 on Information and Electronic Transactions. The criminal acts provided for in the Information and Electronic Transaction Law in Indonesia are wider than those stipulated in the Convention on Cybercrime.

Keywords: Convention on Cybercrime, cybercrime, legal response.

Respon Hukum terhadap Kejahatan di Dunia Maya dalam Dimensi Global dan Nasional

Abstrak

Kejahatan siber adalah kejahatan serius di era global. Kejahatan ini dilakukan dengan menggunakan teknologi canggih, anonimitas, cepat, lintas batas negara, dan memiliki dampak yang luas. Dampak kejahatan siber tidak hanya menyebabkan kerugian material, tetapi juga kerugian immaterial, bahkan mengancam perdamaian dan keamanan dunia. Isu hukum dalam penelitian ini adalah membahas mengenai respon internasional terhadap kejahatan di dunia maya, substansi Convention on Cybercrime, *Budapest, 23.XI.2001, dan*

* PhD Candidate of Faculty of Law, Universitas Gadjah Mada, Jl. Bulaksumur, Caturtunggal, Kec. Depok, Sleman, Daerah Istimewa Yogyakarta; lecturer of Criminal Law in the Department of Law, IHDN Denpasar, Jl. Ratna No. 51, Denpasar, Bali, S.H., M.H. (Universitas Gadjah Mada), bunga8287@gmail.com.

posisi Indonesia dalam Convention on Cybercrime*. Respon internasional terhadap kejahatan di dunia maya dilakukan dengan mengadakan pertemuan internasional yang ada di Kongres PBB yang membahas mengenai upaya pencegahan kejahatan siber.* Convention on Cybercrime*, adalah ketentuan pertama untuk mengatur kejahatan siber. Substansi dari* Convention on Cybercrime *terdiri dari hukum pidana materiil, hukum acara, tanggung jawab korporasi, kerjasama internasional dan sebagainya. Posisi Indonesia dalam Indonesia* Convention on Cybercrime *adalah tidak meratifikasi* Convention on Cybercrime, *tetapi mengadopsi ketentuan* Convention on Cybercrime *pada Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik dan Undang-Undang Nomor 19 Tahun 2016 tentang Perubahan atas Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Elektronik Transaksi. Tindak pidana yang diatur dalam Undang-Undang tentang Informasi dan Elektronik Transaksi di Indonesia lebih luas daripada yang diatur dalam* Convention on Cybercrime*.*

Kata kunci: *kejahatan siber, Konvensi tentang Kejahatan Siber, respon hukum.*

A. Introduction

Cybercrime is a crime phenomenon in the era of digitalization that threatens global security and economy. This crime is a negative effect of the development of information technology, especially the development of internet networks that connect people from various parts of the world. Adami Chazawi and Ardi Ferdian reveal that some people or groups use technological advancements to commit acts against law by attacking individuals, society, and state.[1] Since 1971, Stanford Research International in the United States has researched this type of crime. The research says that there have been 1,600 cases of cybercrime since 1958.[2] The data certainly increases due to the rapid growth of the internet network.

United Nations Office on Drugs and Crime (UNODC)[3] says that cybercrime has been used to describe various crimes. The intended crimes are computer-related forgery and fraud (such as phishing), offences against computer data and systems (such as hacking), content offenses (such as child pornography), and copyright offences (such as the dissemination of pirated content)."

Cybercrime is a serious crime that requires fast handling. According to Widodo, cybercrime is a whole form of crime aimed at computers, computer networks and users, and other forms of traditional crime using computer equipment.[4] Some cases that occur and include cybercrime are illegal access, system destruction,

---

1 Adami Chazawi and Ardi Ferdian, *Tindak Pidana Informasi dan Transaksi Elektronik; Penyerangan terhadap Kepentingan Hukum Pemanfaatan Teknologi Informasi dan Transaksi* Elektronik, Malang: Bayumedia, 2011, p. 2.

2 Widodo, *Aspek Hukum Pidana Kejahatan Mayantara,* Yogyakarta: Aswaja Pressindo, 2013, p. 40.

3 United Nations Office on Drugs and Crime, *The Globalization of Crime A Transnational Organized Crime Threat Assessment,* Vienna: United Nations Office on Drugs and Crime, 2010, p. 12.

4 Widodo, *op.cit.*, p. 102.

online pornography, cyberbullying, online gambling, and so on. These crimes are very dangerous. Today, the virtual world is also used as a medium to commit major crimes such as terrorism and money laundering. This condition certainly endangers international peace and security.

The frequency of cybercrime's occurrence is very fast. Sam Cook, based on a research conducted by the University of Maryland, notes that it is known for hackers to attack computers and networks with an average of 1 constant attack every 39 seconds.[5] Steve Morgan tries to summarize the cybersecurity industry for the past five years and predicts the next five years as follows.

1. The cost of damage caused by cybercrime reaches $6 trillion per year in 2021.
2. Expenditures for virtual security exceed $1 trillion from 2017 to 2021.
3. Cybercrime will more than triple the number of virtual unoccupied security jobs, which is estimated to reach 3.5 million by 2021.
4. The layer of attack on people reaches 6 billion people in 2022.
5. The cost of damage to global ransomware is expected to exceed $5 billion in 2017.[6]

In addition to causing financial losses to damaged network systems, the occurrence of cybercrimes also requires considerable costs to build electronic system security to prevent further attacks. Regarding this, Kai-Lung Hui, Seung Hyun Kim, and Qiu-Hong Wang[7] state the occurrence of cybercrime will cause the government and business organizations to issue resources to build a security system, even though these resources can be used for other things if there is no cybercrime.

Cybercrime is a very serious threat faced by many countries. The loss of this case is not only related to financial losses but also related to moral and behavioral degradation. Therefore, the prevention of cybercrime is very extensive. The European Community on Crime Problems, for example, has a team of experts in the field of cybercrime called the Committee of Experts on Cybercrime in Cyberspace, which has succeeded finishing a draft of convention on cybercrime. In addition, various international meetings involving many states has discussed cybercrime in the framework of crime prevention, as well as specifically discussing cybercrime.

---

5 Sam Cook, "Cybercrime Stats & Facts for 2016–2017", https://www.comparitech.com/vpn/cybercrime-statistics-2016-2017/, accessed on January 2018.

6 Steve Morgan, "Top 5 Cybersecurity Facts, Figures and Statistics for 2017", https://www.csoonline.com/article/3153707/security/top-5-cybersecurity-facts-figures-and-statistics-for-2017.html, accessed on January 2018.

7 Kai-Lung Hui, Seung Hyun Kim, Qiu-Hong Wang, "Cybercrime Deterrence and International Legislation: Evidence from Distributed Denial of Service Attacks", *MIS Quarterly,* Vol. 41 No. 2, 2017, pp. 497-523, p. 518.

At the global level, the Convention on Cybercrime, Budapest, 23.XI.2001 (Cybercrime Convention), is an important milestone in the fight against cybercrime. The Cybercrime Convention is the first international agreement governing crimes committed via the internet and internet networks. It covers copyright infringement in cyberspace, fraud, child pornography, and authority over data traffic, as well as interception and attacks on network security. This international agreement is an open international agreement for both member states of the Council of Europe and non-member states.

The Council of Europe says that the main purpose of this international agreement is to develop criminal policies by adopting appropriate legislation and creating international cooperation to protect people from cybercrime. The Cybercrime Convention is a reference for states of the world to deal with cybercrime.

Every country has different arrangements regarding actions of cybercrime. This study discusses the international response to cybercrime. This section explores the global commitment in responding to the phenomenon of cybercrime, international congresses that have been carried out by states, and the history of the birth of the Cybercrime Convention. This study also discusses Indonesia's position in the Cybercrime Convention. The study also covers the policy of the Government of the Republic of Indonesia on the Cybercrime Convention. Furthermore, this study also compares the substance of the Cybercrime Convention, and the Law Number 11 of 2008 on Information and Electronic Transactions (ITE Law 2008) and the Law Number 19 of 2016 on Amendment to the Law Number 11 of 2008 on Information and Electronic Transactions (ITE Law 2016).

B. International Response to Cybercrime

The internet provides virtual spaces or cyberspace for netizens to do activities in cyberspace. Adrian Cristian Moise states, "Cyberspace represents a global domain in the informational environment and encompasses the identities and objectives which exist in computers networks used by human persons in different purposes."[8] In this virtual space, internet users can commit crimes to attack other network systems and turn traditional crimes into high-tech crimes that can eliminate direct contact between perpetrators and victims.

Crime in cyberspace has the character of anonymity at a very high speed. It causes this crime to have a tremendous impact. Soumyo D. Moitra [9] describes the layered impact of cybercrime as follows.

---

[8] Adrian Cristian Moise, "Some Considerations on the Phenomenon of Cybercrime", *Journal of Advanced Research in Law and Economics*, Vol. 5, Issue 1, 2014, pp. 38-39.

[9] Soumyo D. Moitra, "Developing Policies for Cybercrime Some Empirical Issues", *European Journal of Crime, Criminal Law and Criminal Justice*, Vol. 13, Issue 3, 2005, p. 441.

> *The impacts of cybercrimes can be multifarious. In the first place, the victim can be a user (person or organization) or a computer system. In the second place, each of these can be affected in very different ways, from no detectible damage to major financial losses and there can even be subtle, intangible effects on individuals (such as instilling fear of cyberspace).*

The concerns about widespread cybercrime have been responded by a global strategy. It is created by countries to build international commitments to be wary of cybercrime, encourage the formulation of legal rules to combat cybercrime, build international cooperation to combat cybercrime, and carry out non-reason strategies to deal with cybercrime. In the implementation, the United Nations has made several agreements that cover crimes in cyberspace.

The Tenth Vienna United Nations Congress on the Prevention of Crime and Treatment of Offenders, 10-17 April 2000 at Point 18 states the following.

> *We decide to develop action-oriented policy recommendations on the prevention and control of computer-related crime, and we invite the Commission on Crime Prevention and Criminal Justice to undertake work in this regard, taking into account the ongoing work in other forums. We also commit ourselves to working towards enhancing our ability to prevent, investigate and prosecute high-technology and computer-related crime.*

In The Eleventh Congress taken place in Bangkok, Thailand, the meeting focused on effective measures to combat transnational organized crime, international cooperation against terrorism, and the relation between terrorism and other criminal activities. The meeting is called Bangkok Declaration of Synergies and Responses: Strategic Alliances in Crime Prevention and Criminal Justice. It also covers cybercrime on the following points.

1. We reaffirm the fundamental importance of implementation of existing instruments and the further development of national measures and international cooperation in criminal matters, such as consideration of strengthening and augmenting measures, in particular against cybercrime, money-laundering and trafficking in cultural property, as well as on extradition, mutual legal assistance and the confiscation, recovery and return of proceeds of crime.
2. We note that, in the current period of globalization, information technology and the rapid development of new telecommunication and computer network systems have been accompanied by the abuse of those technologies for criminal purposes. We, therefore, welcome efforts to enhance and supplement existing cooperation to prevent, investigate, and prosecute high

technology and computer-related crime; including by developing partnerships with the private sector. We recognize the important contribution of the United Nations to regional and other international forums in the fight against cybercrime. We also invite the Commission on Crime Prevention and Criminal Justice, taking into account that experience, to examine the feasibility of providing further assistance in that area under the aegis of the United Nations in partnership with other similarly focused organizations.

On April 12-19, 2010, the United Nations organized the Twelfth United Nations Congress on Crime Prevention and Criminal Justice. The Congress Agenda focused on children, adolescents, and crime; migrant smuggling; human trafficking; money laundering; and cybercrime. Regarding the prevention of cybercrime, the meeting has produced the Salvador Declaration on Comprehensive Strategies for Global Challenges: Crime Prevention and Criminal Justice Systems and Their Development in a Changing World as follows.

1. We recommend that the UNODC, upon request, provide, in cooperation with Member States, relevant international organizations and the private sector, technical assistance and training to States to improve national legislation and build the capacity of national authorities, in order to deal with cybercrime, including the prevention, detection, investigation and prosecution of such crime in all its forms, and to enhance the security of computer networks.
2. We invite the Commission on Crime Prevention and Criminal Justice to consider convening an open-ended intergovernmental expert group to conduct a comprehensive study of the problem of cybercrime and responses to it by Member States, the international community and the private sector, including the exchange of information on national legislation, best practices, technical assistance and international cooperation, with a view to examining options to strengthen existing and to propose new national and international legal or other responses to cybercrime.

As an international meeting focused on combating cybercrime, the Twelfth United Nations Congress on Crime Prevention and Criminal Justice discusses the prevention of crime through a Working Paper. The conclusions and recommendations in the working paper are as follows:[10]

1. Investigating cybercrime and prosecuting cybercriminals is challenging for all institutions involved. Taking into account the complexity of the issue and the constant technical development, sustained and ever-expanding training for all authorities involved remains a key issue. The discussion held at the 2009

[10] *See also* United Nations Congress on Crime Prevention and Criminal Justice, "Recent developments in the use of science and technology by offenders and by competent authorities in fighting crime, including the case of cybercrime", *Working Paper,* presented in Twelfth United Nations Congress on Crime Prevention and Criminal Justice, Salvador, Brazil, 12-19 April 2010.

meeting of the UNODC expert group on cybercrime showed that institutionalized capacity building and long-term sustainability are two key factors for measuring the success of future initiatives.

2. In order to eliminate safe havens and improve international cooperation, attention should be paid to closing gaps in existing legislation and to promoting consistency, coherence, and compatibility of laws. Taking into account the importance of harmonizing legislation and of building on the outcomes of the preparatory meetings for the Twelfth United Nations Congress on Crime Prevention and Criminal Justice, the development of a global convention against cybercrime should be given careful and favorable consideration.
3. In the meantime, UNODC, as a standard-setter in crime prevention and criminal justice matters, will offer a multilateral platform with a focus on developing countries. It will continue to adopt a comprehensive, partnership-based and multidisciplinary approach by pooling its already proven legal, law enforcement and technical expertise to counter criminal activities, together with the specific and well-developed expertise of those key partners already involved in countering cybercrime. UNODC will aim to partner with and bring together the tools and experts, including from the private sector (in particular Internet service providers), to tackle the problem in a given country or region. Priority will be accorded to the provision of technical assistance to Member States in need, with a view to addressing the lack of capacity and expertise, and to ensuring long-term sustainability in dealing with computer-related crime.
4. Specifically, UNODC will aim to do the following: assist Member States in adopting legislation for effectively investigating computer-related crimes and prosecuting offenders; build the operational and technical knowledge of judges, prosecutors and law enforcement officers on issues pertaining to cybercrime, through training, the adaptation/development of training materials on investigation and prosecution of computer-related crime etc.; train law enforcement authorities to effectively use international cooperation mechanisms to combat cybercrime; raise the awareness of civil society and create momentum among decision makers to coalesce efforts to prevent and address cybercrime; and identify and disseminate good practices and promote public-private partnerships in preventing and combating cybercrime.

Thirteenth United Nations Congress on Crime Prevention and Criminal Justice held in Doha, Qatar, on 12-19 April 2015 again discussed the prevention of cybercrime. The discussion was conducted in Workshop 3 on Strengthening crime prevention and criminal justice responses to evolving forms of crime, such as

cybercrime and trafficking in cultural property, including lessons learned and international cooperation.

> *National cybercrime policies, strategies, and legislation are an important starting point in setting the framework and priorities for responses to cybercrime. The UNODC online cybercrime repository (to be launched in 2015) will contain details of national strategies identified in some 50 countries, covering areas such as cybercrime awareness-raising, international cooperation, law enforcement capacity, legislation, prevention, and public-private partnerships.*

As an emerging crime, the world gives great attention to the counter on cybercrime. UNODC[11] states that the Cybercrime Program in 2017 covers Central America, East Africa, MENA (Middle East and North Africa), and Southeast Asia and the Pacific with the main objectives as follows.

a. Increased efficiency and effectiveness in conducting investigations, prosecutions, and countermeasures against cybercrime, especially those related to sexual exploitation and abuse of children carried out online, based on strong human rights protection;
b. The long-term, efficient, and effective response from the government to cybercrime includes national coordination, data collection, and the effective preparation of legal frameworks. The response is carried out on an ongoing basis and greater prevention;
c. Strengthen national and international communication between all stakeholders, namely the government, law enforcement, and the private sector through increasing public knowledge of the risks and impacts of crime in cyberspace.

At the international level, discussions on cybercrime have resulted in the Cybercrime Convention. This is the first international legislation that provides a substantive and procedural framework in the field of cybercrime. This international agreement was prepared by the Council of Europe countries and other countries outside the members (Canada, Japan, United States, and South Africa) based on considerations from the Preamble of the Convention as follows.

a. The need for uniform or same policies to protect the public from crime in cyberspace, both through the adoption of legal instruments and international cooperation.
b. The continuous digitalization, convergence, and globalization of computer networks lead to fundamental changes.

---

[11] United Nations Office on Drugs and Crime, "Global Programme on Cybercrime," https://www.unodc.org/unodc/en/cybercrime/global-programme-cybercrime.html, accessed on January 2018.

c. The concern for computer networks that can be used to commit crimes and the storage and transfer of evidence is carried out on the network.
d. The need for cooperation between the countries and the private sector to tackle crime in cyberspace and believe that resistance to crime in cyberspace is carried out with effective international cooperation.
e. The need for deterrent effects for perpetrators of crime in cyberspace through investigation and law enforcement both in the domestic and international spheres.

Paolo Balboni dan Enrico Pelino[12] state that the 2001 Council of Europe Convention on Cybercrime is seen as legal key sources because this international convention covers crimes that attack data, has extensive substance, is signed by many parties, and has legal implications for the issuance of laws from signatory countries.

C. Substance of Convention on Cybercrime, Budapest, 23.XI.2001

The Cybercrime Convention consists of four Chapters. They are Chapter I on the Use of Terms, Chapter II concerning Approaches that must be taken at the National Level, Chapter III International Cooperation, and Chapter IV Closing Provisions. The Cybercrime Convention does not define cybercrime explicitly. In Chapter I of the Cybercrime Convention only formulates the definition of computer systems, computer data, service providers, and traffic data for the purposes of the formulation of this convention.

According to the Cybercrime Convention, "computer system" means any device of interconnected or related devices, pursuant to a program, performs automatic processing of data. On the other hand, "computer data" means any representation of facts, information systems for processing in a computer system, including a system to perform a function.

The Cybercrime Convention provides two definitions of service providers. Firstly, any public or private entity that provides users with the ability to communicate with means of a computer system. Secondly, any other entity that processes or stores computer data on behalf of such communication services or users of such service. Traffic data, however, means any computer data relating to a communication by means of a computer system. It is generated by a computer system that formed a part of the chain of communication that indicates the communication's origin, destination, route, time, date, size, duration, or type of underlying service.

---

[12] Paolo Balboni and Enrico Pelino, "Law Enforcement Agencies' Activities in the Cloud Environment: a European Legal Perspective", *Information & Communications Technology Law*, Vol. 22, No. 2, 2013, p. 170.

The policy of criminalizing cybercrime, which is an international standard, can be seen in Chapter II of the Cybercrime Convention. Chapter II deals with approaches that must be taken at the national level, one of them is in the material criminal law. In this section, the actions, which include cybercrime, are divided into four categories.

1. Offences against the confidentiality, integrity, and availability of computer data and systems. These actions include
   (1) Illegal access;
   (2) Illegal interception;
   (3) Data interference;
   (4) System interference; and
   (5) Misuse of devices.
2. Computer-related offences. These actions include
   (1) Computer-related forgery; and
   (2) Computer-related fraud.
3. Content-related offences:
   Offences related to child pornography.
4. Offences related to infringements of copyright and related rights.

The approach that must be taken at the national level also includes the ancillary liability and sanctions (additional responsibilities and sanctions). They consist of arrangements regarding trials, assistance, and agreement on criminal acts, especially cybercrime. Article 11(1) states that Each Party must take legislative action and other actions that may be needed to be determined as a criminal offence under national law, if done intentionally, assisting or abetting a crime determined in accordance with Article 2 to 10. This Convention is intended for the purpose of such violations. Furthermore, Article 2 states that each Party must take legislative action and other actions that may be needed to be determined as a criminal offense based on its national law, if it is done intentionally, an attempt to commit a violation determined in accordance with Articles 3 to 5, 7, 8 and 9.1.a and c. of this Convention.

Article 12 of the Cybercrime Convention regulates the responsibility of the corporation. Legal reform that places corporations as legal subjects who can be convicted. Glanville Williams, in Muladi and Dwidja Priyatno, states that the liability of a corporation, such as strict liability, exemplifies the theory of utilitarianism in criminal law not based on the theory of justice.[13] The Convention establishes criteria for corporate responsibility as accountability for crimes committed for their benefit by individuals in a leading position both acting individually and as part of organs of legal entities, based on

[13] Muladi and Dwidja Priyatno, *Pertanggungjawaban Pidana Korporasi*, Jakarta: Kencana Prenada Media Group, 2010, p. 18.

1. a power of representation of the legal person;
2. an authority to take decisions on behalf of the legal person; and
3. an authority to exercise control within the legal person.

A legal entity can be held accountable if there is a lack of supervision from responsible individuals as mentioned above for the benefit of a legal entity by an individual acting under his authority. The Convention also determines the responsibilities of legitimate persons, which can be criminal, civil, or administrative. Such responsibility must be without reducing the criminal responsibility of the people who have committed the violation. The final provision of the material law in the Convention on Cybercrime is to ensure that states parties apply laws and guarantee the accountability of perpetrators with sanctions that are effective, proportionate, deterrent, revoke freedom, or impose other measures such as financial sanctions.

As a guideline that becomes the standard of countries in formulating the Law on Crime Prevention in cyberspace, the Convention on Cybercrime also regulates the procedural law for this crime. This Convention wants the state party to regulate procedural law for investigating criminal acts in this virtual world.

As provided otherwise in Article 21, each Party shall apply the powers and procedures referred to in paragraph 1 of this article to

(1) the criminal offences established in accordance with Articles 2 through 11 of this Convention;
    1. other criminal offences committed by means of a computer system; and
    2. the collection of evidence in electronic form of a criminal offence.

Other parts are also regulated in the procedural law according to the Cybercrime Convention. They are custody and security, acceleration of computer data maintenance, acceleration of storage and partial disclosure of data traffic, orders for submission, search and confiscation of computer data, real-time computer data collection, and tapping data content that can be regulated in domestic law by upholding the protection of human rights. The Cybercrime Convention regulates jurisdictions that can be established in cyberspace. Jurisdiction is the power or authority of state law against people, objects, or events (law)."[14]

According to Maskun, jurisdiction in cyberspace is still confusing given the growth of trade on the internet. The court itself does not understand these problems to be able to set detailed standards.[15] Jurisdiction, as stipulated in the

[14] Huala Adolf, *Aspek-aspek Negara dalam Hukum Internasional,* revised edition, Jakarta: PT Raja Grafindo Persada, 2002, p. 183.

[15] Maskun, *Kejahatan Siber; Cyber Crime Sutau Pengantar,* Jakarta: Kencana Prenada Media Group, 2013, p. 105.

Cybercrime Convention, refers to territorial principles and their expansion. In general, all countries in the world adhere to the territorial principle and the expansion of territorial jurisdiction to anticipate various crimes committed outside the territory of a country.[16] The Cybercrime Convention determines the full jurisdiction regulated in Article 22 as follows.

1. Each Party shall adopt such legislative and other measures as may be necessary to *establish jurisdiction over any offence established in accordance with Articles 2 through 11 of this Convention, when the offence is committed:*
    a. in its territory; or
    b. on board a ship flying the flag of that Party; or
    c. on board an aircraft registered under the laws of that Party; or
    d. by one of its nationals, if the offence is punishable under criminal law where it was committed or if the offence is committed outside the territorial jurisdiction of any State.
2. Each Party may reserve the right not to apply or to apply only in specific cases or conditions the jurisdiction rules laid down in paragraphs 1.b through 1.d of this article or any part thereof.
3. Each Party shall adopt such measures as may be necessary to establish jurisdiction over the offences referred to in Article 24, paragraph 1, of this Convention, in cases where an alleged offender is present in its territory and it does not extradite him or her to another Party, solely on the basis of his or her nationality, after a request for extradition.
4. This Convention does not exclude any criminal jurisdiction exercised by a Party in accordance with its domestic law.
5. When more than one party claims jurisdiction over an alleged offence established in accordance with this Convention, the parties shall, whenever it is appropriate, consult with a view to determining the most appropriate jurisdiction for prosecution.

International cooperation is needed in the disclosure of cybercrime cases. This is due to the transnational aspect of cybercrime that can be carried out across national borders without calculating how far the real distance is between the perpetrator and the victim. Muladi and Diah Sulistyani state “International cooperation as part of criminal policy is very important and even very strategic for dealing with international and transnational crime because countries with

[16] Eddy O.S. Hieriej, *Pengantar Hukum Pidana Internasional,* Jakarta: Erlangga, 2009, p. 37.

sovereignty and resource issues cannot handle it unilaterally."[17] International cooperation is carried out through relevant international legal instruments in criminal matters. Therefore, arrangements are agreed upon under uniform or reciprocal laws and national laws to the maximum extent possible for the purpose of investigating or processing criminal acts relating to computer systems and data, or for collecting evidence in the form of electronic criminal violations.

The Cybercrime Convention defines international cooperation in the form of extradition and mutual assistance. In connection with extradition to criminal acts, criminal jurisdiction is the authority (law) of a country's court against cases involving criminal law, whether it is involved in foreign or national elements.[18] Extradition is a legal institution whose age is old, because it was already known in Greek, Roman, and Ancient Egypt. The practices of taking and bringing back criminals from a country who have fled to another country, have repeatedly been carried out in the same way and procedure throughout or in a large part of this world region.[19] Extradition in the Cybercrime Convention is regulated in Article 24.

1. *a.) This article applies to extradition between Parties for the criminal offences established in accordance with Articles 2 through 11 of this Convention, provided that they are punishable under the laws of both Parties concerned by deprivation of liberty for a maximum period of at least one year, or by a more severe penalty.*

   b.) Where a different minimum penalty is to be applied under an arrangement agreed on the basis of uniform or reciprocal legislation or an extradition treaty, including the European Convention on Extradition (ETS No. 24), applicable between two or more parties, the minimum penalty provided for under such arrangement or treaty shall apply.
2. *The criminal offences described in paragraph 1 of this article shall be deemed to be included as extraditable offences in any extradition treaty existing between or among the Parties. The Parties undertake to include such offences as extraditable offences in any extradition treaty to be concluded between or among them.*
3. *If a Party that makes extradition conditional on the existence of a treaty receives a request for extradition from another Party with which it does not have an extradition treaty, it*

---

17 Muladi dan Diah Sulistyani, *Kompleksitas Perkembangan Tindak Pidana dan Kebijakan Publik,* Bandung: Alumni, 2016, p. 170.

18 Huala Adolf, *Aspek-aspek Hukum Pidana Internasional*, Jakarta: Raja Grafindo Persada, 1996, p. 145.

19 I Wayan Parthiana, *Hukum Pidana Internasional,* Bandung: Yrama Widya, 2006, pp. 136-137.

may consider this Convention as the legal basis for extradition with respect to any criminal offence referred to in paragraph 1 of this article.

4. *Parties that do not make extradition conditional on the existence of a treaty shall recognize the criminal offences referred to in paragraph 1 of this article as extraditable offences between themselves.*
5. *Extradition shall be subject to the conditions provided for by the law of the requested Party or by applicable extradition treaties, including the grounds on which the requested Party may refuse extradition.*
6. *If extradition for a criminal offence referred to in paragraph 1 of this article is refused solely on the basis of the nationality of the person sought, or because the requested Party deems that it has jurisdiction over the offence, the requested Party shall submit the case at the request of the requesting Party to its competent authorities for the purpose of prosecution and shall report the final outcome to the requesting Party in due course. Those authorities shall take their decision and conduct their investigations and proceedings in the same manner as for any other offence of a comparable nature under the law of that Party.*
7. *a.) Each Party shall, at the time of signature or when depositing its instrument of ratification, acceptance, approval or accession, communicate to the Secretary General of the Council of Europe the name and address of each authority responsible for making or receiving requests for extradition or provisional arrest in the absence of a treaty.*

   b.) The Secretary-General of the Council of Europe shall set up and keep updated a register of authorities so designated by the Parties. Each Party shall ensure that the details held on the register are correct at all times.

In the practice of crime prevention, countries have carried out extradition in illegal ways. Usually, this extradition is carried out by developed states. The illegal extradition forms are as follows.[20]

a. Abduction

Abduction is illegal because the person concerned is forcibly taken out by the country that abducted him, without the knowledge or consent of the country in which he was located. This illegal nature starts with the investigation of the

[20] *Ibid.,* pp. 151-152.

identity of the person and the place in the country. Then, the preparation plan for the abduction is conducted after the person is found in the country (without his own knowledge). On the day of the abduction, the action took him outside the territory of the country. Finally, the person concerned was brought into the abduction country to finally be tried under his national law.

b. Forcible retrieval of an offender without being known and approval from the country in which he is located.

In this case, the extraction is carried out by a state against a person who is in another state, without the consent of the state concerned. In contrast to the kidnapping carried out in secret, the withdrawal in the forced retrieval is carried out openly without the country where the person is located can do anything. Such actions are clearly contrary to the most fundamental principles of international law, namely, the principle of respect for the sovereignty and independence of fellow countries. However, there are states that actually practice it. Of course, they are big and strong states aimed at smaller and weaker states.

Mutual assistance in principle is carried out based on mutually beneficial relationships. This collaboration is carried out in the investigation, prosecution, and collection of evidence related to criminal acts in this virtual world. The convention on crime in cyberspace also regulates the requirements for reciprocal assistance without an international agreement by involving the central authority responsible for sending and answering requests. These provisions are regulated in Article 27 of the Cybercrime Convention.

The last part of the Cybercrime Convention is the closing provision. The Cybercrime Convention regulates the signing and validity period, additional clauses, limited implementation, legal consequences, statements, federal provisions, reservations, status and revocation of reservations, amendments, dispute resolution, stakeholder consultation, resignation, and notice.

Cybercrime Convention is an international regulation compiled in 2001. This condition causes not all harmful acts operating in cyberspace, regulated in Cybercrime Convention. In fact, in its development, there are acts such as cyberwar which attack a country's defense system and are actually carried out by other countries.[21] Nonetheless, the Cybercrime Convention is an important milestone that arouses the awareness of countries in the world of crime in cyberspace.

[21] *See* Daniar Supriyadi and Katherine E. Dethan, "On the lookout for cyberwar", https://www.thejakartapost.com/academia/2018/05/14/on-the-lookout-for-cyberwar.html, accessed on March 2018

D. Indonesia's position in the Convention on Cybercrime

Indonesia is a country committed to tackling crime in cyberspace. This is proven by the formulation of rules regarding various forms of cybercrime as stipulated in ITE Law 2008 and ITE Law 2016. In practice, Indonesia was involved in the G20 Meeting in Washington DC, United States of America at the end of 2017. In the speech, Sri Mulyani[22] says, to tackle potential cybercrime, Indonesia already has a digital economic roadmap. The road map includes the form of handling security issues.

The transborder characteristic of crime in cyberspace requires global mitigation. The Digital Watch Observatory says that several international frameworks have been created to combat cybercrime, most notably the European Council Convention on Cybercrime, which contains provisions on the types of violations, procedural law, and international cooperation between countries. [23] There have been 56 states that has ratified the Convention on Cybercrime.

Cybercrime Convention is an international convention that has a hard law character that gives birth to global regulation. The Convention regulates the common interests of countries in the world to fight cybercrime. UNODC, in the Comprehensive Study on Cybercrime, confirms that countries that have not ratified or acceded to binding international conventions can continue to use these legal instruments as inspiration for national legislative provisions.[24]Indonesia itself is not a non-member country that has participated in compiling the Convention on Cybercrime. Until now, Indonesia has not participated in ratifying the Cybercrime Convention, but the agreement in the Cybercrime Convention was adopted and harmonized in ITE Law 2008 and ITE Law 2016. This can be seen in the following table:

Table 1

Material criminal comparison matrix between Convention on Cybercrime and the Law on Information and Electronic Transactions

---

[22] Reiny Dwinanda, "G20 Meeting Discusses Cybercrime: Sri Mulyani", http://en.republika.co.id/berita/en/national-politics/17/10/16/oxwxi4414-g20-meeting-discusses-cybercrime-sri-mulyani, accessed on January 2018.

[23] Digital Watch Observatory, "Legal Frameworks", https://dig.watch/issues/cybercrime, accessed on January 2018.

[24] United Nations Office on Drugs and Crime, *Comprehensive Study on Cybercrime Draft February 2013*, New York: United Nations, 2013, p. 65.

No	Material Crime according to the Convention on Cybercrime	Material Crime according to ITE Law 2008 and ITE Law 2016.
1.	Offences against the confidentiality, integrity, and availability of computer data and systems	
	a. Illegal access	Article 30(1)(2) of ITE Law 2008.
	b. Illegal interception	Article 41 of ITE Law 2016.
	c. Data interference	Article 32(1), 32(2), 32(3) of ITE Law 2016.
	d. System interference	Article 30(3) of ITE Law 2008.
	e. Misuse of devices	Article 34 of ITE Law 2008.
2.	Computer-related offences	
	a. Computer-related forgery	Article 35 of ITE Law 2008.
	b. Computer-related fraud	Article 35 of ITE Law 2008.
3.	Content-related offences	
	Offences related to child pornography	Article 27(1) to Article 52(1) of ITE Law 2008.
4.	Offences related to infringements of copyright and related right	Article 25 of ITE Law 2008.

In connection with table 1, it can be seen that all criminal acts regulated in the Cybercrime Convention have been formulated in the ITE Law 2008 and the ITE Law 2016, although there are slight differences. The Cybercrime Convention stipulates that actions including violations related to content in cyberspace are child pornography. While in the ITE Law 2008, criminal acts refer to decency offences as stipulated in Article 27(1) of the ITE Law 2008 stating "Everyone intentionally and without rights distributes and/or transmits and/or makes accessible Electronic Information and/or Electronic Documents that have contents that violate morality."

The Cybercrime Convention itself regulates criminal acts that are narrower than that are stipulated in ITE Law 2008, where pornography is one of the actions in the decency offence group. Convention on Cybercrime also does not concern pornography carried out by adults. This is fairness considering that many countries legalize the pornography industry in their national law, but criminalize child pornography and even consider that children's involvement in pornography is a very serious problem. Criminalization of child pornography in ITE Law 2008 refers to Article 27(1) *jo.* Article 52(1) which states "In the case of criminal offences as referred to in Article 27(1) on sexual decency or exploitation of children subjects to one third of the principal penalty."

ITE Law 2008 and ITE Law 2016 regulate criminal offenses not regulated in the Convention on Cybercrime, namely:

1. Online gambling (Article 27(2) of ITE Law 2008).
2. Insult and/or defamation carried out in cyberspace (Article 27(3) of ITE Law 2008).
3. Extortion and/or threats made in cyberspace (Article 27(4) of ITE Law 2008).
4. Distribution of false and misleading news (Article 28(1) of the ITE Law 2008).
5. Speech of hatred based on ethnicity, religion, race, and intergroup (Article 28(2) of ITE Law 2008).
6. Threats of violence or scare intended personally (Article 29 of ITE Law 2008).

Provisions regarding gambling, humiliation and/or defamation and the spread of hoaxes are not criminal acts in many countries. The criminalization of gambling is indeed varied. Some legalize gambling, legalize gambling with strict rules, and some even expressly prohibit gambling. Liberal countries that legalize gambling regulate internet gambling because the value will harm the country. Gambling arrangements in secular countries are carried out with the consideration that on the one hand it is seen as a business that brings profit, but on the other hand, creates a negative impact on society.[25] Countries that legalize gambling do not necessarily legalize online gambling because online gambling is feared not to provide income to the state and instead tend to be used as a means to fund terrorist activities and illegal arms trade.

Greece, Italy, Spain, the United States, Malaysia, Singapore, Hong Kong, and many others are countries that legalize gambling. Indonesia itself is a country that prohibits gambling both conventionally as stipulated in Article 303 of the Indonesian Criminal Code, as well as those carried out online as stipulated in Article 27(2) of ITE Law 2008. Online gambling is indeed quite dangerous considering the number of frauds that can befall the players from access to their credit cards. Online gambling also makes it easier for children to access gambling, because it cannot always detect the age of its players, unlike gambling in casino areas that can strictly prohibit children from entering the gambling arena.

Criminalization of insults and/or defamation and the spread of hoaxes are not also regulated in the Cybercrime Convention. They are indeed gray areas that limit freedom of expression and individual protection. Countries are very careful in criminalizing insults and/or defamation and the spread of hoaxes. This is because the state must make a strict boundary to protect the right to argue in accordance with democratic values. On the other hand, it also must protect the interests of individuals and society. There are countries that do not criminalize the spread of hoaxes and view it as unimportant matters. This is because the government

[25] Sigid Suseno, *Yurisdiksi tindak Pidana Siber,* Bandung: Refika Aditama, 2012, p. 168.

believes that its citizens are intelligent citizens who can distinguish between true news and untrue news.

Speeches of hatred based on ethnicity, religion, race, and intergroup and the threat of violence or scare intended personally are not regulated in the Cybercrime Convention. However, they are regulated in the Additional Protocol to Cybercrime concerning the criminalization of acts of a racist and xenophobic nature committed through Strasbourg computer systems, 28.I.2003 (Treaty No. 189). Article 2(1) of Treaty No.189 states

> *For the purposes of this Protocol: "racist and xenophobic material" means any written material, any image or any other representation of ideas or theories, which advocates, promotes or incites hatred, discrimination or violence, against any individual or group of individuals, based on race, color, descent or national or ethnic origin, as well as religion if used as a pretext for any of these factors.*

The existence of this Additional Protocol to the Cybercrime Convention is a response to the disappointment of the parties in connection with the absence of arrangements to eradicate the spread of racism or similar propaganda via the internet in the Cybercrime Convention.[26] As a country that interacts with the outside world, it is a moral obligation for Indonesia to harmonize laws with provisions in international legal instruments in tackling cybercrime.

E. Conclusion

The international response to cybercrime can be seen in the discussion on high-tech crime in several UN congresses, such as the United Nations Congress on the Prevention of Crime and Treatment of Offenders, Bangkok Declaration of Synergies and Responses: Strategic Alliances in Crime Prevention and Criminal Justice, Twelfth United Nations Congress on Crime Prevention and Criminal Justice, and Thirteenth United Nations Congress on Crime Prevention and Criminal. In particular, the first legislation regarding cybercrime is the Convention on Cybercrime, Budapest, 23.XI.2001. The Cybercrime Convention consists of 4 Chapters namely Chapter I on the Use of Terms, Chapter II on Approaches that Must be Taken at the National Level, Chapter III International Cooperation, and Chapter IV Closing Provisions. Indonesia does not ratify the Cybercrime Convention but adopts provisions in the Cybercrime Convention in ITE Law 2008 and ITE Law 2016.

---

[26] *See* Hukum Online, "Perjanjian Internasional untuk Tanggulangi Cybercrime Disiapkan", http://www.hukumonline.com/berita/baca/hol2579/perjanjian-internasional-untuk-tanggulangi-icybercrimei-disiapkan, accessed on January 2018.

References

Books

Adami Chazawi dan Ardi Ferdian, *Tindak Pidana Informasi dan Transaksi Elektronik; Penyerangan terhadap Kepentingan Hukum Pemanfaatan Teknologi Informasi dan Transaksi Elektronik, Bayumedia*, Malang, 2011.

Eddy O.S. Hieriej, *Pengantar Hukum Pidana Internasional*, Erlangga, Jakarta, 2009.

Huala Adolf, *Aspek-aspek Hukum Pidana Internasional*, RajaGrafindo Persada, Jakarta, 1996.

Huala Adolf, *Aspek-aspek Negara dalam Hukum Internasional,* revised edition, PT Raja Grafindo Persada, Jakarta, 2002.

Maskun, *Kejahatan Siber; Cyber Crime Suatu Pengantar*, Kencana Prenada Media Group, Jakarta, 2013.

Muladi and Diah Sulistyani, *Kompleksitas Perkembangan Tindak Pidana dan Kebijakan Publik*, Alumni, Bandung, 2016.

Muladi and Dwidja Priyatno, *Pertanggungjawaban Pidana Korporasi*, Kencana Prenada Media Group, Jakarta, 2010.

I Wayan Parthiana, *Hukum Pidana Internasional*, Yrama Widya, Bandung, 2006.

Sigid Suseno, *Yurisdiksi tindak Pidana Siber*, Refika Aditama, Bandung, 2012.

United Nations Office on Drugs and Crime, *The Globalization of Crime A Transnational Organized Crime Threat Assessment*, United Nations Office on Drugs and Crime, Vienna, 2010.

----------, *Comprehensive Study on Cybercrime Draft February 2013*, United Nations, New York, 2013.

Widodo, *Aspek Hukum Pidana Kejahatan*, Mayantara, Aswaja Pressindo, Yogyakarta, 2013.

Other Documents

Balboni, Paolo and Pelino, Enrico, "Law Enforcement Agencies' Activities in the Cloud Environment: a European Legal Perspective", *Information & Communications Technology Law*, Vol. 22, No. 2, 2013.

Cook, Sam, "Cybercrime Stats & Facts for 2016–2017", https://www.comparitech.com/vpn/cybercrime-statistics-2016-2017/, accessed on January 2018.

Digital Watch Observatory, "Legal Frameworks", https://dig.watch/issues/cybercrime, accessed on January 2018.

Hui, Kai-Lung, Seung Hyun Kim, Qiu-Hong Wang, "Cybercrime Deterrence and International Legislation: Evidence From Distributed Denial of Service Attacks", *MIS Quarterly,* Vol. 41 No. 2, 2017.

Hukum Online, "Perjanjian Internasional untuk Tanggulangi Cybercrime Disiapkan", http://www.hukumonline.com/berita/baca/hol2579/perjanjian-

internasional-untuk-tanggulangi-icybercrimei-disiapkan, accessed on January 2018.

Moise, Adrian Cristian, "Some Considerations on the Phenomenon of Cybercrime", *Journal of Advanced Research in Law and Economics*, Vol. 5, Issue 1, 2014.

Moitra, Soumyo D., "Developing Policies for Cybercrime Some Empirical Issues", *European Journal of Crime, Criminal Law and Criminal Justice*, Vol. 13, Issue 3, 2005.

Morgan, Steve, "Top 5 Cybersecurity Facts, Figures and Statistics for 2017", https://www.csoonline.com/article/3153707/security/top-5-cybersecurity-facts-figures-and-statistics-for-2017.html, accessed on January 2018.

Reiny Dwinanda, "G20 Meeting Discusses Cybercrime: Sri Mulyani", http://en.republika.co.id/berita/en/national-politics/17/10/16/oxwxi4414-g20-meeting-discusses-cybercrime-sri-mulyani, accessed on January 2018.

Supriyadi, Daniar and Dethan, Katherine E. "On the lookout for cyberwar", https://www.thejakartapost.com/academia/2018/05/14/on-the-lookout-for-cyberwar.html, accessed on March 2018.

United Nations Congress on Crime Prevention and Criminal Justice, "Recent developments in the use of science and technology by offenders and by competent authorities in fighting crime, including the case of cybercrime", *Working Paper*, presented in Twelfth United Nations Congress on Crime Prevention and Criminal Justice, Salvador, Brazil, 12-19 April 2010.

United Nations Office on Drugs and Crime, "Global Programme on Cybercrime," https://www.unodc.org/unodc/en/cybercrime/global-programme-cybercrime.html, accessed on January 2018.

Legal Documents

Law Number 11 of 2008 on Information and Electronic Transactions [*Undang-Undang Nomor 11 Tahun 2008 Tentang Informasi dan Transaksi Elektronik*].

Law Number 19 of 2016 on Amendments to The Act of Republic of Indonesia Number 11 of 2008 on Information and Electronic Transactions [*Undang-Undang Nomor 19 Tahun 2016 Tentang Perubahan atas Undang—Undang Nomor 11 Tahun 2008 Tentang Informasi dan Transaksi Elektronik*].

Convention on Cybercrime, Budapest, 23.XI.2001 (Treaty 185).

Additional Protocol to the Convention on Cybercrime, concerning The Criminalisation of Acts of a Racist and Xenophobic Nature Committed through Computer Systems Strasbourg, 28.I.2003 (Treaty No.189).