Sortuz. Oñati Journal of Emergent Socio-legal Studies
Volume 16, Issue 1 (2026), 70-88
ISSN 1988-0847
DOI link: https://doi.org/10.35295/sz.iisl.2411

Enforcement of the universality principle in combating cybercrime as a transnational crime

Sahat Maruli Tua Situmeang[1]
Elvina Rahma Kamilia[2]
Nurul Lutfiyah[3]
Dinda Marshanda Aurora[4]

Abstract:

Cybercrime, as a borderless, technologically advanced transnational threat exemplified by ransomware and cross-border intrusions, challenges territorially bound criminal jurisdiction. This article investigates whether universal jurisdiction applies to cybercrime under current international law and evaluates the Budapest Convention's role in jurisdictional challenges. Using normative juridical methods with doctrinal and comparative approaches, it analyzes international instruments, criminal law principles, and scholarly views. Findings reveal cybercrime lacks universal jurisdiction status in positive law; the Budapest Convention promotes territorial and extraterritorial jurisdiction via domestic law harmonization and cooperation, not universality. Conflating universal and extraterritorial jurisdiction breeds doctrinal confusion and uncertainty. The study advocates clearer distinctions between these bases to bolster legal certainty and aid enforcement against transnational cybercrime.

Keywords:

Combating, cybercrime, enforcement, transnational crime, universality principle.

[1] Sahat Maruli Tua Situmeang, Universitas Komputer Indonesia, Jl. Dipatiukur No. 112-114 Bandung, Email: sahat@email.unikom.ac.id ORCID 0009-0003-6893-3958
[2] Elvina Rahma Kamilia, Universitas Komputer Indonesia, Jl. Dipatiukur No. 112-114 Bandung. Email: elvina.31622019@mahasiswa.unikom.ac.id
[3] Nurul Lutfiyah, Universitas Komputer Indonesia, Jl. Dipatiukur No. 112-114 Bandung. Email: nurul.31622027@mahasiswa.unikom.ac.id
[4] Dinda Marshanda Aurora, Universitas Komputer Indonesia, Jl. Dipatiukur No. 112-114 Bandung. Email: dinda.31622002@mahasiswa.unikom.ac.id

Resumen:

La ciberdelincuencia, como amenaza transnacional sin fronteras y tecnológicamente avanzada como ejemplifican el ransomware y las intrusiones transfronterizas, pone a prueba la jurisdicción penal, limitada territorialmente. Este artículo investiga si la jurisdicción universal se aplica a la ciberdelincuencia en el marco del derecho internacional vigente y evalúa el papel del Convenio de Budapest en los retos jurisdiccionales. Mediante métodos jurídicos normativos con enfoques doctrinales y comparativos, analiza los instrumentos internacionales, los principios del derecho penal y las opiniones académicas. Los resultados revelan que la ciberdelincuencia carece de estatus de jurisdicción universal en el derecho positivo; el Convenio de Budapest promueve la jurisdicción territorial y extraterritorial a través de la armonización del derecho interno y la cooperación, no de la universalidad. La confusión entre la jurisdicción universal y la extraterritorial genera confusión doctrinal e incertidumbre. El estudio aboga por distinciones más claras entre estas bases para reforzar la seguridad jurídica y facilitar la lucha contra la ciberdelincuencia transnacional.

Palabras clave:

Lucha contra la delincuencia, ciberdelincuencia, aplicación de la ley, delincuencia transnacional, principio de universalidad.

TABLE OF CONTENTS

1. INTRODUCTION

The exponential growth of digital technologies has fundamentally transformed social, economic, and political interactions across borders. Alongside these developments, cybercrime has emerged as one of the most pervasive and disruptive forms of transnational crime. According to the Internet Crime Complaint Center (IC3) of the Federal Bureau of Investigation, global losses caused by cybercrime reached billions of US dollars annually, affecting individuals, corporations, and state institutions alike.

Ransomware attacks such as *WannaCry* (Siregar and Sinaga 2021). and large-scale cyber intrusions exemplified by the *SolarWinds* (Zhou *et al.* 2024). incident demonstrate that cybercrime is no longer limited to isolated criminal acts but constitutes a systemic threat to national security, (Parulian *et al.* 2021). economic stability, and public trust in digital infrastructures. (Sviatun *et al.* 2021).

The transboundary nature of cybercrime poses a profound challenge to the traditional architecture of criminal jurisdiction, which has historically been anchored in territorial sovereignty. Cyber offences are frequently committed remotely, anonymously, and simultaneously across multiple jurisdictions, often without the physical presence of perpetrators in the affected states. (Al-Amaireh 2024).

As a result, territorial jurisdiction—the cornerstone of classical criminal law has become increasingly inadequate as a sole basis for law enforcement in cyberspace. This jurisdictional gap has prompted states to rely more heavily on extraterritorial jurisdiction and international cooperation mechanisms, while also reigniting scholarly debate on the potential applicability of universal jurisdiction to cybercrime.

In international criminal law, universal jurisdiction constitutes an exceptional principle that allows states to prosecute certain crimes regardless of the location of the offence or the nationality of the offender or victim. Traditionally, this principle has been reserved for crimes considered to offend the international community as a whole, such as genocide, crimes against humanity, war crimes, and piracy. Nevertheless, the severe global impact of cybercrime has led some scholars to argue that cyber offences may justify an expansion of universal jurisdiction beyond its classical scope. This argument, however, remains highly contested and has not been conclusively grounded in positive international law.

Within this context, the Budapest Convention on Cybercrime (2001) is frequently cited as the most significant international legal instrument addressing cybercrime. While the Convention aims to harmonise substantive criminal law and enhance cross-border cooperation, its precise implications for jurisdictional authority are often misunderstood. In particular, some interpretations erroneously suggest that the Budapest Convention implicitly authorises the exercise of universal jurisdiction over cybercrime. Such claims risk generating doctrinal confusion and legal uncertainty, especially for law enforcement authorities tasked with prosecuting transnational cyber offences.

Against this background, this article critically examines the relationship between cybercrime, universal jurisdiction, and extraterritorial jurisdiction under contemporary international law. It argues that cybercrime has not attained the status of an offence subject to universal jurisdiction under existing legal frameworks. Furthermore, this study contends that the Budapest Convention does not establish universal jurisdiction but instead reinforces territorial and extraterritorial jurisdiction through harmonisation of domestic laws and structured international cooperation mechanisms. Accordingly, the central research question of this article is formulated as follows: under what circumstances, if any, can universal jurisdiction be applied to cybercrime, and how does it differ from extraterritorial jurisdiction as regulated under the Budapest Convention?

2. LITERATURE REVIEW

2.1. HISTORY AND CONCEPT OF THE UNIVERSALITY PRINCIPLE

The universality principle originates from international law, allowing states to prosecute certain crimes regardless of where they occur or the nationality of the perpetrators. Historically, this principle was first applied to piracy on the high seas. Pirates were deemed "enemies of all mankind," justifying prosecution by any nation. Over time, the principle expanded to cover war crimes, genocide, terrorism, and, more recently, cybercrime. With globalization and technological advancements, cybercrime has become a significant transnational threat. Criminals can exploit digital vulnerabilities to conduct large-scale attacks, such as ransomware incidents and data breaches. Hacking activities can include the use of hardware or improperly implemented software to obtain passwords illegally and gain unauthorized access to a computer system (Andini 2021). Given the global impact of such crimes, the universality principle provides a legal framework for prosecuting cybercriminals, regardless of their location.

However, applying the universality principle to cyberspace presents challenges, including differences in national cybersecurity regulations. Some countries lack robust cyber laws, while others prioritize digital privacy and freedom, leading to jurisdictional conflicts. Furthermore, developing nations often struggle with weak cybersecurity infrastructure and limited law enforcement capabilities. These issues are further complicated by the fact that states express broad and diverse demands in defining 'cybercrime', which generally falls under a multiplicity of domestic legal systems that remain loosely organized (X Wang 2024).

Extending the concept of the universality principle to cyberspace is a strategic step to address global threats. This principle enables countries to prosecute cybercriminals even if the crime did not occur within their jurisdiction, provided that it has a significant impact on the international community as a whole. With the increasing global threats such as cyberattacks on critical infrastructure, large-scale data theft, and the spread of malware, the application of the universality principle in cyberspace is becoming increasingly urgent. For example, the WannaCry ransomware attack in 2017, which affected more than 150 countries, demonstrated that cybercrimes can simultaneously impact multiple countries. In cases like this, the application of the universality principle can provide a legal basis for countries to cooperate in apprehending and prosecuting perpetrators, regardless of their location. This underscores the importance of international collaboration governed by

global legal instruments, such as the Budapest Convention on Cybercrime, which aims to harmonize laws and improve investigative techniques to combat cybercrime globally (Ramayanti and Lubis 2023).

Before the internet, criminals had to be physically present to commit a crime. However, the internet changed everything. It connected servers and storage devices, allowing cybercriminals to access, steal, or change data from anywhere in the world (Bunga 2019). The Cybercrime Convention defines service providers in two ways: first, any public or private entity that enables users to communicate through a computer system; second, any entity that processes or stores data for these communication services or users. Traffic data refers to any computer data related to communication through a computer system (Wicki-Birchler 2020).

The Budapest Convention stands as the first global treaty dedicated to international cooperation against cybercrime. Its primary aim is to tackle such offenses by aligning national laws through a unified legal strategy across nations (Iqbal and Beigh 2017). Cybercriminals can exploit these specific security gaps if operating systems or software are not consistently updated, making the need for coordinated efforts even more urgent (Milon *et al.* 2024). Furthermore, it promotes the creation of effective legal frameworks and the advancement of investigative methods to enhance cross-border cooperation and protect the global community from cyber threats.

Data breaches frequently occur due to malware or fraudulent activities. Criminals want to get personal or company data for many reasons. Sometimes, they want secret information. At other times, they sell the data or use it to solicit money. Stolen data can also be used to steal more money. Most of these crimes are committed for financial gain (Świątkowska 2020). This highlights the importance of clear laws and regulations. Countries have the right to make and enforce laws. This is called jurisdiction. A country can apply its laws to people, things, and events, even outside its borders (Aryudhanty *et al.* 2023).

Ensuring the integrity and protection of digital evidence requires meticulous sealing and careful handling to prevent any form of damage or tampering (Azam *et al.* 2023). This is particularly important because all economic activities that are carried out without a strong legal basis are highly vulnerable to various issues. When such problems arise, especially involving compromised evidence, they can lead to significant financial losses due to legal disputes, prolonged investigations, and reputational damage (Shevchenko *et al.* 2021). One of the practices of data counterfeiting, for example, is the falsification of documents on e-commerce sites, made to appear as mere typos or mistyped entries, which ultimately benefits the perpetrator and further complicates the legal process (Umanailo *et al.* 2019). The presence of risk factors among cyber offenders was commonly linked to a history of criminal behavior and instability in a family or marital circumstances (Bossler and Berenblum 2019).

The more sensitive the stolen information, the more money criminals can make. This encourages them to take advantage of weak laws (Gupta and Mata-Toledo 2016). A major challenge in combating cybercrime is the existence of 'safe havens' in countries where criminals can operate to evade prosecution. These safe havens primarily exist in countries that lack robust laws against cybercrime. As a result, criminals often choose to operate from

those countries to escape punishment. This makes it challenging to stop serious crimes that affect people worldwide.

However, extending the universality principle to cyberspace presents challenges. One of the primary obstacles is the disparity in cyber regulations across different countries. Some countries lack adequate regulations to address cybercrime, while others employ different approaches to privacy and internet freedom. This lack of harmony can hinder the application of the universality principle, especially when a country is reluctant to cooperate due to policy differences or political reasons. Additionally, applying the universality principle in cyberspace requires enhanced technical capacity and resources in developing countries. These countries often become primary targets or transit points for cybercrime due to weak cyberinfrastructure and limited law enforcement capabilities in handling complex cases.

All nations should continuously improve their national legislation and support the reinforcement of the rule of law in global cyberspace governance. It is essential to uphold the authority of international law and reject the application of double standards. Domestically, in exercising cyber sovereignty, states must safeguard the lawful rights and interests of their citizens, legal entities, and other organizations operating in cyberspace. Internationally, they must respect the cyber sovereignty of other nations and comply with international legal norms. No country should misuse the internet to interfere in another nation's internal affairs or participate in, support, or promote cyber activities that threaten the national security of other states. Additionally, firm action should be taken forward against the perpetrators of cyber hate targeting the armed forces if their actions result in harm to or the reduction of military reputation (M. I. Ali 2024).

States must refrain from conducting cyber operations that infringe upon the sovereignty of other nations (Schmitt and Vihul 2017). One of the most pressing challenges in cyberspace governance today lies in maintaining cyber sovereignty and ensuring cybersecurity, both of which inherently demands international collaboration (G. Wang 2021). Given the complex and borderless nature of cyberspace, particularly in identifying the actual location of cyber activity, there has been a growing shift toward objective territoriality over subjective territoriality. For instance, the European Union has adopted objective territoriality and complementary jurisdictional principles in its data protection framework (Benthem *et al.* 2024). Nonetheless, cyber operations are still being utilized by certain states to fulfill strategic or political interests. A notable example is the PRISM program implemented by the United States' National Security Agency (NSA), as disclosed by Edward Snowden. This classified initiative, which collected foreign communications data via American servers, was widely condemned for violating the sovereignty of other countries, including long-standing allies of the U.S. Such incidents underscore the urgent need to reinforce the principle of universality in cyberspace governance and ensure respect for international law and state sovereignty (Zhu and Chen 2023).

2.2. RELEVANCE OF THE UNIVERSALITY PRINCIPLE TO CYBERCRIME

The universality principle provides a legal framework that enables countries to enforce laws against perpetrators of serious crimes with a global impact, including cybercrime, even if the perpetrators are located in a jurisdiction other than their own. This principle is based on the idea that there are certain crimes so severe that the international community has a

shared interest in prosecuting the perpetrators. In the context of cybercrime, the universality principle becomes important because the cross-border nature of these crimes often complicates law enforcement efforts based on traditional jurisdictional boundaries. By applying the universality principle, countries can pursue cybercriminals who attack critical infrastructure or steal personal data.

To apply the principle of universality effectively, it is crucial to understand how cybercrime has evolved and how the legal framework has responded to this evolution. Analysis of the development of cybercrime reveals that hackers continue to exploit weaknesses in increasingly advanced technologies, while legal and policy measures tend to lag and respond to circumstances. Due to this imbalance, it is essential to strengthen the international legal system, such as the principle of universality, to close the gaps that transnational criminals often exploit. Therefore, this analysis provides a crucial foundation for understanding the challenges associated with jurisdictional implications and the difficulties faced by the judicial system in addressing cybercrime (Allahrakha 2024).

The increasing number of cybercrimes committed online is jeopardizing the integrity of the criminal justice system. Perpetrators of these crimes easily exploit the internet as a haven, especially since these crimes extend beyond national borders. Due to the many laws applicable to cybercrimes, this raises procedural and objective issues. The wide-ranging results and losses of cybercrimes pose significant challenges to the perpetrators themselves. The question of whether the perpetrators have multiple nationalities when committing these crimes arises. Criminals may commit an offense in a country that prohibits it within its jurisdiction. However, because they hold the nationality of another country, they are also liable for punishment under the principle of personal jurisdiction (Magableh and Al-Shawabkeh 2024).

The application of the universality principle to cybercriminals is supported by international frameworks such as the Budapest Convention on Cybercrime. This instrument encourages countries to expand their jurisdiction and enhance cooperation in investigations and prosecutions. For example, large-scale ransomware attacks often involve perpetrators operating from different jurisdictions. With the universality principle, victim countries can collaborate to bring the perpetrators to justice, even if they are hiding in a country that does not have an extradition treaty with the victim's country. This demonstrates how the universality principle can close legal gaps in addressing cross-border crimes.

The application of the universality principle in the context of cybercrime must consider its impact on human rights. It is essential to ensure that law enforcement efforts do not infringe upon individuals' rights to privacy or freedom of expression. A transparent approach based on international law can help create a balance between global security and respect for human rights. Thus, the universality principle serves not only as a legal tool but also as a mechanism to achieve global justice in the digital age.

The universality principle provides a framework that can be applied to various types of cybercrimes with cross-border impacts and significant implications for the international community. Attacks like this illustrate the complexity and cross-border nature of cybercrime, highlighting the importance of the principle of universality (Malik *et al.* 2022). A concrete example of this type is the WannaCry ransomware attack that occurred in 2017 (Qudus 2025). This attack affected more than 150 countries and infected hundreds of

thousands of computers worldwide, including healthcare systems, large corporations, and government institutions. The attack spreads through system security gaps, especially on devices that have not been updated, and through phishing email attacks, which increases the reach of the attack (Faquir *et al.* 2021). The perpetrators of the attack exploited software vulnerabilities to encrypt the victims' data and demand a ransom in the form of cryptocurrency. With such a wide-ranging impact, the Wannacry attack is one of the cybercrimes that is relevant to address through the universality principle.

The global WannaCry cyberattack highlighted the complexities of coordination in incident response, particularly as many organizations lack robust cybersecurity practices and are slow to apply available patches. WannaCry demonstrated the importance of international cooperation in the face of increasingly complex and cross-border ransomware threats. Furthermore, the scale of the attack demonstrated the importance of coordinated incident response at the international level. It highlighted broader policy implications, such as the need for proactive vulnerability management and mandatory reporting of cybersecurity incidents. Policymakers are beginning to consider legal reforms such as stricter data protection regulations and mandatory cybersecurity standards, especially for critical infrastructure sectors.

The Wannacry case demonstrates how cybercrime can cause global harm and involve perpetrators operating from various jurisdictions. In this case, the affected countries can collaborate to identify and prosecute the perpetrators using the universality principle. Although the perpetrators are physically located in a specific country, the widespread impact of the crime makes it a threat to the international community. The application of the universality principle allows countries to overcome jurisdictional barriers that often pose significant challenges in addressing cross-border cybercrime. This also highlights that jurisdictional challenges continue to be a significant obstacle to law enforcement efforts against transnational cybercrime (Syaakirah *et al.* 2025).

2.3. IMPLEMENTATION OF THE UNIVERSALITY PRINCIPLE IN INTERNATIONAL CONVENTIONS

This principle establishes that the country with the closest connection to the crime should have priority in prosecuting international crimes. The rapid development of cybercrime is increasingly challenging the application of the jurisdictional principle, which prioritizes the closeness of the state's relationship with the crime (Orlovskyi *et al.* 2023). The territorial principle, the nationality principle, and the protective principle should be prioritized before other countries can exercise universal jurisdiction (Putri 2022). The jurisdiction of a state refers to the power or authority of a country to declare and enforce the laws created by that state or nation itself (Pratiwi 2019). As cyberspace continues to develop as a fertile ground for criminal activity, the legal landscape is grappling with a variety of challenges, necessitating a careful review of contemporary issues in the criminal justice system (Amoo *et al.* 2024).

The implementation of the universality principle in international law emphasizes the importance of establishing jurisdiction to prosecute international crimes in countries that have the closest connection to the crime. This reflects the need to maintain a balance between a country's jurisdiction and the principle of international cooperation. Before applying universal jurisdiction, priority should be given to the principles of territoriality,

nationality, and protection. In this way, countries that have a direct connection to the crime are prioritized to exercise their judicial authority. However, no country is willing or able to do so. In that case, the principle of universality provides an opportunity for other countries with related interests to take legal action against the perpetrators of international crimes. This complexity highlights the need to apply the principle of universality in addressing jurisdictional challenges during the investigation and prosecution of transnational cybercrimes (Arifi and Arifi 2020).

One example of the application of the universality principle in the context of transnational crime is the 2001 Budapest Convention on Cybercrime. This convention provides an international legal framework for addressing crimes involving information and communication technology, which are often transnational in nature. This convention is a crucial foundation because it is the first international legal instrument to regulate the use and transmission of data through information systems, in line with the need to address cross-border cybercrime. Technological developments have encouraged the integration of information and telecommunications, which ultimately increases the risk of misuse. Therefore, the term "computer crime" then evolved into "cybercrime" to reflect the scope of more complex and global crimes (Horovic *et al.* 2021). Although the principles of territoriality, nationality, and protection remain the primary foundations of law enforcement, the Budapest Convention also permits countries to exercise universal jurisdiction over cybercrimes, even if they have no direct connection to the criminal act in question. The Convention establishes specific procedures for the collection of electronic evidence. Given the transnational nature of cybercrime, regulations for expeditious international cooperation are needed. The protection of rights and freedoms, as well as cybersecurity, are other topics covered in the convention (Abaje 2024).

The convention on cybercrime, ratified in 2001, can serve as an alternative to resolving dilemmas in legal regulations, particularly concerning internet criminalization policies. As part of an international effort, the agreement has garnered support from 49 countries, including Canada, the US, and Japan, signaling an early commitment to a global approach (Natsag *et al.* 2025). However, over time, several issues have emerged regarding the acceptance of this convention within the international community. One of the main problems is the fact that this convention was established within a regional context, leading many countries to exhibit resistance or rejection toward the norms, regulations, legal infrastructure, and legal products developed within a regional framework in which they are not members (Kurnia, n.d.). Despite challenges to its adoption, the Budapest Convention has helped guide domestic legislation worldwide in response to the growing need for comprehensive cyber regulation (Bracco 2022). The need for cross-border collaboration is becoming increasingly urgent as the transnational nature of cybercrime knows no jurisdictional boundaries (Kumar 2024).

This convention offers an international legal framework that supports intergovernmental cooperation in addressing cybercrimes, which are often transnational in nature. By emphasizing the universality principle, this convention provides countries with the opportunity to exercise universal jurisdiction over cybercrimes, even in cases where there is no direct connection to the perpetrators or the criminal acts. This framework emphasizes the importance of international collaboration, encompassing information exchange, mutual legal assistance, and the harmonization of national policies in collectively combating global cyber threats.

The purpose of the convention is to enhance national laws, establish investigative procedures, and foster international cooperation. Key provisions include criminalizing computer-related offenses such as unauthorized access, data interference, and computer fraud. Although the Budapest Convention is a significant document, it has some shortcomings. Non-member countries especially face these issues. China and Russia have not adopted the convention because they are concerned about data sovereignty and jurisdictional authority. Despite its limitations, the Budapest Convention promotes international cooperation and serves as a model for global cyber law (J. Ali 2024).

3. METHODOLOGY

This research employs a normative juridical method, analyzing secondary data from primary legal sources, such as the Criminal Code (KUHP), Law No. 19 of 2016 on Amendments to Law No. 11 of 2008 on Electronic Information and Transactions (UU ITE) and Law Number 1 of 2024 concerning the Second Amendment to Law Number 11 of 2008 on Electronic Information and Transactions (UU ITE).

4. DISCUSSION

Transnational cybercrime is a global threat that is becoming increasingly complex with the advancement of information and communication technology. This type of crime crosses national borders, affecting perpetrators, victims, and its overall impact. The transnational, hidden and universal character of cybercrime demonstrates the importance of applying the principle of universality to foster practical international cooperation (Wong 2024). In addressing this challenge, the application of the universality principle is a highly relevant approach. The universality principle allows countries to claim jurisdiction over certain crimes that are recognized as serious threats to the international community, regardless of the location of the crime or the nationality of the perpetrator and victim. Thus, this principle provides a comprehensive framework for tackling transnational cybercrime.

The application of the universality principle in the context of transnational cybercrime is based on the idea that certain crimes, such as cyberterrorism, attacks on critical infrastructure, and the mass exploitation of personal data, pose a threat to the common interests of humanity. This is also reflected in Indonesia's cybersecurity strategy, which emphasizes the importance of integrated response, capacity building, and international cooperation in addressing complex cyber threats (Komalasari and Mustafa 2023). In this context, every country is considered to have a responsibility to prosecute and punish the perpetrators of such crimes, regardless of whether the offender or the victim is a citizen of that country. This aligns with the spirit of international cooperation in maintaining global stability and security.

The implementation of the universality principle in international law faces various challenges, particularly those related to jurisdiction and state sovereignty. This encourages countries to strengthen their cyber capabilities in the face of increasingly complex threats (Viganò *et al.* 2020). This principle allows states to prosecute international crimes, such as war crimes and terrorism, even if they have no direct connection to the offense. However, this often leads to tensions between the involved countries. One of the main challenges in

implementing this principle is finding a balance between a state's authority to prosecute crimes committed outside its territory and the rights of other states to maintain their sovereignty and enforce their laws. Additionally, there are differences in perspectives regarding which types of crimes fall under the universality principle and how countries can collaborate in law enforcement without disrupting international relations.

To apply the principle of universal jurisdiction, a country must meet several requirements. First, the country must have provisions in its national law that allow it to prosecute perpetrators of international crimes. Second, the act committed must be classified as an international crime. If a country lacks laws regulating the prosecution of international crimes, it cannot exercise the rights granted by international law to prosecute offenders (Pratiwi 2019).

Universal jurisdiction arises from the need for a collective response to the most serious international crimes. However, its implementation often clashes with the principle of state sovereignty. The international community should have a shared commitment to addressing crimes with significant global impacts. However, the international response to universal jurisdiction has been lukewarm, as it raises concerns about the dominance of powerful nations, which could use it as a pretext to intervene in the sovereignty of other states (Kurnia n.d.).

As cybercrime frequently transcends national boundaries, international cooperation becomes indispensable. However, differences in regulations and laws between countries can hinder effective law enforcement (Mustam 2023). All countries, without exception, can claim and assert jurisdiction based on the principle of universality. In this context, jurisdictional competition among various nations with vested interests is often unavoidable. This competition involves the country where the crime occurred, the country of the victim, and the country where the perpetrator is located or has fled. To claim and establish jurisdiction over such offenses, the relevant countries should have developed national legal regulations that can be effectively used to address these cases.

The lack of international cooperation is a significant challenge in combating cybercrime. Given its cross-border nature, cybercrime often spans multiple jurisdictions, making it challenging to address effectively. Disparities in national legal systems, regulatory differences, and limitations in collaboration mechanisms create significant obstacles in tackling this threat. Therefore, governments, law enforcement agencies, and international organizations must collaborate in developing a stronger global legal framework. Additionally, proactive measures, such as enhancing cybersecurity, strengthening law enforcement capacity, and promoting intergovernmental collaboration, are crucial to effectively addressing these challenges and ensuring more effective law enforcement in the digital world (Laksana and Mulyani 2024).

In 2017, the WannaCry ransomware attack became one of the worst cybercrime incidents in the world. The virus spread to over 200 countries, including Indonesia, and infected approximately 300,000 computers. Its impact was severe, particularly on Indonesia's medical system, forcing hospitals and healthcare workers to operate offline. WannaCry also involved individuals from multiple countries, making international cooperation essential in the law enforcement process to track down and prosecute those responsible (Kurniawan *et al.* 2021). WannaCry encrypted data and demanded ransom to unlock infected files,

causing estimated losses in the billions of dollars. An analysis based on the universality principle can be utilized to prosecute the perpetrators, considering the transnational impact and the serious violations of global interests it caused. The affected countries can take action to prosecute the perpetrators under the principle of universal jurisdiction.

SolarWinds: The SolarWinds attack began in 2019 and utilized key tools and techniques commonly used by hackers to carry out the attack successfully. Approximately 18,000 users were affected by the SolarWinds supply chain attack, posing a significant risk of sensitive and personal data breaches by employees (Kruti *et al.* 2023).

This attack was carried out using the Supply Chain Attack method, in which an IT infrastructure provider was targeted, subsequently affecting numerous organizations. A software supply chain attack occurs when hackers infiltrate the code in a third-party software component, thereby compromising the applications that rely on it (Martínez and Durán 2021). In this context, SolarWinds, a company that provides network management and Orion monitoring solutions, became the primary target. By applying the universality principle, affected countries can collaborate to identify the perpetrators and formulate a legal enforcement framework based on this principle. The universality principle grants any country the authority to prosecute the perpetrators, regardless of where the crime occurred or the nationality of the offenders, as long as there is international consensus to collaborate.

In both situations, efforts to capture and prosecute the perpetrators require strong international collaboration through mechanisms such as Interpol and other global forums. Affected countries must share intelligence data related to attack techniques and the perpetrators' digital footprints, which will facilitate the identification of the perpetrators. Additionally, it is crucial to strengthen the international legal framework that supports universal jurisdiction over cybercrime to close legal loopholes that criminals might exploit. Specialized training for law enforcement officials is also necessary to ensure they fully understand cross-border cybercrime, enabling them to effectively address threats and promote joint action in global law enforcement. The increasing number of cyber threats demands strengthening international cooperation, harmonizing legal frameworks, and enhancing law enforcement capacity, so that the principle of universality can be applied effectively in prosecuting transnational cybercriminals (Kausar *et al.* 2023).

The universality principle provides a legal basis for countries to prosecute cyber criminals, irrespective of jurisdictional limitations. However, its implementation faces challenges, including differences in national regulations and enforcement capacities. Strengthening international cooperation, harmonizing legal frameworks, and enhancing law enforcement capabilities are crucial to ensuring the effective prosecution of cybercrime. Furthermore, enhancing cybersecurity awareness and encouraging intergovernmental collaboration can reinforce the application of the universality principle in addressing transnational cybercrime. The application of the universality principle can also be extended to specific cybercrimes, such as ransomware attacks, whose impacts cross borders and require a collective law enforcement approach (Connell 2023).

5. Conclusion and Recommendation

The universality principle provides a legal basis for countries to prosecute cyber criminals, irrespective of jurisdictional limitations. However, its implementation faces challenges, including differences in national regulations and enforcement capacities. Strengthening international cooperation, harmonizing legal frameworks, and enhancing law enforcement capabilities are crucial to ensuring effective prosecution of cybercrime. Furthermore, enhancing cybersecurity awareness and encouraging intergovernmental collaboration can reinforce the application of the universality principle in addressing transnational cybercrime.

References

Abaje, O. D., 2024. Globalization of computer networks: The need for accession to regional cybercrime treaties. *Wallaga University Journal of Law* [online], *2*(1), 56–71. Available at: https://journals.wgu.edu.et/index.php/jol/article/view/1336

Al-Amaireh, M. A.-A. M., 2024. The role of cybersecurity in enhancing the effectiveness of law against cybercrimes. *Revista de Gestao Social e Ambiental (RGSA)* [online], *18*(8), 1–18. Available at: https://doi.org/10.24857/rgsa.v18n8-124

Ali, J., 2024. Cybercrime and cybersecurity : A critical analysis of legal frameworks and enforcement mechanisms. *Bharati International Journal of Multidisciplinary Research & Development (BIJMRD)*, *2*(8), 137–154.

Ali, M. I., 2024. Protecting national honor : Advocating for legislation against cyber hate targeting Pakistan's armed forces. *Scientific Bulletin* [online], *29*(2), 189–194. Available at: https://doi.org/10.2478/bsaft-2024-0020

Allahrakha, N., 2024. Transformation of crimes (cybercrimes) in digital age. *International Journal of Law and Policy* [online], *2*(2), 1–19. Available at: https://doi.org/10.59022/ijlp.156

Amoo, O. O., *et al.*, 2024. The legal landscape of cybercrime: A review of contemporary issues in the criminal justice system. *World Journal of Advanced Research and Reviews* [online], *21*(2), 205–217. Available at: https://doi.org/10.30574/wjarr.2024.21.2.0438

Andini, O. P., 2021. Cyber terrorism criminal acts in the perspective of transnational organized crime. *Unnes Law Journal: Jurnal Hukum Universitas Negeri Semarang* [online], *7*(2), 333–346. Available at: https://journal.unnes.ac.id/journals/ulj/article/download/38698/7560/127883

Arifi, D., and Arifi, B., 2020. Cybercrime: A challenge to law enforcement. *SEEU Review* [online], *15*(2), 42–55. Available at: https://doi.org/10.2478/seeur-2020-0016

Aryudhanty, D. D., Yen, L. T., and Chan, N. J., 2023. Pros and cons of application of extraterritorial jurisdiction in international law: Various practices in Southeast Asian countries. *International Law Discourse in Southeast Asia* [online], *2*(1), 57–74. Available at: https://doi.org/10.15294/ildisea.v2i1.58389

Azam, H., *et al.*, 2023. Cybercrime unmasked: Investigating cases and digital evidence. *International Journal of Emerging Multidisciplinaries: Computer Science and Artificial Intelligence* [online], *2*(1), 1–31. Available at: https://doi.org/10.54938/ijemdcsai.2023.02.1.255

Benthem, T., *et al.*, 2024. *Jurisdiction in cyberspace*. Geneva Centre for Security Policy.

Bossler, A. M., and Berenblum, T., 2019. Introduction: New directions in cybercrime research. *Journal of Crime and Justice* [online], *42*(5), 495–499. Available at: https://doi.org/10.1080/0735648X.2019.1692426

Bracco, J., 2022. The complexities of international cybercrime and security: Updating laws for a new digital age. *Journal of International Business and Law* [online], *21*(2), 211–234. Available at: https://scholarlycommons.law.hofstra.edu/jibl/vol21/iss2/6

Bunga, D., 2019. Legal response to cybercrime in global and national dimensions. *Padjadjaran Journal of Law* [online], *6*(1), 69–89. Available at: https://doi.org/10.22304/pjih.v6n1.a4

Connell, S. O., 2023. To ban ransomeware payments, or not to ban ransomware payments : The problems drafting legislation in reponse to ransomware. *Journal of International Business and Law* [online], *22*(1), 151–176. Available at: https://scholarlycommons.law.hofstra.edu/jibl/vol22/iss1/6

Faquir, D., *et al.*, 2021. Cybersecurity in smart grids, challenges and solutions. *AIMS Electronics and Electrical Engineering* [online], *5*(1), 24–37. Available at: https://www.aimspress.com/article/doi/10.3934/electreng.2021002

Gupta, P., and Mata-Toledo, M., 2016. Cybercrime: In disguise crimes. *Journal of Information Systems & Operations Management*, 1–10.

Horovic, S., Boban, M., and Stipanovic, I., 2021. Cybersecurity and criminal justice in digital society. *Economic and Social Development 66th International Scientific Conference on Economic and Social Development (ESD) Book of Proceedings*, 52–60.

Iqbal, J., and Beigh, B. M., 2017. Cybercrime in India : Trends and challenges. *International Journal of Innovations & Advancement in Computer Science*, *6*(12), 187–196.

Kausar, S., Leghari, A. R., and Iftikhar, E., 2023. Analysis of the cyber security challenges and solutions. *Journal of Positive School Psychology*, *7*(1), 163–171.

Komalasari, R., and Mustafa, C., 2023. A healthy game-theoretic evaluation of NATO and Indonesia's policies in the context of international law. *Jurnal Pertahanan: Media Informasi Tentang Kajian & Strategi Pertahanan Yang Mengedepankan Identity, Nasionalism & Integrity* [online], *9*(2), 333–349. Available at: https://doi.org/10.33172/jp.v9i2.16794.

Kruti, A., Butt, U., and Sulaiman, R., 2023. *A review of SolarWinds attack on Orion platform using persistent threat agents and techniques for gaining unauthorized access* [online]. 1–6. Available at: https://arxiv.org/abs/2308.10294

Kumar, A., 2024. Examining cybersecurity laws : Protecting critical infrastructure against emerging threats and global cybercrimes. *Journal of Law and Intellectual Property Rights*, 1(1), 21–29.

Kurnia, A. C., n.d. Penerapan Prinsip Yurisdiksi Universal Terhadap Penegakan Hukum Dalam Tindak Pidana Siber (Cybercrime) Di Indonesia. *Jurnal Ilmu Hukum Yustisia* [online], 23(1), 1–14. Available at: [FHUI Depok].

Kurniawan, I. A., Mahmud, H., and Dewi, N., 2021. Penyebaran virus ransomware Wannacry berdasarkan undang-undang No. 11 Tahun 2008. *Jurnal Inovasi Penelitian* [online], *2*(2), 427–432. https://www.neliti.com/publications/469704/penyebaran-virus-ransomware-wannacry-berdasarkan-undang-undang-no-11-tahun-2008

Laksana, T. G., and Mulyani, S., 2024. Faktor-Faktor Mendasar Kejahatan Siber Terhadap Kemanusiaan. *Jurnal Hukum Prioris*, *11*(2), 136–160.

Magableh, H. Y., and Al-Shawabkeh, B. K. A., 2024. The problem of jurisdictional conflict and the applicable law on cybercrime. *Pakistan Journal of Criminology* [online], *16*(3), 1287–1298. Available at: https://doi.org/10.62271/pjc.16.3.1287.1298

Malik, S., *et al.*, 2022. Critical feature selection for machine learning approaches to detect ransomware. *International Journal of Computing and Digital Systems* [online], *11*(1), 1167–1176. Available at: https://doi.org/10.12785/ijcds/110195

Martínez, J., and Durán, J. M., 2021. Software supply chain attacks, a threat to global cybersecurity: SolarWinds' case study. *International Journal of Safety and Security Engineering* [online], *11*(5), 537–545. Available at: https://doi.org/10.18280/ijsse.110505

Milon, M. N. U., *et al.*, 2024. An in-depth PRISMA based review of cybercrime in a developing economy: Examining sector-wide impacts, legal frameworks, and emerging trends in the digital era. *Edelweiss Applied Science and Technology*

[online], *8*(4), 2072–2093. Available at: https://doi.org/10.55214/25768484.v8i4.1583

Mustam, A. M. A., 2023. Memerangi Kejahatan Siber Di Indonesia: Analisis Regulasi Hukum Pidana Yang Berlaku Dan Tantangannya. *Uniba* [online], *35*(1), 10–14. https://www.journal.uniba.ac.id/index.php/GM/article/view/1145

Natsag, B., *et al.*, 2025. Implications of cyber warfare on global power dynamics : Pakistan' s cyber security needs in evolving international arena. *Pakistan Journal of Life and Social Sciences* [online], *23*(1), 8536–8548. Available at: https://doi.org/10.57239/pjlss-2025-23.1.00664

Orlovskyi, R., *et al.*, 2023. Countering cybercrime under martial law. *Journal of Cyber Security and Mobility* [online], *12*(6), 893–910. Available at: https://doi.org/10.13052/jcsm2245-1439.1264

Parulian, S., Pratiwi, D. A., and Cahya Yustina, M., 2021. Ancaman dan Solusi Serangan Siber di Indonesia. *Telecommunications, Networks, Electronics, and Computer Technologies (TELNECT)* [online], *1*(2), 85–92. Available at: https://doi.org/10.17509/telnect.v1i2.40866.

Pratiwi, D. K., 2019. Implementasi Prinsip Yurisdiksi Universal Mengenai Pemberantasan Kejahatan Perompakan Laut di Indonesia. *Supremasi Jurnal Hukum* [online], *2*(1), 119–130. Available at: https://doi.org/10.36441/supremasi.v2i1.111

Putri, D. K., 2022. Urgensi Asas Subsider Pada Pengaturan Asas Universal Dalam Rancangan Kitab Undang-Undang Hukum Pidana. *Jurnal Masalah-Masalah Hukum* [online], *51*(2), 162–170. Available at: https://doi.org/10.21456/vol%viss%ipp605-616.

Qudus, L., 2025. Cybersecurity governance : Strengthening policy frameworks to address global cybercrime and data privacy challenges. *International Journal of Science and Research Archive* [online], *14*(01), 1146–1163. Available at: https://doi.org/10.30574/ijsra.2025.14.1.0225

Ramayanti, H., and Lubis, A. F., 2023. Peran Hukum dalam Mengatasi Serangan Cyber yang Mengancam Keamanan Nasional. *Jurnal Hukum Dan HAM Wara Sains* [online], *2*(09), 904–912. Available at: https://doi.org/10.58812/jhhws.v2i09.672

Schmitt, M. N., and Vihul, L., 2017. Respect for sovereignty in cyberspace. *Texas Law Review* [online], 95, 1639–1670. https://texaslawreview.org/wp-content/uploads/2017/11/Schmitt.Vihul_.pdf

Shevchenko, P. V., *et al.*, 2021. The nature of losses from cyber-related events: Risk categories and business sectors. *Journal of Cybersecurity* [online], *9*(1), 1–24. Available at: https://doi.org/10.1093/cybsec/tyac016

Siregar, G., and Sinaga, S., 2021. The law globalization in cybercrime prevention. *International Journal of Law Reconstruction* [online], *5*(2), 1–14. Available at: https://doi.org/10.26532/ijlr.v5i2.17514

Sviatun, O. V., *et al.*, 2021. Combating cybercrime: Economic and legal aspects. *WSEAS Transactions on Business and Economics* [online], 18, 751–762. Available at: https://doi.org/10.37394/23207.2021.18.72.

Światkowska, J., 2020. *Tackling cybercrime to unleash developing countries' digital potential. Background paper 33* [online]. January. Pathways For Prosperity Commission. https://pathwayscommission.bsg.ox.ac.uk/sites/default/files/2020-01/tackling_cybercrime_to_unleash_developing_countries_digital_potential.pdf

Syaakirah, C. R., Syifa, L., and Muda, I., 2025. Digital Forensic investigation in cybercrime cases : Case studies and recommendations. *Multidisciplinary Journal of Engineering and Technology* [online], *2*(1), 9–15. Available at: https://doi.org/10.61784/mjet3018

Umanailo, M. C. B., *et al.*, 2019. Cybercrime case as impact development of communication technology that troubling society. *International Journal of Scientific and Technology Research* [online], *8*(9), 1224–1228. https://www.ijstr.org/final-print/sep2019/Cybercrime-Case-As-Impact-Development-Of-Communication-Technology-That-Troubling-Society.pdf

Viganò, E., Loi, M., and Yaghmaei, E., 2020. Cybersecurity of Critical Infrastructure. *The International Library of Ethics, Law and Technology* [online], 21, 157–177. Available at: https://doi.org/10.1007/978-3-030-29053-5_8

Wang, G., 2021. Are there international rules governing cyberspace? *Journal of International and Comparative Law* [online], *8*(2), 357–384. https://www.jicl.org.uk/storage/journals/November2021/j2mAGhUYxXihobo2dVBr.pdf

Wang, X., 2024. Global (re-)framing of cybercrime: An emerging common interest in flux of competing normative powers? *Leiden Journal of International Law* [online], *38*(2), 1–27. Available at: https://doi.org/10.1017/S0922156524000402

Wicki-Birchler, D., 2020. The Budapest Convention and the General Data Protection Regulation: Acting in concert to curb cybercrime? *International Cybersecurity Law Review* [online], 1, 63–72. Available at: https://doi.org/10.1365/s43439-020-00012-5.

Wong, H. M., 2024. Research on international cooperation in cracking down cross-border cyber-telecoms fraud. *Transactions on Social Science, Education and Humanities Research* [online], 12, 8–14. Available at: https://doi.org/10.62051/dfk43n30

Zhou, Y., *et al.*, 2024. Metacrime and cybercrime: Exploring the convergence and divergence in digital criminality. *Asian Journal of Criminology* [online], 19, 419–439. Available at: https://doi.org/10.1007/s11417-024-09436-y.

Zhu, L., and Chen, W., 2023. Chinese Approach to international law with regard to cyberspace governance and cyber operation: From the perspective of the five principles of peaceful co-existence. *Baltic Yearbook of International Law Online* [online], 187–208. Available at: https://doi.org/10.1163/22115897_02001_010