GIJLSS
Greenation International Journal of Law and Social Sciences
+62 81210467572 https://research.e-greenation.org/GIJLSS greenation.info@gmail.com
GREENATION RESEARCH

DOI: https://doi.org/10.38035/gijlss.v3i3
https://creativecommons.org/licenses/by/4.0/

Legal Dynamics of Handling Transnational Cybercrime Based on International Legal Principles

Gunawan[1], Muhammad Zainudin[2], Naya Amin Zaini[3]
[1]Universitas Darul Ulum Islamic Centre Sudirman Guppi, Indonesia,
gunawanlintang70@gmail.com
[2]Universitas Darul Ulum Islamic Centre Sudirman Guppi, Indonesia,
mzundaris@gmail.com
[3]Universitas Darul Ulum Islamic Centre Sudirman Guppi, Indonesia,
nayaaminzaini@gmail.com

Corresponding Author: gunawanlintang70@gmail.com[1]

Abstract: Cyber law enforcement at the international level faces complex challenges due to differences in jurisdiction and rapid technological developments. The study examines the significance of bilateral and multilateral cooperation in strengthening the effectiveness of cyber law enforcement, both through agreements between countries and coordination with international organizations such as INTERPOL and Europol. In addition, investment in cybersecurity technology, increasing human resource capacity, and collaboration between governments and the private sector are crucial factors in strengthening resilience to cyber threats. The role of technology companies is increasingly significant in developing more sophisticated security systems and supporting public education on data protection. With an integrated strategy, this study emphasizes the need for a holistic approach in dealing with cybercrime so that the investigation and law enforcement process can run more effectively and be coordinated globally.

Keywords: Cybercrime, Transnational, International Law

INTRODUCTION

The development of information technology has brought significant changes in various sectors of life, including government, finance, business, and social (Ardianto, 2024). Digitalization has increased global efficiency and connectivity, but on the other hand, it improve human dependence on information technology and the internet. New technologies such as cloud computing, the Internet of Things (IoT), and artificial intelligence are accelerating digital transformation, making it easier to manage data and communication (Hindarwati, 2024). However, this progress also opens up gaps for increasingly complex and difficult-to-control cybercrime threats, especially when involving cross-border actors with criminal or even political goals.

Cybercrime is no longer limited to the national scale but has developed into a transnational threat involving perpetrators from various countries by exploiting different legal and technological loopholes (Wahyuningsih, 2016). The forms of transnational cybercrime are very diverse, ranging from hacking, phishing, ransomware, and identity theft, to attacks on critical infrastructure such as banking, energy, and communication systems. These cyber-attacks are often carried out by organized criminal groups or even supported by certain countries for geopolitical interests (Rahmawati, 2017). Without good international coordination, many cybercrimes are difficult to prosecute due to differences in legal regulations in various countries.

Cases of major cyber attacks have shown how serious this threat is on a global scale. A real example is the WannaCry attack in 2017 which spread to more than 150 countries and paralyzed various important institutions, including hospitals and large companies. The NotPetya attack, which initially targeted Ukraine, also had a wide impact, disrupting multinational companies in various parts of the world. In addition, attacks on financial and government infrastructure are increasingly frequent, posing a major risk to the economic and political stability of a country (Bainus, 2023). With this increasing threat, closer international cooperation and the application of international legal principles are needed to ensure effective law enforcement against transnational cybercriminals (Pangestika, 2024).

Cybercrime has become a serious threat to national security because it can disrupt a country's political and economic stability (Wati, 2024). Cyberattacks targeting government institutions, financial systems, and critical infrastructure such as energy and transportation can paralyze public services and disrupt the economy. For example, cyberattacks on the electricity grid or banking system can cause social chaos and panic. In addition, threats to the state security system through theft of confidential data or sabotage of the defense system also have the potential to weaken state sovereignty and increase the risk of geopolitical conflict (Sarjito, 2024).

In the political realm, cyberattacks on elections or state institutions can disrupt a country's democracy and sovereignty (Mudjiyanto, 2024). For example, foreign interference through hacking of election systems or the spread of false information (disinformation campaigns) has become a strategy used to influence election results in various countries. In addition, terrorist groups or state actors can use cyberspace to conduct espionage, sabotage, or spread propaganda that threatens global order. Cybercrime also provides space for other illegal activities, such as terrorism financing, illegal arms trade, and money laundering carried out through the dark web (Iskandar, 2021).

The impact of cybercrime is not only limited to one country but can also shake global security (Saramuke, 2025). Transnational cybercrime is often difficult to handle because it involves various jurisdictions and differences in legal systems between countries, complicating law enforcement efforts. Cyberattacks on multinational companies or global financial institutions can cause international economic instability, especially if the attack impacts global financial markets or supply chains (Wangke, 2021). In addition, international-scale personal data breaches are an increasing threat, given that many technology companies store sensitive information from millions of users in various countries (Pakarti, 2023). With this increasing risk, stronger international cooperation and harmonization of regulations are needed to effectively deal with the threat of cybercrime.

Law enforcement against cybercrime faces various complex challenges, especially in terms of jurisdiction. Cybercrime is often committed across countries, where the perpetrator can be in one country, the victim in another country, and the infrastructure used to attack a different country (Arifah, 2011). It makes it difficult to determine which laws apply and which authorities have the authority to prosecute the perpetrators. In addition, differences in cyber law regulations between countries further complicate international cooperation,

because not all countries have the same standards in dealing with cybercrime (Tobing, 2024). For example, some countries do not criminalize certain actions that are considered cybercrimes in other countries, thus hampering the process of extradition and prosecution of perpetrators.

In international law, the principles of sovereignty and non-intervention play an important role in dealing with cases of interstate cybercrime (Pangestika, Application of International Legal Principles in Law Enforcement Against Cybercrime and Cyber Attacks., 2024). Every country has the right to protect its information systems and infrastructure from cyber attacks originating from abroad. However, this principle also limits a country's ability to prosecute perpetrators who are in the jurisdiction of another country without international cooperation. Therefore, cooperation between countries is a key element in cyber law enforcement. One of the main mechanisms that has been implemented is the Budapest Convention on Cybercrime, which provides a framework for countries to cooperate in the investigation, extradition, and prosecution of cyber criminals (Budiyanto, 2025).

In addition to international cooperation, efforts are needed to harmonize cyber law at the global level to be more effective in dealing with the threat of transnational cybercrime. Many developing countries still have limitations in terms of technology and human resources to deal with cybercrime, so they need assistance from developed countries to train and technology transfer. Harmonization of regulations at the international level can also help create clearer standards in dealing with various forms of cybercrime, including mechanisms for sharing information and coordinating law enforcement. Thus, the application of international legal principles in law enforcement against cybercrime not only aims to prosecute perpetrators effectively but also to strengthen global cybersecurity through closer cooperation between countries.

This research has a high urgency considering the rapid development of information technology accompanied by the increase in transnational cybercrime that can threaten national and global security. The complexity of cybercrime involving transnational actors poses challenges in law enforcement, especially related to differences in regulations, jurisdictions, and technological capacities between countries. Although international legal principles such as sovereignty, non-intervention, and international cooperation have become the basis for dealing with cybercrime, their implementation still faces many obstacles. Therefore, this study is important to examine how the application of international legal principles in handling cybercrime, identify the challenges faced and formulate strategies that can increase the effectiveness of law enforcement. By strengthening international cooperation, harmonization of regulations, and strengthening state capacity in dealing with cyber threats, this study is expected to contribute to building a legal system that is more responsive to the dynamics of transnational cybercrime.

METHOD

This study uses a literature study method by reviewing various relevant sources, including academic journals, books, policy documents, and reports from international organizations that focus on cyber law and global security. The approach used is a normative legal approach, which examines the application of international legal principles in handling cybercrime based on laws and regulations and international legal instruments such as the Budapest Convention. In addition, this study also applies a comparative approach to compare regulations and policies of various countries in handling transnational cybercrime so that effective patterns and challenges faced in harmonizing cyber law at the global level can be identified.

RESULT AND DISCUSSION

Principles of International Law in Handling Cybercrime

The principle of state sovereignty in international law emphasizes that every country has the exclusive right to regulate all activities within its territory, including cyberspace within its jurisdiction (Cahyadi, 2018). The application of this principle is challenging because the nature of cyberspace does not recognize territorial boundaries. Cyber attacks originating from abroad, such as hacking of government systems or data theft, often raise issues related to jurisdiction and law enforcement authority. Several countries have attempted to develop cyber regulations that affirm their sovereignty, for example by implementing rules regarding local data storage (data localization) and restricting access to foreign platforms. However, in practice, law enforcement against cybercriminals operating across countries continues to face obstacles, mainly due to differences in regulations and the lack of effective international cooperation.

The principle of non-intervention in international law prohibits a country from interfering in the domestic affairs of another country, including in cybersecurity policies (Hidayat, 2024). However, in the case of transnational cybercrime, the boundaries of this principle become unclear, especially when countries have to face threats from foreign actors, whether individuals, groups, or those supported by other countries. For example, if a cyberattack damages a country's critical infrastructure, retaliatory actions or investigative efforts that involve access to systems or data in other countries could be considered a form of intervention. In many cases, countries must balance between maintaining their cyber sovereignty and cooperating with foreign actors in efforts to mitigate global cyber threats. Therefore, there is a need for an international cooperation mechanism that can respect the principle of sovereignty but still allow for an effective response to cross-border cybercrime threats.

International cooperation is a crucial aspect of dealing with cross-border cybercrime. Because cybercriminals can operate from one country to attack systems in another state, a mechanism for cooperation between countries is needed to improve the effectiveness of law enforcement. This form of cooperation includes bilateral and multilateral agreements, where countries can collaborate in sharing cyber intelligence information, conducting joint investigations, and providing mutual legal assistance. For example, several countries have formed special task forces to deal with cyberattacks that attack critical infrastructure, such as financial systems and communication networks. Without solid cooperation, cybercriminals will find it easier to evade law enforcement by exploiting differences in jurisdiction and regulation between countries.

Several international legal instruments have been developed to strengthen global cooperation in dealing with cybercrime. One of the most significant is the Budapest Convention on Cybercrime, which is the main legal framework for dealing with transnational cybercrime. In addition, United Nations (UN) resolutions on cybersecurity and the role of international organizations such as INTERPOL and Europol also play an important role in coordinating global cyber law enforcement efforts. However, the implementation of this cooperation does not always run smoothly due to differences in the legal systems and national interests of each country. Some countries are reluctant to cooperate due to concerns about data sovereignty and the risk of information exploitation. Therefore, efforts are needed to harmonize regulations and increase trust between countries so that cooperation in effectively combat cybercrime.

The Budapest Convention, adopted by the Council of Europe in 2001, is the first international legal instrument specifically designed to address cybercrime. The background to its formation was driven by the increasing threat of cybercrime that crosses national borders and the need for legal standards that can be applied globally. The main objectives of this

Convention are to harmonize national laws on cybercrime, increase cooperation between countries in investigation and prosecution, and ensure that there is an effective mechanism for dealing with cybercriminals across jurisdictions. By providing a clear and systematic legal framework, the Budapest Convention seeks to reduce obstacles in law enforcement efforts against increasingly sophisticated and complex cybercrime.

The Budapest Convention sets out several key principles that member states must implement, including harmonization of national laws in criminalizing various forms of cybercrime, such as illegal access to computer systems, data tampering, and the distribution of malicious devices. In addition, this convention also encourages increased international cooperation through mutual legal assistance mechanisms, information exchange, and coordination in cross-border investigations. Several countries have ratified and adopted the provisions of this Convention into their domestic laws, including the United States and most European countries. However, several countries such as China and Russia have not ratified this Convention, arguing that its provisions are considered to be more beneficial to Western countries and could threaten their national legal sovereignty.

Although considered the main standard in handling transnational cybercrime, the Budapest Convention still faces various challenges in its implementation. One of the main limitations is the lack of participation from several large countries, which limits the scope of cooperation. In addition, there are differences in the interpretation of the law among member states, so the implementation of its provisions is not always consistent. Another challenge is the capacity gap between developed and developing countries in implementing the provisions of this convention effectively, especially regarding technological resources and law enforcement capabilities. Therefore, further efforts are needed to increase the effectiveness of the Budapest Convention, including encouraging more countries to join, strengthening cooperation mechanisms, and adapting regulations to increasingly dynamic technological developments.

Challenges in Law Enforcement Against Cybercrime

The capacity gap between developed and developing countries in dealing with cybercrime is mainly caused by differences in technological infrastructure and available human resources. Developed countries generally have more sophisticated cybersecurity systems, with strong digital infrastructure and law enforcement teams trained in handling cyber threats. In contrast, many developing countries still face limitations in terms of technology, funding, and a lack of experts who are competent in the cybersecurity. This makes developing countries more vulnerable to cyber attacks, whether from individuals, criminal groups, or state actors who are more technologically powerful. In addition, the legal systems in several developing countries are not fully aligned with international standards, so law enforcement against cybercrime is often less effective.

To address this gap, various strategic efforts are needed that involve international cooperation and investment in cybersecurity infrastructure. Developing countries can increase their technological capacity through training for law enforcement officers, strengthening cybersecurity policies, and cooperation with international organizations such as INTERPOL and Europol in improving cyber investigation capabilities. In addition, technical assistance and funding from developed countries or multilateral institutions can be used to establish cyber incident response centers (Computer Emergency Response Teams – CERTs) that serve as the frontline in detecting and responding to cyber threats. By investing in technology development and increasing human resource capacity, developing countries can strengthen their cyber resilience and be more effective in participating in global cooperation to address transnational cybercrime.

Differences in cyber legal regulations across countries are one of the main challenges in law enforcement efforts against transnational cybercrime. Each country has different policies and approaches to regulating cybersecurity, depending on its legal system, level of technological development, and national interests. For example, some countries apply strict regulations regarding data protection and privacy, while others are more flexible in their approach to online activities. In addition, some countries give law enforcement officers broad authority to conduct cyber surveillance, while others limit this authority to protect individual freedoms. These differences often complicate international cooperation in addressing cybercrime because not all countries have the same standards in defining, criminalizing, or enforcing the law against illegal cyber activities.

Obstacles to the harmonization of international regulations also arise due to different national interests, especially in economic, security, and geopolitical aspects. Some countries are reluctant to adjust their regulations to international standards because they are worried about losing control over their national data or strategic interests. For example, large countries such as China and Russia have different regulations from the standards applied in the Budapest Convention, so they did not join the agreement. In addition, countries with technology-based economic interests are often reluctant to share information that could hinder their digital industry. These differences make it difficult to formulate effective global policies to deal with cybercrime. Therefore, a more inclusive and flexible approach is needed in international negotiations so that cyber law regulations can be more aligned without sacrificing the interests of each country.

International cooperation in dealing with cybercrime often faces obstacles that stem from political and economic factors. A country's political interests can affect its involvement in international agreements or cooperation related to cyber law enforcement. For example, countries with strained diplomatic relations tend to be reluctant to share information or cooperate in cybercrime investigations, especially if the perpetrators are from the country concerned. Economic factors also play a role in determining nation can contribute to international cooperation. Countries with limited resources may not have the technological infrastructure to support cross-border investigations or adhere to international standards in conventions such as the Budapest Convention. Additionally, some countries view certain cyber activities, such as economic espionage and cyberwarfare, as part of their national strategy, and are therefore unwilling to fully participate in stricter international regulations.

Extradition and jurisdictional issues are also major obstacles to international cooperation on cybercrime. Cybercrime often involves perpetrators operating from other countries, but their home countries may not have extradition treaties with the victim country. It makes it difficult to prosecute cybercriminals because the host country may not consider the act a crime or may have different rules regarding extradition. In addition, differences in jurisdictional principles also complicate international cooperation. Some countries adopt jurisdiction based on the location of the victim, while others enforce the law based on the location of the perpetrator. As a result, governments often experience a deadlock in processing cross-border cybercrime cases because there is no legal mechanism uniform to deal with these jurisdictional differences. Therefore, further efforts are needed to develop more effective extradition treaties and law enforcement mechanisms at the international level.

Efforts to Increase the Effectiveness of Cyber Law Enforcement

Bilateral and multilateral cooperation are the main strategies for increasing the effectiveness of cyber law enforcement at the international level. Countries can strengthen bilateral relations through cooperation agreements in the exchange of cyber intelligence information, joint investigations, and mutual legal assistance mechanisms. On the other hand, multilateral cooperation, such as the Budapest Convention, allows countries to adopt the

same legal standards in dealing with cybercrime. This harmonization of legal policies is important to overcome the challenges of cross-country jurisdiction so that the investigation and prosecution process against cybercriminals can run more effectively.

In addition to agreements between countries, international organizations also have an important role in strengthening global cooperation in cybersecurity. Organizations such as Interpol, Europol, and the United Nations (UN) serve as coordinating bodies in dealing with transnational cybercrime. They assist in formulating global policies, providing training for developing countries, and facilitating the exchange of information related to developing cyber threats. The existence of these organizations allows countries with different legal systems to continue to work together to prevent and handle cybercrime in a more coordinated manner.

Investing in cybersecurity technology development is a crucial step in increasing the effectiveness of cyber law enforcement. Countries need to allocate greater resources to build strong cyber defense systems, such as advanced firewalls, cyber attack detection systems, and artificial intelligence to analyze threats in real-time. In addition, strengthening digital infrastructure must also include better data protection mechanisms so that sensitive information is not easily hacked by cybercriminals. With adequate investment, countries can increase resilience to cyber-attacks and accelerate identifying and handling criminals.

Increasing human resource capacity is also a major factor in the effectiveness of cyber law enforcement. Law enforcement officers, such as cyber police and prosecutors, must receive intensive training on cyber investigation methods, digital forensics, and an in-depth understanding of international cyber law regulations. Developing countries that still have limited resources can collaborate with developed countries or international organizations to get assistance in the form of training and technology transfer. By having competent experts, the law enforcement process against cybercrime can run more effectively and efficiently.

Collaboration between the government and the private sector is one of the keys to improving cybersecurity. Many companies, especially those engaged in technology and banking, have sophisticated cybersecurity systems and important data related to cyber threats. Therefore, cooperation in the form of sharing cyber threat information, preventing cyber attacks, and preparing more effective cybersecurity regulations are steps that need to be strengthened. The government can collaborate with private companies to build a cybersecurity incident response center (CSIRT) to coordinate actions to handle cyber attacks more quickly and in a structured manner.

Technology companies also have a significant role in supporting cybersecurity policies. Digital service providers, such as Google, Microsoft, and Facebook, can contribute by developing more secure encryption technology, stricter authentication systems, and transparency policies in handling cyber threats. In addition, the private sector can also work with the government in educating their citizens regarding cyber threats and how to protect their personal data from cyber-attacks. With synergy between the government and the private sector, the cyber security system can become more resilient in facing increasingly complex threats.

CONCLUSION

In dealing with increasingly complex and cross-border cybercrime, a comprehensive law enforcement strategy is needed to balance the principles of state sovereignty, international cooperation, and the use of existing legal instruments, such as the Budapest Convention. The main challenges in cyber law enforcement lie in the differences in regulations between countries, the gap in technological capacity, and limitations in global cooperation mechanisms. Therefore, efforts to strengthen bilateral and multilateral cooperation, increase the capacity of cybersecurity technology and infrastructure, and collaborate with the private sector are strategic steps that must continue to be developed. By

harmonizing regulations and increasing trust between countries, the effectiveness of cyber law enforcement can be increased to face the growing threats in the digital era.

The capacity gap between developed and developing countries in dealing with cybercrime is mainly caused by differences in technological infrastructure, human resources, and legal regulations that are not yet uniform. Developing countries still face limitations in terms of technology and funding, while different cyber law regulations in each country are a challenge to international cooperation. In addition, political and economic factors often hinder coordination between countries in dealing with transnational cybercrime, including in the aspects of extradition and jurisdiction. Therefore, a strategic approach is needed through increased investment in cybersecurity infrastructure, training of experts, and harmonization of more inclusive and flexible international legal regulations so that global cooperation in dealing with cyber threats can be more effective.

Cyberlaw enforcement at the international level depends on bilateral and multilateral cooperation, investment in security technology, increasing human resource capacity, and synergy between governments and the private sector. Harmonization of regulations through international agreements and the involvement of global organizations such as Interpol and Europol is essential in overcoming jurisdictional challenges and accelerating cross-border cybercrime investigations. In addition, strengthening digital infrastructure and developing sophisticated security technologies must be supported by training law enforcement officers to be better prepared to face increasingly complex cyber threats. The private sector also plays a role in providing better security systems and sharing cyber threat information with governments. With an integrated strategy, countries can improve their cyber resilience and strengthen law enforcement efforts against cybercrime globally.

REFERENCES

Ardianto, R. (2024). Transformasi digital dan antisipasi perubahan ekonomi global dalam dunia perbankan. *MARAS: Jurnal Penelitian Multidisiplin*, 80-88.

Arifah, D. A. (2011). Kasus cybercrime di indonesia. *jurnal Bisnis dan Ekonomi* .

Bainus, A. (2023). Hubungan Internasional Digital (Digital International Relations). *Intermestic: Journal of International Studies*, 1-18.

Budiyanto. (2025). *Pengantar Cybercrime dalam Sistem Hukum Pidana di Indonesia.* Banten: Sada Kurnia Pustaka.

Cahyadi, I. (2018). Tata kelola dunia maya dan ancaman kedaulatan nasional. *Jurnal Politica Dinamika Masalah Politik Dalam Negeri dan Hubungan Internasiona*.

Hidayat, K. S. (2024). Efektivitas Peran ASEAN Dalam Penanganan Kudeta Myanmar Tahun 2021. *Journal of Global Perspective*, 72-84.

Hindarwati, E. N. (2024). *Inovasi Bisnis: Membangun Keunggulan Bersaing di Era Digital.* Yogyakarta: Green Pustaka Indonesia.

Iskandar, B. (2021). Kebijakan Formulasi Hukum Pidana Tentang Penanggulangan Tindak Pidana Terorisme Siber (Cyber Terorism) Di Indonesia. *Jurnal Hukum Ius Publicum* , 119-138.

Mudjiyanto, B. (2024). endensi politik kejahatan dunia maya. *JIKA (Jurnal Ilmu Komunikasi Andalan)*, 26-51.

Pakarti, M. H. (2023). Pengaruh Perkembangan Teknologi Terhadap Perlindungan Privasi Dalam Hukum Perdata. *SULTAN ADAM: Jurnal Hukum dan Sosial* , 204-212.

Pangestika, E. Q. (2024). Penerapan Prinsip Hukum Internasional Dalam Penegakan Hukum Terhadap Kejahatan Siber Dan Serangan Siber. *Jurnal Review Pendidikan dan Pengajaran (JRPP)*, 5782-5788.

Pangestika, E. Q. (2024). Penerapan Prinsip Hukum Internasional Dalam Penegakan Hukum Terhadap Kejahatan Siber Dan Serangan Siber. *Jurnal Review Pendidikan dan Pengajaran (JRPP)*, 5782-5788.

Rahmawati, I. (2017). Analisis manajemen risiko ancaman kejahatan siber (cyber crime) dalam peningkatan cyber defense. *Jurnal Pertahanan dan Bela Negara*, 35-50.

Saramuke, S. S. (2025). Ancaman Keamanan Siber dan Peran Aktor Non-Negara di Dunia Digital. *Syntax Idea*, 141-152.

Sarjito, A. (2024). *Geodefense Konsep Pertahanan Masa Depan.* Bandung: Indonesia Emas Group.

Tobing, C. I. (2024). "Globalisasi Digital Dan Cybercrime: Tantangan Hukum Dalam Menghadapi Kejahatan Siber Lintas Batas. *Jurnal Hukum Sasana*, 105-123.

Wahyuningsih, S. E. (2016). Kebijakan Penegakan Hukum Pidana Terhadap Penanggulangan Money Laundering Dalam Rangka Pembaharuan Hukum Pidana Di Indonesia. *Jurnal Pembaharuan Hukum*, 46-56.

Wangke, H. (2021). *Diplomasi digital dan kebijakan luar negeri Indonesia.* Jakarta: Yayasan Pustaka Obor Indonesia.

Wati, D. S. (2024). Dampak Cyber Crime Terhadap Keamanan Nasional dan Strategi Penanggulangannya: Ditinjau Dari Penegakan Hukum. *Jurnal Bevinding* , 44-55.