International Journal of Law, Crime and Justice

E-ISSN: 3047-1362
P-ISSN: 3047-1370

*Review Article*

# Position of Civil Crime as a Transnational Crime

**Muhammad Hatta [1*], Dianti Novita Marwa [2], Lisa Lestari [3], Lena Mahara Simahate [4], Herika Novita [5], Abdul Azis[6]**

[1,2,3,4,6] Magister Hukum Fakultas Hukum, Universitas Malikussaleh, Indonesia 1,2,3,4,6; e-mail : muhammad.hatta@unimal.ac.id
[5] Magister Hukum Fakultas Hukum Universitas Malikussaleh, Indonesia 5; e-mail : herika.247410101047@mhs.unimal.ac.id
*****Corresponding Author : Muhammad Hatta

**Abstract:** Cybercrime is an unlawful act committed using the internet based on sophisticated computer technology, networks and other information technologies. This crime not only affects individuals, but also financial institutions, critical infrastructure, and even national and international security. Cybercrime has characteristics that distinguish it from conventional forms of crime, namely the ability to cross geographical boundaries of countries without physical barriers so that in this case this cybercrime is referred to as transnational crime. The purpose of this study is to examine and analyze the position of cybercrime in the perspective of international law and to examine and analyze the position of cybercrime in the perspective of national law. The results of the study were obtained from the perspective of international law, cybercrime has a strategic position as a global threat that requires a cross-country legal approach. Meanwhile, from the perspective of national law, cybercrime has a central position in the reform of the Indonesian criminal law system. Through the formation and improvement of the ITE Law, as well as increasing the capacity of law enforcement and the community, the state seeks to create a safe, fair and responsible digital space

**Keywords:** Crime; Mayantara; Position; Transnational

## 1. Introduction

The development of information and communication technology has brought about major changes in the patterns of social, economic, and political interactions throughout the world. On the one hand, digitalization has provided convenience and efficiency in various aspects of life. However, on the other hand, this progress has also been exploited by irresponsible parties to commit crimes online, known as cyber-crime.

Cybercrime is one of the new forms or dimensions of modern crime caused by the rapid development of technology. This crime has even become an international concern. Cybercrime is one of the dark sides of technological progress that has a very broad negative impact on all areas of modern life today. Cybercrime is an unlawful act carried out using the internet which is based on sophisticated computer and telecommunications technology. Cybercrime actually not only uses sophisticated computer technology but also utilizes information technology in its operations.

This crime not only impacts individuals, but also financial institutions, critical infrastructure, and even national and international security. Ransomware attacks, theft of personal data, cross-border fraud, and the spread of global malware are clear examples of how cybercrime crosses the boundaries of national sovereignty and requires a cross-jurisdictional response. Cybercrime is a problem faced by all countries in the world. The proof is that cybercrime was made one of the topics of discussion at the 8th UN Congress on The

**Received: April, 20 2025**
**Revised: May, 04 2025**
**Accepted: May, 18 2025**
**Online Available: May, 20 2025**
**Curr. Ver.: May, 20 2025**

Prevention of Crime and the Treatment of Offender in 1990 in Havana, Cuba and the 10th in Vienna, Austria.

The number of Cyber Crime cases or crimes in cyberspace that occur in Indonesia is the highest in the world, among other things, because of the many activities of hackers in the country. Cyber Crime cases in Indonesia are number one in the world. Cyber Crime against children is said to have become a new trend in many countries, including Indonesia. The use of the internet that is almost uncontrolled makes children vulnerable to becoming victims of various crimes in cyberspace. Sexual crimes, pornography, trafficking, bullying and other forms of crime committed online are an increasingly big threat to the next generation of the nation. According to data published by KPAI, from 2011 to 2014, the number of children who are victims of pornography and online crimes in Indonesia has reached 1,022 children. In detail, children who are victims of online pornography are 28%, online child pornography 21%, online child prostitution 20%, pornographic CD objects 15% and children who are victims of online sexual violence 11%. This number is predicted to continue to increase if not addressed optimal.

Cybercrime has characteristics that distinguish it from conventional forms of crime, namely the ability to cross geographical borders without physical barriers. Perpetrators can carry out their actions from other countries, attack targets in different locations, and store the proceeds of their crimes on servers spread across the world. These characteristics make cybercrime a transnational crime, as defined in United Nations Convention Against Transnational Organized Crime (UNTOC).

Indonesia itself has recognized the seriousness of the threat of cybercrime by adopting a number of legal provisions, such as through Law Number 11 of 2008 concerning Electronic Information and Transactions (UU ITE) and international cooperation in the field of cyber law enforcement. However, a national approach alone is not enough. Because of the cross-border nature of this crime, efforts to combat it must involve international cooperation, both in terms of exchanging intelligence information, mutual legal assistance, and extradition of perpetrators.

Therefore, understanding the position of cybercrime as part of transnational crime is very important, not only in the context of developing a national legal system that is responsive to global dynamics, but also as a basis for Indonesia to strengthen its legal position and strategy in international forums.

This paper aims to analyze the position of cybercrime as a transnational crime, with the focus of the study being 1. examining and analyzing the position of cybercrime from an international legal perspective and 2. examining and analyzing the position of cybercrime from a national legal perspective.

## 2. Literature Review

Cybercrime is a crime that occurs in cyberspace that does not recognize jurisdictional boundaries and internet use by anyone and anytime throughout the world. It can be classified that cybercrime is a transnational crime. Because of its transnational nature, proof of cybercrime is also something that requires attention for every country including Indonesia.

Conceptually, transnational crime is a criminal act or crime that crosses countries. This concept was first introduced internationally in the 1990s at the Eight United Nations Congress on the Prevention of Crime and the Treatment of Offenders. According to the United Nations Convention Against Transnational Organized Crime in 2000, a crime can be said to be transnational if it consists of:

a. 1)Conducted in more than one country,
b. 2)Conducted in one country but the essentials of preparation, planning, directing and supervision are conducted in another country,
c. 3)Carried out in one country but involving an organized crime group (organized criminal) where the crime is committed in more than one country.
d. 4)Done in one country but has consequences in another country.

Cybercrime, which is a transnational crime, is closely related to the use of technology that is primarily based on computers and telecommunications networks. There are many classifications of cybercrime groups. Cybercrime as a transnational crime can be grouped into several forms, including:

a. Unauthorized access to computer system and service

   A crime committed by entering/infiltrating a network system illegally without permission or without the knowledge of the owner of the computer system being entered.

b. Illegal Contents

   It is a crime to enter data or information on the internet about something that is incorrect, unethical and can be considered unlawful or disruptive to public order.

c. Dataforgery

   It is a crime to falsify data on important documents stored as scriptless documents via the internet.

d. Cyber Expionage

   It is a crime that uses the internet network to carry out spying activities against other parties, by entering the computer network system. (computer network sistem).

e. Cyber Sabotage and Extortion

   This crime is committed by causing disruption, damage or destruction to data, computer programs or computer network systems connected to the internet.

## 3. Proposed Method

### 3.1 Type And Research Approaches

The type of research in this study is qualitative research. namely research that intends to understand the phenomenon of what is experienced by the research subject, for example behavior, perception, motivation, actions and others. This research approach uses a normative legal approach. Normative legal research is legal research that places law as a building of a normative system. The normative system in question is regarding the principles, norms, rules of laws and regulations, court decisions, agreements and doctrines.

### 3.2 Data Source

The data sources in this study come from secondary legal materials obtained through library research consisting of primary legal materials, secondary legal materials, and tertiary legal materials.

### 3.3 Data Collection Technique

The data collection technique used is library research (Literature Studi) and Document Study.

### 3.4 Data Analysis

Data analysis in this thesis research was analyzed qualitatively, namely analysis with analytical and prescriptive descriptive analysis.

## 4. Results and Discussion

### 4.1 The Position of Cybercrime in the Perspective of International Law

Cybercrime has developed into one of the most complex forms of crime and threatens global security stability. From an international legal perspective, this crime is recognized as a cross-border issue that requires cooperation between countries, because the perpetrators often operate from one jurisdiction, attack systems in other countries, and utilize digital infrastructure that is spread global.

Cybercrime does not yet have a single international legal instrument that is universally binding. However, a number of regional and multilateral instruments have attempted to regulate and coordinate its handling. One of the most influential international instruments is the Convention on Cybercrime or Budapest Convention (2001) adopted by the Council of Europe. This convention is the first international agreement to comprehensively regulate cybercrime, including aspects of criminalization, legal procedures, and cooperation between countries.

In international law, the position of cybercrime is also related to the principle of non-intervention and state sovereignty in cyberspace. Countries have sovereignty over the digital infrastructure in their territory, but at the same time are faced with a jurisdictional dilemma if the perpetrator or impact of the crime occurs outside the boundaries of national jurisdiction. This makes international cooperation a major pillar in dealing with cybercrime, either in the

form of bilateral/multilateral agreements, mutual legal assistance treaties (MLAT), as well as technical and intelligence cooperation between law enforcement agency.

In addition, the United Nations (UN) through the United Nations Office on Drugs and Crime (UNODC) also encourages countries to develop national and regional legal instruments to deal with cybercrime. In 2022, the UN General Assembly even approved the negotiation process towards a global convention on cybercrime, which aims to create a more inclusive and representative international legal framework.

However, differences in views between countries – for example between the European/US approach that emphasizes freedom of information and protection of digital human rights, versus the approach of other countries that emphasize state control over the digital space – pose a challenge in harmonizing international law on cybercrime. Cybercrime is categorized as a transnational crime because it can involve perpetrators, victims, and technological infrastructure from various jurisdictions. This crime covers various forms, from online fraud, digital identity theft, hacking of systems, to the distribution of illegal content through global networks. This creates challenges for international law, especially in terms of jurisdiction, extradition of perpetrators, data exchange, and standardization of electronic evidence (Schjolberg, 2008).

International legal instruments that are the main reference: Budapest Convention on Cybercrime (2001) – It is the first and most comprehensive international treaty on the prevention, disclosure and prosecution of cybercrime. Although drafted by the Council of Europe, the convention is joined by many non-European countries, such as Japan, the United States and Australia. However, countries such as Russia, China and India reject the convention on the grounds of digital sovereignty.

The public international legal instrument that regulates Cyber Crime issues that currently receives the most attention is the 2001 Convention on Cyber Crime initiated by the European Union. Although this convention was initially created by a European regional organization, in its development it is possible to be ratified and accessed by any country in the world that has a commitment to overcoming Cyber Crime. The countries that are members of the European Union (Council of Europe) on November 23, 2001 in the city of Budapest, Hungary have created and agreed to the Convention on Cybercrime which was then included in the European Treaty Series with Number 185. This convention will come into effect after being ratified by at least 5 (five) countries, including at least ratification by 3 (three) member countries of the Council of Europe. The substance of the convention covers a fairly broad area, even containing a criminal policy that aims to protect society from cyber-crime, both through laws and international cooperation. This is done with full awareness regarding the increasing intensity of digitalization, convergence and ongoing globalization of information technology, which according to experience can also be used to commit criminal acts.

UN General Assembly Resolution No. A/RES/75/282 (2021) – Through this resolution, the UN initiated negotiations towards the establishment of a new, more inclusive and representative international convention to combat cybercrime globally. United Nations Convention Against Transnational Organized Crime (UNTOC, 2000) – Although it does not specifically address cybercrime, this convention is the basis for international law in combating transnational organized crime, including in the context of the digital world

In addition to international agreements, regional frameworks also play an important role. For example, ASEAN has adopted the ASEAN Regional Plan of Action on Cybersecurity Cooperation which encourages cooperation between member states in enhancing legal and technical capacity to deal with cybercrime. However, there are still major challenges in harmonizing international cyber law, such as:

a. 1)Differences in legal systems and countries' approaches to internet regulation.
b. 2)The issue of digital sovereignty and state control over data and technological infrastructure.
c. 3)Lack of trust between countries in sharing intelligence data or digital evidence

The position of cybercrime in the perspective of international law occupies a very strategic and complex position, because it involves the dimensions of law, technology, and relations between countries. This crime is seen as a transnational threat that can cross state jurisdictional boundaries without physical barriers, thus challenging the basic principles of international law such as state sovereignty, non-intervention, and national criminal law jurisdiction.

Efforts that can be made to prevent transnational cybercrime can be done by strengthening international cooperation, extradition agreements between countries for cybercriminals, Mutual Legal Assistance Treaties (MLAT) or mutual legal assistance agreements, and exchanging intelligence information and digital forensic data between law enforcement agencies.

**4.2 The Position of Cybercrime in the Perspective of National Law**

The UN Congress has called on member states to tackle Cyber Crime with penal means. Although in reality it is not easy, but because the cybercrime cases that have occurred recently have caused unrest for the community, especially those who use computer and information facilities, legal protection for those who are harmed is a necessity that must be created immediately by the State.

Cybercrime in national law occupies an important and increasingly strategic position along with the rapid development of information and communication technology. Cybercrime not only impacts individuals or groups, but also threatens public interests, state security, and the integrity of the national legal system. Therefore, countries—including Indonesia must provide an appropriate legal response to address it. Cybercrime is often transnational in nature, so international cooperation in the form of extradition, mutual legal

assistance, and cooperation between law enforcement agencies is very important in handling this case.

The position of Cybercrime in national law is categorized as a special crime that is different from conventional crimes, both in terms of methods, tools, and scope. This causes national criminal law to have to adapt to be able to reach crimes committed through electronic media and internet networks.

Cybercrime has a significant position in the perspective of national law. Although there is no specific regulation that criminalizes every form of cybercrime, Law Number 1 of 2024 concerning the Second Amendment to Law Number 11 of 2008 concerning Electronic Information and Transactions (UU ITE) provides a strong legal basis for handling these cases. The ITE Law allows law enforcement against various crimes committed via the internet, such as fraud, data theft, hacking, and the distribution of illegal content.

The ITE Law is the main and strategic national legal instrument in dealing with the dynamics of cybercrime (cybercrime) in Indonesia. With a broad scope of regulations and developing enforcement mechanisms, the ITE Law is the foundation for creating a safe, orderly, and fair digital ecosystem. However, the continued effectiveness of the ITE Law remains dependent on regulatory updates and the balance between cybersecurity and the protection of civil rights.

**4.3 Discussion**

Based on the results of the study above, it can be stated that cybercrime is an unlawful act committed using the internet based on sophisticated computer technology, networks and other information technology. This crime not only affects individuals, but also financial institutions, critical infrastructure, and even national and international security. Cybercrime has characteristics that distinguish it from conventional forms of crime, namely the ability to cross geographical boundaries of countries without physical barriers so that in this case this cybercrime is referred to as transnational crime. The position of cybercrime in the perspective of international law, cybercrime has a strategic position as a global threat that requires a cross-country legal approach. Meanwhile, in the perspective of national law, cybercrime has a central position in the reform of the Indonesian criminal law system. Through the formation and improvement of the ITE Law, as well as increasing the capacity of law enforcement officers and the community, the state seeks to create a safe, fair and responsible digital space. Efforts that can be made to prevent transnational cybercrime can be done by strengthening international cooperation, extradition agreements between countries for cybercriminals, Mutual Legal Assistance Treaties (MLAT) or mutual legal assistance agreements Exchange of intelligence information and digital forensic data between law enforcement agencies.

## 5. Conclusions

From the research results, it can be concluded that cybercrime from an international legal perspective is seen as a very complex form of transnational crime, because it involves various legal jurisdictions, cross-border technology, and cross-country actors. Cybercrime is considered a form of global crime that does not recognize geographical boundaries, so it cannot be handled effectively only with national legal instruments.

## References


[1] A. K. Putra, "Harmonization of Cyber Crime Convention In Nation Law," *Jurnal Al-Ishlah Journal Science of Law*, vol. 20, no. 2, Faculty of Law, University Hasanuddin, Makassar.
[2] B. S. W. Brenner, *Cybercrime and the Law: Challenges, Issues, and Outcomes*. Northeastern University Press, 2010.
[3] Council of Europe, *Convention on Cybercrime (Budapest Convention)*, 2001.
[4] Empirical Legal Research, *Pustaka Pelajar*, Yogyakarta.
[5] Indonesian Child Protection Commission (KPAI), *Annual Report*, Indonesian Child Protection, 2015.
[6] Jurnal Hukum & Development, "Indonesia," *Journal Hukum & Development*, vol. 49, no. 2.
[7] Legal Science Journal, Faculty of Law, Jambi University, Jambi, 2014.
[8] L. J. Moleong, *Qualitative Research Methods*, Bandung: PT Remaja Rosdakarya, 2014.
[9] M. F. N. D. Mukti and Y. Achmad, *Dualism of Normative and Empirical Legal Research*, Yogyakarta: Pustaka Pelajar, 2010.
[10] M. S. Akub, *Cyber Crime Regulations in the Indonesian Legal System*, 2018.
[11] Raodia, "The Influence of Technological Developments on Cyber-Crime (Cybercrime)," *Jurnal Jurisprudentie*, vol. 2, no. 2, University Sarwegading Makassar, 2019.
[12] Rivandioza, "Criminal Policy for Handling Mayantara Crimes at the Southeast Aceh Criminal Research Unit," *Jurnal EduTech*, vol. 6, no. 1, Mar. 2020, Pasca Sarjana University Muhammadiyah Sumatera Utara.
[13] F. Simangunsong, "Law Enforcement Challenges Against Cybercrime in Southeast Aceh Criminal Research Unit," *Jurnal EduTech*, vol. 6, no. 1, Mar. 2019.
[14] United Nations, "United Nations Convention Against Transnational Organized Crime," Palermo, 2000.
[15] United Nations General Assembly, "Resolution 55/63: Combating the Criminal Misuse of Information Technologies," 2000.
[16] United Nations Office on Drugs and Crime (UNODC), *Comprehensive Study on Cybercrime*, 2013.
[17] United Nations Office on Drugs and Crime (UNODC), *Practical Guide for Requesting Electronic Evidence Across Borders*, 2021.