CYBERCRIME AND GLOBAL SECURITY THREATS: A CHALLENGE IN INTERNATIONAL LAW

WIDYA SETIABUDI SUMADINATA
Faculty of Social and Political Sciences, Padjadjaran University, Bandung, Indonesia
Email: w.setiabudi@unpad.ac.id

Abstract
This research aims to examine the challenges faced in handling cyber crimes and global security threats from the perspective of international law. In the digital era, cyber crimes are increasing and causing detrimental impacts both at the national and international levels. Therefore, international cooperation and strong law enforcement are needed to overcome this challenge. The research method used in this study is a descriptive-analytical approach. This research was conducted by analyzing regulations and policies that apply at the international and national levels, as well as literature studies from reliable sources. The results of the research show that the challenges faced in handling cyber crime and global security threats cannot be solved individually by a country. Strong international cooperation and harmonization of international law are needed to overcome this challenge. International cooperation between countries in the field of information and technology is very important to build better cybersecurity.

Keywords: Cyber Crime, Global Security, International Law.

I. INTRODUCTION

Changes in the world in the last few decades have had a significant impact on countries, especially regarding threats. When threats to physical military security—such as war—in the world are decreasing in intensity, discussions about security for countries are also expanding in terms of territory, politics, economy, and technology (Ramadhan, 2019). This is because the world is currently in a phase of globalization which has led to global interdependence while increasing competition between countries in various aspects. In the era of competitive globalization, technology then becomes a very influential aspect for a country to survive (Yazid & Lie, 2020).

Most people today use some type of ICT, and internet-based technologies in particular have encouraged widespread adoption. (Chotimah, 2019). Due to the difficulty in identifying actors in cyberspace (cyber) for specific acts and actions in a place that have an effect or impact in all parts of the world, a wide variety of actors, both state and non-state, pose potential threats to disrupt the network. As a result, the Internet is now an integral element of contemporary life. (Jaishankar, 2007)

Alterations in interstate disputes have also resulted from the rapid growth of internet use. Traditional and conventional methods of warfare are no longer employed by countries. Therefore, the power of a state is measured not just in terms of its military might, but also in terms of its cultural influence, economic might, political influence, and technological prowess. (Madu, 2008). Because of this, rivalry and war are becoming more covert. Wars and conflicts within a country are fought not just by the military, but also by non-military, non-state entities. Cyberspace is becoming vulnerable to forms of warfare that have abandoned conventional tactics. Cyberspace now faces new dangers from forms of warfare that abandon conventional tactics. (Haikal, 2019). Cyberattack precursor threats are a real and present danger. A nation that recognizes the risks associated with information sharing online will likely invest in a security infrastructure capable of mitigating those risks. Cybercrime assaults using Distributed Denial of Service (DDoS) have stopped state activity in the past, as seen in the events of Estonia in 2007 and Georgia in 2008.

Individual hackers, hacker groups, hacker activities, NGOs, terrorism, organized crime groups, and the private sector (including internet service providers, wireless carriers, and security firms) pose the greatest danger to national security and sovereignty in cyberspace. (Rahmawati, 2017). The Indonesian president and other high-ranking state officials were the targets of cyber crime threats after it was revealed that Australia had spied on their private communications using documents leaked by former National Security Agency (NSA) contractor Edward Snowden. (Rahman, 2020).

Computer crime has evolved into cybercrime. According to Rene L. Pattiradjawane, the legal concept of cyberspace, cyberlaw, and cyberline that can create a large community of internet network users (60 million) involving 160 countries has raised the wrath of legal practitioners to create security through regulation, especially protection of private property. (Rene L.

Pattiradjawane, 2000). International law defines international crime as acts that threaten the stability of international community ties and harm the legitimacy of several or all countries; cybercrime fits this description. (Ketaren, 2016).

John Spiropoulos disclosed that cybercrime is both effective and quick, making it very challenging for law enforcement to apprehend those responsible for the crimes. (Sipropoulus, 1999). The law serves multiple purposes, one of which is to ensure that the process of national development is carried out without hiccups and to protect the outcomes that have been reached. It needs to be able to defend the rights of those who utilize internet services while also being able to take tough action against people who commit cybercrime. The number of offenses committed through the use of the internet, also known as "cyber crime," has significantly increased in recent years. This is in agreement with the adage that "crime is a product of society itself," where crime committed through the use of this information technology mode will gradually grow in a society that is increasingly accustomed to cyberspace. [Cyberspace] (Van Duyne, 1995).

In dealing with cyber crimes and global security threats, a strong and effective legal framework is needed. However, challenges in the field of international law are still a serious concern. This is caused by differences in legal systems and policies between countries as well as problems in international coordination and cooperation in law enforcement (Ardiyanti, 2016). Therefore, this research will examine the challenges in dealing with cyber crimes and global security threats from the perspective of international law. This research will look for effective solutions to overcome these challenges by considering strong international cooperation and harmonization of international law.

This research is expected to provide benefits in providing a better understanding of the challenges in dealing with cyber crimes and global security threats from an international legal perspective and provide policy recommendations that can enhance international cooperation and effective law enforcement in addressing these challenges . Besides that, this research is expected to be a source of information for research related to cyber security and international law.

II. METHODS

This study uses a qualitative approach that refers to the meaning, concept, definition, characteristics, metaphors, symbols, and descriptions of things. Qualitative research is carried out through searching for an answer by examining various social settings and groups or individuals in a social setting (Rukajat, 2018). In this case, qualitative research understands the environment studied through symbols, rituals, social structures, social roles, and so on. According to Berg et al., qualitative techniques here allow researchers to share in the understanding and perceptions of others and explore how people structure and give meaning to everyday life. 16 In the data collection technique here, the author only uses literature studies or literature reviews with descriptive method from previous research sources and other secondary data. These libraries come from annual reports as well as studies conducted by government and non-government agencies, international treaty documents, government magazines, and online news that are still relevant to the research object.

III. RESULTS AND DISCUSSION

1. Cyber Crime as a Transnational Crime

A transnational crime or transnational crime is a crime or crimes that cross national borders, according to one definition of the term. At the Eighth United Nations Congress on the Prevention of Crime and the Treatment of Offenders, which took place in the 1990s, this idea was presented to the international community for the first time. (Clark, 1989). Prior to that time, the phrase "organized crime" was the one that came into use initially. structured crime is defined by the United Nations as "large-scale and complex criminal activity carried out by groups of persons, however loosely or efficiently organized for the enrichment of those participating and at the expense of the community and its members." In other words, organized crime is a problem that affects the entire community. (Abadinsky, 2012).

It is a social phenomenon that involves individuals, locations, and groups, and it is also influenced by a variety of social, cultural, and economic elements. Transnational crime is a social phenomenon. As a direct consequence of this, several nations have a propensity to adhere to a variety of distinct philosophies with regard to the notion of transnational crime. According to Haken (2011), one definition of transnational crime is the behavior of ongoing organizations that involve two or more nations, with such activity being recognized as criminal by at least one of these nations. Specifically, transnational crime may be defined as the behavior of ongoing organizations that involve two or more nations.

In the meantime, the use of internet technology has given rise to a new type of criminal activity known as cybercrime. According to some points of view, cyber crime is synonymous with computer crime. A computer crime is "any illegal act that requires knowledge of computer technology for its perpetration, investigation, or prosecution," according to the definition provided by the Department of Justice of the United States. (Abidin, 2017). In his article from 1989, Andi Hamzah defined "computer crime" as "Crime in the field of computers in general can be interpreted as illegal use of computers." This was stated in Andi Hamzah's work. This definition is the same as that which is provided by the Organization for the Development of European Community, which defines computer crime as "any illegal, unethical, or unauthorized behavior relating to the automatic processing and/or the transmission of data." This definition has been adopted by the World Wide Web Consortium.

From some of the definitions above, I can briefly say that cybercrime can be defined as an illegal act committed by using the internet as the main medium based on the sophistication of computer and telecommunications technology. In this case, of course, it will be difficult for us to track down who the person who committed the crime is, but it is not impossible to find the perpetrators.

Currently, several countries categorize cybercrimes as transnational crimes, because the actions can be carried out in Country B, by citizens of Country A, but the victims are in Country C. In a technological setting, the nature of cyber activities is borderless or cross-border. The transnational dimension attached to cyber technology greatly benefits criminals. Perpetrators of crimes can commit crimes against victims in any country where the victim is located. Victims of cybercrime are not limited to individuals, but also organizations or companies and even countries as a whole. Another advantage for cybercriminals is the disparity in regulations relating to cybercrime in each country. In fact, there are still many countries that do not yet have laws that specifically regulate cyber crimes. This certainly makes it easier for cybercriminals to freely carry out their activities without being entangled in the law.

Based on the motives of their activities, telematics crimes (cyber crimes) can be classified into:

a) Unauthorized entry. A crime committed when someone illegally penetrates or infiltrates a computer network system without the permission or knowledge of the computer network system's owner. This offence includes probing and port. Criminals (hackers) typically do this with the goal of sabotage or theft of sensitive and confidential information. However, there are individuals who do it just because they want to test their talents against a system with a high level of protection. With the advancement of Internet/intranet technologies, this type of crime is becoming more common.
b) Illegal Materials. Crimes done by entering data or information on the internet concerning something that is wrong, unethical, illegal, or disrupts public order. Loading of fake news or slander that will destroy the dignity or self-esteem of other parties, matters related to pornography or loading of information that is a state secret, agitation and propaganda against the legitimate government, and so on.
c) Intentional virus spread. The virus is typically disseminated through the use of e-mail. People whose email systems are infected with viruses are frequently unaware of this. The malware is then emailed to another location.
d) Forgery of data. Crimes conducted with the intent of altering data on vital papers stored on the internet. These documents are typically owned by institutions or organizations with database websites. This crime is typically targeted at e-commerce documents by making it appear as if there was a "typo," which benefits the culprit because the victim enters personal information and credit card numbers that can be exploited.
e) Extortion, sabotage, and cyber espionage Cyber espionage is a crime that involves using the internet to conduct espionage against other parties by breaking into the target party's computer network system.
f) Cyberstalking Using a computer, this type of crime is committed to annoy or harass someone.
g) Carding Carding is a crime performed to steal credit card numbers from other individuals and use them in internet trading operations.
h) Cracker and hacking The term "hacker" usually refers to someone who is fascinated with computer systems and how to increase their capabilities. Crackers are those who frequently carry out damaging behaviors on the internet. You could say that this cracker is a hacker who exploits his abilities for evil.

i) Typosquatting and Cybersquatting Cybersquatting is a crime performed by registering another person's domain name and then attempting to sell it to that firm for a greater price.
j) Terrorism in the Cyberspace Cyberterrorism is an act of cybercrime if it threatens the government or citizens, such as hacking into government or military sites.

Cybercrime is a form of crime committed using computer technology and internet networks. Cybercrime is no longer limited to the national scope, but has become a global phenomenon because it can be committed by actors from any country and have a wide impact. Therefore, cyber crime which is a transnational crime is a threat to global security (Broadhurst, 2006).

Cybercrime does not only threaten a country's national security, but can also have a broad and global impact. Currently, business, finance, trade and political activities are increasingly dependent on information technology and internet networks. Therefore, cyber crime can threaten global economic stability and national security around the world (Grabosky, 2014)

Cybercriminals can use technology to create malicious software, such as viruses and malware, to attack critical systems and networks in various sectors, such as the financial, energy and healthcare sectors. In some cases, cyberattacks have caused significant economic losses and impacted critical infrastructure, such as electricity and transportation systems (Choo, 2011).

Cybercrime can also pose a threat to a country's national security. Several countries have been known to use cyber technology to carry out espionage and hacking against other countries, both for economic and political purposes. In addition, terrorist and criminal groups also use cyber technology to carry out their crimes, such as carrying out attacks on government websites and networks, committing personal data theft, and committing online fraud (Jang-Jaccard & Nepal, 2014).

To deal with global security threats caused by cyber crimes, it is necessary to make collaborative efforts between countries, international institutions and the private sector. Coordination and cooperation between countries is very important in overcoming cyber crime, because cyber crime is not limited by national borders and can occur in different areas at the same time.

In addition, efforts are needed to strengthen the international legal framework that can overcome challenges in global security. The Budapest Convention on Cybercrime is an example of an international agreement that can facilitate international cooperation in overcoming cybercrime. However, strong and effective policies and international legal frameworks need to be continuously developed to be able to deal with increasingly sophisticated and complex cyber crimes.

1. International Legal Instruments in Combating Cyber Crime

Cyber crime is still a new discussion in international law, so there are no specific rules governing this cyber crime. In committing this crime, hackers take advantage of cyber space to access data and copy data. Cyber space which includes computer networks and the internet can eliminate state jurisdiction in law enforcement if it is done from a different country. Regarding this matter, law enforcement with conditions like this requires legal instruments that can accommodate the laws of other countries. The rules that can regulate behavior between countries including international communities and organizations are international law (Storey & Wallace, 2001).

Global Strategy has responded to fears about pervasive cybercrime. Countries came up with it so that everyone would be on the same page about being watchful about cybercrime, so that there would be international obligations to combat cybercrime, so that there would be international collaboration to combat cybercrime, and so that a no-nonsense plan could be implemented to deal with cybercrime. The United Nations has implemented a number of agreements related to cybercrime.

At Point 18 of the Tenth Vienna United Nations Congress on the Prevention of Crime and the Treatment of Offenders, conducted from April 10-17, 2000, the following was stated. We have decided to request the Commission on Crime Prevention and Criminal Justice to make action-oriented policy recommendations on the prevention and control of computer-related crime, taking into account the work being done in various venues. In addition, we will continue to work to improve our capacities in the areas of high-tech crime prevention, investigation, and prosecution.

At the eleventh United Nations Congress in Bangkok, Thailand, effective methods of combating transnational organized crime, international cooperation against terrorism, inter-terrorist relations, and other criminal activities were discussed. The meeting in Bangkok was entitled Strategic Alliance in Crime Prevention and Criminal Justice. In addition, online offenses committed by point-followers are discussed.

a) We reiterate the importance of implementing existing laws and increasing national and international cooperation in criminal matters, with special focus on preventing cybercrime, money laundering, and trafficking. There has been no breach of the agreement regarding the extradition of cultural property, the provision of mutual legal assistance, or the return of confiscated commodities and criminal gains.
b) We acknowledge that the rapid development of communication networks and new computer systems in the present age of globalization has led to an increase in the criminal exploitation of information technology. As a result, we support efforts to forge partnerships with the business community in order to better prevent, investigate, and prosecute crimes committed using technology and computers. We commend the United Nations' efforts to combat cybercrime on a global scale, including its participation in regional and other international forums. We urge the Commission on Crime Prevention and Criminal Justice to use its existing expertise to look into the possibilities of additional help in this area under the auspices of the United Nations in collaboration with other like-minded organizations.

At the Thirteenth United Nations Congress on Crime Prevention and Criminal Justice, which took place in Doha, Qatar, between April 12 and 19, 2015, the topic of cybercrime prevention was discussed once again. Doha, Qatar was the site of the Thirteenth United Nations Congress on Crime Prevention and Criminal Justice from April 12th through the 19th, 2015, and Workshop 3 of this event focused on crime prevention in the digital era. The third workshop explored the potential of education and global collaboration to improve responses to cybercrime and the trafficking of cultural artifacts inside the criminal justice system. National cybercrime policies, strategies, and regulations should serve as the basis for developing response frameworks and setting priorities. The United Nations Office on Drugs and Crime (UNODC) plans to launch a digital database dedicated to cybercrime in the near future. This database will include information on cybercrime awareness and education, international collaboration, law enforcement capabilities, legislation, prevention, and public-private partnerships. (scheduled for release in 2015).

The European Union's Convention on Cyber Crime from 2001 is the primary international legal instrument now gaining the greatest attention for regulating the issue of cyber crime. Despite having its origins in a European regional organization, this convention has evolved to the point that any nation with a commitment to combating cyber crime can ratify it and gain access to its resources. On November 23, 2001 in Budapest, Hungary, EU (Council of Europe) member states drafted and adopted the Convention on Cybercrime, which is now numbered 185 in the European Treaty Series. The Convention will enter into force once it has been approved by at least five (5) nations, including at least three (3) countries that are members of the Council of Europe.

Four separate sections make up the Cybercrime Convention. Included are chapters on definitions and definitional issues; national approaches; international cooperation; and final provisions. The definition of cybercrime is left vague in the Cyber Crime Convention. For the purposes of creating this convention, Chapter I of the Cybercrime Convention only defines computer systems, computer data, service providers, and data traffic.

The Cybercrime Convention not only controls procedural legislation for these crimes, but also serves as a guideline that countries can use as the norm for enacting laws to prevent crimes committed in cyberspace. The goal of this agreement is to have the participating states standardize the application of procedural legislation to the investigation of cybercrime. Unless otherwise specified in Article 21, the authorities and processes specified in paragraph 1 of this article shall be used by each Party for

(1) offenses established pursuant to Articles 2 to 11 of this Convention;
   a. other criminal acts committed using a computer system; And
   b. collection of evidence in electronic form from a crime.

Procedural law also applies to other aspects of the Cybercrime Convention. In particular, measures that can be regulated within the country include safeguarding and securing, speeding up the maintenance of computer data, speeding up the storage and disclosure of some data traffic, handover orders, searching and seizing computer data, collecting computer data in real time, and wiretapping data content. maintaining legal safeguards for people's rights. Cyberspace jurisdictions are established in accordance with the Cybercrime Convention. To have jurisdiction over anything means to have the legal authority to make decisions about that something, be it a person, a place, or an event. (law).

The sharing of information about cybercrime cases across borders is an area where international cooperation is urgently needed. This is because the transnational nature of cybercrime allows crimes to be perpetrated across national borders regardless of the location of either the offender or the victim. Since states with sovereignty and resource concerns cannot handle it individually, international collaboration as part of a criminal policy is necessary and even strategic for combatting international and transnational crimes, as noted by Muladi and Diah Sulistyani. International cooperation in criminal situations is carried out through relevant international law instruments. As a result, agreements reached under uniform or reciprocal laws and national laws are used, to the maximum extent possible, to probe or process crimes involving electronic systems and data or to collect evidence of such crimes.

The Budapest Convention lays the groundwork for international cooperation in the field of cybersecurity, including the exchange of information on cybercrimes, investigative cooperation, and extradition of cybercriminals. In addition, the convention encourages member nations to improve their national cybersecurity and legal systems. Even though this convention is a significant step in the fight against cybercrime, there are still a number of things that need to be improved in international law pertaining to the prevention of cybercrime. First, efforts are still required to increase global awareness and comprehension of cybercrime. This can be achieved by intensifying public education and campaigning.

Second, there needs to be a more comprehensive legal framework to deal with increasingly complex and diverse cyber crimes. This includes regulations on spreading hoaxes and harmful propaganda, as well as regulations on data privacy and the use of advanced technologies such as artificial intelligence and blockchain. Third, it is necessary to increase cooperation between countries and international institutions in overcoming cyber crimes. There is a need for more effective cooperation and exchange of information in terms of preventing and acting on cybercrime around the world.

In order to improve protection against cyber crimes, there needs to be continuous efforts to develop a strong and effective international legal framework. This will require collaboration between states, the private sector, and international institutions in addressing the increasingly complex and rapidly evolving challenges of global security.

IV. CONCLUSION

Based on the discussion above, it can be concluded as follows, that cyber crime is a crime that threatens global stability and security. This crime has become a loophole for perpetrators to carry out their actions, especially in countries that have low digital security and experience a legal vacuum regarding cybercrime activities during peacetime. Thus, preventive measures that can be taken by each country in dealing with crimes against their country are increasing digital security and forming legal instruments that discuss cybercrime activities and specific sanctions. the Budapest Convention on Cybercrime has provided a comprehensive legal framework, but greater efforts are still needed to increase awareness and understanding of cybercrime, develop a more comprehensive legal framework, and enhance cooperation between countries and international institutions in dealing with cybercrime. In the face of increasingly complex and rapidly evolving global security challenges, there is a need for close collaboration between countries and the private sector in developing effective cybersecurity technologies and strategies. In this regard, international law has an important role in providing a strong and clear legal framework for dealing with cyber crimes, as well as facilitating international cooperation in the field of cyber security. Therefore, efforts to improve international law related to cybersecurity need to be continued to ensure the security and stability of a world that is increasingly connected and dependent on digital technology.

REFERENCES

[1] Abadinsky, H. (2012). Organized crime. Cengage Learning.

[2] Abidin, D. Z. (2017). Crime in Information and Communication Technology. Processor Journal, 10(2), 509-516.

[3] Ardiyanti, H. (2016). Cyber-security and its development challenges in Indonesia. Journal Politica Dynamics of Domestic Political Problems and International Relations, 5(1).

[4] Broadhurst, R. (2006). Developments in the global law enforcement of cyber-crime. Policing: An International Journal of Police Strategies & Management, 29(3), 408-433.

[5] Choo, K. K. R. (2011). The cyber threat landscape: Challenges and future research directions. Computers & security, 30(8), 719-731.

[6] Chotimah, H. C. (2019). Indonesian Cyber Security Governance and Cyber Diplomacy Under the National Cyber and Encryption Agency. Journal of Politica Dynamics of Domestic Political Problems and International Relations, 10(2), 113-128.

[7] Clark, R. S. (1989). The Eighth United Nations Congress on the Prevention of Crime and the Treatment of Offenders-Havana, Cuba, August 27-September 7, 1990. Crim. LF, 1, 513.

[8] Grabosky, P. (2014). The global dimension of cybercrime. In Global Crime Today (pp. 146-157). Routledge.

[9] Haikal, M. H. (2019). China's Censorship Policy Against Multinational Companies in the Field of Ict (Information Communication Technologies) (Case Study of Google Inc.). Global Political Studies Journal, 3(1), 73-89.

[10]Haken, J. (2011). Transnational crime in the developing world. Global financial integrity, 32(2), 11-30.

[11]Honey, L. (2008). Ambalat Netwar between Indonesia and Malaysia, 2005: Theoretical Reflections on International Relations in the Internet Age. Global & Strategic, 2(1), 1-22.

[12]Jaishankar, K. (2007). Establishing a theory of cyber crimes. International Journal of Cyber Criminology, 1(2), 7-9.

[13]Jang-Jaccard, J., & Nepal, S. (2014). A survey of emerging threats in cybersecurity. Journal of Computer and System Sciences, 80(5), 973-993.

[14]Ketaren, E. (2016). Cybercrime, cyber space, and cyber law. Journal of the Times, 5(2), 35-42.

[15]Pattiradjawane, R. L. (2000). Globalization and Technology Towards a New Balance. Compass Daily. Date, 28.

[16]Rahman, L. L. A. (2020). Implications of Defense Diplomacy on Cyber Security in the Context of Security Politics. Journal of Defense Diplomacy, 6(2), 1-93.

[17]Rahmawati, I. (2017). Analysis of Risk Management of Cyber Crime Threats (Cyber Crime) in Increasing Cyber Defense. Journal of Defense & State Defense, 7(2), 35-50.

[18]Ramadhan, I. (2019). Cyber Security Security Strategy in the Southeast Asia Region. Journal of Asia Pacific Studies, 3(2), 181-192.

[19]Rukajat, A. (2018). Qualitative research approach (Qualitative research approach). Deepublish.

[20]Sipropoulus, J. (1999). Cyber Crime Fighting, The Law Enforcement Officer's Guide to Online Crime. The National Cybercrime Training Partnership, Introduction.

[21]Storey, H., & Wallace, R. (2001). War and peace in refugee law jurisprudence. American Journal of International Law, 95(2), 349-366.

[22]Van Duyne, P. C. (1995). The phantom and threat of organized crime. Crime L. & Soc. Change, 24, 341.

[23]Yazid, S., & Lie, L. D. J. (2020). The impact of the pandemic on human mobility in Southeast Asia. Scientific Journal of International Relations, 75-83.