Research Article

Perspective of State Sovereignty in Law Enforcement Related to Cyberlaw Jurisdiction

Benny Irawan[1], Dewi Mulyanti[2], Hendi Budiaman[3], Yogi Muhammad Rahman[4], Asari Taufiqurrohman[5]

[1]Faculty of Law, Universitas Sultan Ageng Tirtayasa, Indonesia
[2,3,4]Faculty of Law, Universitas Galuh, Indonesia
[5]Summer School CPG-Goethe Universitat, Germany

ABSTRACT

Digital development brings both positive and negative impacts. One of the negative consequences of this transformation is the increasing prevalence of criminal activities in the digital realm. This study aims to examine criminal regulatory policies related to cybercrime in Indonesia, particularly those that pose a threat to national sovereignty. The research method employed is normative juridical, using secondary data sources.The findings indicate that criminal law, as a branch of legal science, bears the responsibility of adapting to societal changes—especially in safeguarding citizens, as this is closely linked to state sovereignty. Cybercrime has emerged as a widely discussed issue in both academic and non-academic contexts. These crimes disrupt the security of individuals and threaten national sovereignty, as seen in incidents such as the hijacking of Indonesian citizens' personal data.The study concludes that more technical regulations are required for addressing cybercrimes committed beyond the territory of the Unitary State of the Republic of Indonesia. One proposed solution is the adoption of a "police-to-police" cooperation framework. This approach is expected to serve as an alternative for the government to respond more effectively to such issues, thereby facilitating the development of laws that are both efficient and effective.

Keywords: Jurisdiction; Law Enforcement; Cyberlaw; Nation Dignity

A. INTRODUCTION

The digital era has brought significant transformations to various aspects of societal life, particularly in the field of information technology. This technology plays a crucial role not only in the present but also in shaping the future. However, these advancements are not solely accompanied by positive developments—such as the emergence of email, e-commerce, and online business—but are also often followed by negative consequences. These adverse effects can lead to certain actions being classified as criminal offenses.

The term *criminal offense* originates from the Dutch criminal law term *Strafbaar feit*, which consists of three components: *straf*, *baar*, and *feit*. *Straf* translates to "punishment" or "penalty"; *baar* to "capable" or "permissible"; and *feit* to "act," "event," or "violation" (Chazawi, 2007).

Cybercrime is a term that has become increasingly prevalent in recent years. It represents a new form of criminal activity that has emerged directly from the advancement of information technology, utilizing the internet as a medium for committing offenses. In various academic sources, cybercrime is often used

interchangeably with computer crime (Dupont, Fortin, & Leukfeldt, 2024).

The U.S. Department of Justice defines computer crime as: "...any illegal act requiring knowledge of computer technology for its perpetration, investigation, or prosecution." Similarly, the Organization for Economic Co-operation and Development (OECD) describes it as: "any illegal, unethical, or unauthorized behavior relating to the automatic processing and/or the transmission of data." Hamzah also defines cybercrime as "a crime in the field of computers, generally understood as the illegal use of computers."

These definitions illustrate the broad scope and complexity of cybercrime, particularly as it intersects with legal and technological domains (Fuady, 2025).

According to John Arquilla and David Ronfeldt, the information revolution has brought about significant changes that support the growth of networks, enabling various actors to communicate, coordinate, and operate without being constrained by space and time (Arquilla & Ronfeldt, 1993). In the 1980s, particularly in European and North American countries, there was an emerging trend toward the criminalization of new offenses associated with the use of computer technology to commit conventional crimes. Several international conventions have addressed cybercrime, including those initiated by the Organisation for Economic Co-operation and Development (OECD), the United Nations (UN), the Group of Eight (G8), and the Council of Europe (CoE).

In Indonesia, the advancement of technology during the 1990s became a significant concern for both the public and the government. By the year 2000, the government began to take concrete steps to regulate various activities within cyberspace. One of the earliest efforts was the drafting of a Bill on the Utilization of Information Technology, initiated by the Directorate General of Post and Telecommunications under the Ministry of Transportation (Situmeang, 2020). Over time, this draft evolved into the Bill on Information, Communication, and Electronic Transactions.

In March 2003, responsibility for the drafting of the Bill on Information, Communication, and Electronic Transactions was transferred to the Ministry of Communication and Information Technology. This transition led to a further refinement of the draft into the Bill on Electronic Information and Transactions. Eventually, the bill was enacted and promulgated as Law No. 11 of 2008 on Electronic Information and Transactions, which was later amended by Law No. 19 of 2016.

Widodo outlines several key principles related to cyberlaw, as follows (Widodo, 2013):

1) Subjective Territoriality: This principle holds that the law is applicable based on the location where the cybercrime was initiated, even if the resolution or effects of the offense occur in another country.
2) Objective Territoriality: Under this principle, the law applies based on the location where

the primary consequences of the cybercrime take place, especially if the impact significantly affects the concerned nation.

3) Passive Nationality: This principle emphasizes jurisdiction based on the nationality of the victim, asserting that a state may exercise legal authority if its citizens are affected by criminal acts abroad.
4) Protective Principle: This principle permits a state to apply its laws extraterritorially to safeguard its national security and interests. It is commonly invoked when the crime directly threatens the state or its government.
5) Universality: Known as the "universal jurisdiction principle," this concept allows a state to claim jurisdiction over certain serious crimes regardless of where they were committed or the nationalities of the perpetrators or victims. It is particularly relevant in addressing cybercrime cases with cross-border implications.

Based on the types of activities involved, cybercrimes can be classified into several categories, as outlined by Hiariej (2016):

1. Illegal Content: This refers to crimes involving the dissemination of false, unethical, or unlawful data or information via the internet that may disturb public order or violate legal norms.
2. Data Forgery: This type of crime involves the falsification of data in essential documents found on the internet, typically with the intent to deceive or commit fraud.
3. Infringement of Privacy: These crimes target individuals' private and confidential information, which is considered highly personal and sensitive.
4. Offenses Against Intellectual Property: These involve violations of intellectual property rights belonging to individuals or entities on the internet.
5. Unauthorized Access: This offense occurs when an individual unlawfully infiltrates a computer network system without authorization, consent, or the knowledge of the system's owner.

In practice, numerous cybercrime cases have been reported in Indonesia. The following are summarized cases compiled by the author (Farid, 2022):

1. Hacker War Between Indonesia and Australia (2013)

   This incident began after Edward Snowden, a former U.S. intelligence officer, revealed that Australia had wiretapped President Susilo Bambang Yudhoyono (SBY). The disclosure provoked strong reactions from Indonesian hackers, leading to the formation of a group known as *Anonymous Indonesia*.
2. Tiket.com and Citilink Hacked (2016)

   In October 2016, a group of teenage hackers breached the online ticketing platform Tiket.com and gained access to Citilink's servers. As a result, Tiket.com experienced financial losses amounting to IDR 4.1 billion, while Citilink suffered damages of approximately IDR 2 billion.

3. Data Breach at Tokopedia (2020)
   In 2020, Tokopedia suffered a major data breach when a hacker group known as *ShinyHunters* leaked the personal data of 91 million users and over seven million e-commerce merchants. This sensitive information was later sold online for approximately IDR 70 million.
4. Hacking of BRI Life Insurance Company (2021)
   In July 2021, around two million customer records from BRI Life were allegedly compromised and offered for sale online at a price of $7,000, equivalent to approximately IDR 101.6 million.
5. Data Breach in e-HAC by the Ministry of Health (2021)
   Also in July 2021, the Electronic Health Alert Card (e-HAC) application managed by the Ministry of Health was targeted by cyber attackers, resulting in the exposure of data from 1.3 million Indonesian citizens.
6. Indihome Customer Data Breach (2022)
   In August 2022, approximately 26 million data entries, allegedly belonging to Indihome customers, were leaked and sold on *Breach Forums* by a hacker identified as *Bjorka*. The leaked information included search histories, keywords, email addresses, names, genders, and national identification numbers.
7. Cyberattack on Jasa Marga (2022)
   Also in August 2022, the state-owned toll road operator Jasa Marga was attacked by a hacker group known as the *Desorden Group*. The attackers leaked 252 GB of data, including internal records, coding scripts, and documents from five of the organization's servers.

The cases presented by the author illustrate how critical and confidential data owned by corporate entities—as well as data commonly held by Indonesian citizens—have become commodities traded on open-market platforms by irresponsible parties. When such actions occur within the territory of the Republic of Indonesia, they can be addressed relatively effectively by law enforcement authorities, particularly the Indonesian National Police, utilizing advanced technological tools. However, when these actions are perpetrated outside the jurisdiction of the Republic of Indonesia, they present significant challenges to law enforcement efforts.

Jurisdiction refers to the authority of a state to apply legal rules within its legal domain, encompassing individuals, objects, or events. According to the general principles of international law, every state possesses sovereignty and jurisdiction over its own territory (Jaya et al., 2024), thereby limiting the actions a state can undertake beyond its borders. As a result, no state may infringe upon the sovereignty of another by conducting legal or enforcement activities within the latter's territory.

The application of criminal jurisdiction by a sovereign state under international law is based on several well-established jurisdictional principles (Adolf, 1991; Setiyono et al., 2020):

1) The Territorial Principle: This principle allows a state to exercise national jurisdiction over all individuals (citizens or foreigners), legal entities, and objects located within its territorial boundaries. It serves as the primary foundation for the exercise of jurisdiction by a state.
2) The Active Nationality Principle: Under this principle, the nationality of the perpetrator serves as the connecting factor that permits the state of origin to apply its jurisdiction.
3) The Passive Nationality Principle: This principle grants a state the authority to prosecute individuals for criminal acts committed abroad if those acts cause harm to its citizens.
4) The Protective Principle: This principle permits a state to assert jurisdiction over acts committed outside its territory if those acts pose a threat to its national security or vital legal interests.
5) The Universal Principle: Under this principle, a state may exercise jurisdiction over criminal acts that violate universally recognized values upheld by the international community, regardless of where the acts occur or the nationalities involved.

Cybercrime is classified as a transnational crime, involving the interests of multiple countries. Transnational crimes are offenses that have consequences extending across national borders, involving citizens of various nations and utilizing means and infrastructure that transcend jurisdictional boundaries (Situmeang, 2020).

Cybercrime, as a transnational criminal offense, often entails the involvement of multiple jurisdictions in its commission (Arnell & Faturoti, 2022). Jurisdiction becomes a critical issue when legal frameworks differ across these regions. From a legal standpoint, Indonesian law provides for the enforcement of criminal provisions related to cybercrime, even beyond the territory of the Republic of Indonesia.

However, the law remains merely a written text in the absence of institutions capable of enforcing it. This is what is referred to as the structure of law. In the context of cyberlaw enforcement, the author emphasizes the urgency for law enforcement agencies—particularly the Indonesian National Police—to swiftly develop the technical frameworks and operational mechanisms necessary for effective enforcement.

Based on the description above, this study aims to examine criminal regulatory policies related to cybercrime in Indonesia that pose a threat to state sovereignty.

This research differs from previous studies published in both national and reputable international journals. The previous studies referred to include the following: research published in national journals such as the study on cyber law enforcement in Indonesia, addressing its challenges and opportunities (Pansariadi & Soekorini, 2023); a study on law enforcement against cybercrime committed by hackers (Arisandy, 2020); and research on legal protection for child victims of cybercrime in

Indonesia through penal and non-penal approaches (Djanggih, 2018).

Meanwhile, studies published in reputable international journals include research on normative shifts in the enforcement of cybercrime laws (Ryngaert, 2023), as well as studies on international legal regulations concerning cybercrime that threatens state sovereignty (Chatinakrob, 2024).

Based on a comparison with these previous studies, both at the national and international levels, it can be concluded that no prior research has specifically addressed cybercrime that threatens state sovereignty from the perspective of Indonesian criminal law, as is examined in this study. Therefore, this research offers a distinct contribution and possesses novelty in its focus and legal analysis.

B. RESEARCH METHODS

This study employs a normative juridical research method, which involves library-based legal investigation grounded in legal norms derived from both international regulations and Indonesian national legislation. Normative legal research emphasizes the normative aspects of law and functions as a practical discipline within normative jurisprudence. It contributes to the legal decision-making process by addressing legal gaps, clarifying vague or ambiguous norms, narrowing the interpretation or definition of legal provisions to ensure their applicability to specific legal cases, and even discovering new legal rules (Alam, 2020).

A key characteristic of normative legal research is its reliance on secondary data sources (Jaya et al., 2023). Legal materials are categorized into primary, secondary, and tertiary sources (Jaya et al., 2024). Primary legal materials include international treaties and statutory laws; secondary legal materials comprise scholarly works such as books, journal articles, and research reports; while tertiary legal materials consist of supporting references like online databases and encyclopedias used during the research process (Irawan et al., 2024).

This study adopts a statutory approach, focusing on jurisdictional provisions contained within the Indonesian Criminal Code. Data collection techniques involve conducting a comprehensive literature review and analyzing various cybercrime cases that have occurred in Indonesia. The data are then analyzed qualitatively (Benuf & Azhar, 2020). In addition, this study incorporates a legal principles approach, which seeks to identify applicable legal standards or doctrines found in positive law (Bachtiar, 2018).

C. RESULTS AND DISCUSSION

1. Criminal Regulations Related to Cybercrime in Indonesia That Threaten State Sovereignty

Before discussing the jurisdictional aspects of such acts, it is essential to first address the substantive law governing cybercrimes. Prior to the enforcement of the Electronic Information and Transactions Law, law enforcement authorities

relied on the provisions of the Indonesian Criminal Code to prosecute cybercrimes. In this context, the applicable Criminal Code refers to the old Indonesian Criminal Code, as the new Criminal Code, stipulated under Law No. 1 of 2023, will not come into effect until 2026.

The provisions used to address cybercrime within the Indonesian Criminal Code include regulations on forgery (Articles 263–276), theft (Articles 362–372), fraud (Articles 378–395), and property damage (Articles 407–412). In practice, multiple articles of the Indonesian Criminal Code are often applied simultaneously, as cybercrime typically involves several interconnected actions that fall under different legal provisions (Subagyo, 2015; Soponyono & Bernadhi, 2016).

Law No. 19 of 2016, which amends Law No. 11 of 2008 on Electronic Information and Transactions, serves as a new source of positive law concerning cybercrime. The Electronic Information and Transactions Law provides regulations regarding any legal actions that result in legal consequences and harm the interests of the Republic of Indonesia.

Regarding jurisdictional issues in internet or cybercrime cases, Darrel Menthe proposed a theory stating that interactions in cyberspace involve two fundamental issues: the provision of information and the retrieval of information into and out of cyberspace, or, in this case, the cyber world. Menthe's theory is referred to as the "Uploader and Downloader Theory." This theory distinguishes between two roles: the uploader, who provides information to cyberspace, and the downloader, who retrieves that information at a later time, regardless of their identities (whether as the uploader or the downloader).

Johnson and Post argue that the application of traditional principles of "Due Process and personal jurisdiction" is inappropriate and causes confusion when applied to cyberspace. According to Johnson and Post, cyberspace should be regarded as a distinct "space" separate from the "real world" and subject to its own set of laws (Situmeang, 2020).

In addressing jurisdictional issues in cyberspace, Barda Nawawi Arief states that the universal origin or ubiquity principle is used to tackle the problem of cybercrime. The ubiquity principle asserts that a crime committed or occurring partly within the territorial boundaries of a country and partly outside the country's boundaries must be brought under the jurisdiction of the respective countries involved. This principle was recommended at the International Meeting of Experts on The Use of Criminal Sanctions in the Protection of the Environment, Internationally, Domestically, and Regionally, held in Portland, Oregon, United States, from March 19 to 23, 1994 (Arief, 2007).

In criminal law doctrine concerning locus delicti, the theory of *leer van instrument* or the "instrument theory" is recognized. According to this theory, the locus delicti is determined by the instrument used, and through this instrument, the criminal act is carried out. Eddy Hiariej explains that the application of this instrument theory is particularly significant in crimes with sophisticated

modus operandi or those that occur across borders, such as cybercrime (Hiariej, 2016).

The legal principles or foundations outlined by the author earlier are abstract in nature. Mertokusumo explains that legal principles or foundations are not concrete legal regulations, but rather general ideas or the background of specific regulations that exist within and behind every legal system, as reflected in legal provisions (Mochtar & Hiariej, 2021). In other words, the author interprets that the implementation of a legal principle or foundation becomes applicable only once it has been concretized into a regulation.

The old Criminal Code regulates the territorial limits of criminal provisions within Indonesian legislation as follows:

Article 2: Criminal provisions in Indonesian legislation apply to any individual who commits a criminal offense within Indonesia.

Article 3: Criminal provisions in Indonesian legislation apply to any individual who, outside the territory of Indonesia, commits a criminal offense aboard an Indonesian vessel or aircraft.

Article 4: Criminal provisions in Indonesian legislation apply to any individual who commits the following offenses outside Indonesia:

1. Any crime stipulated in Articles 104, 106, 107, 108, and 131.
2. A crime related to currency or banknotes issued by the state or bank, or concerning stamps issued by the Government of Indonesia, or trademarks used by the Government of Indonesia.
3. The forgery of debt instruments or certificates of debt under the responsibility of Indonesia, or those of a region within Indonesia, including the forgery of coupons, dividend slips, or interest slips attached to such documents, and those issued as substitutes for these documents, or the use of such forged or falsified documents as though they were genuine.
4. Any crime listed in Articles 438, 444 through 446 concerning piracy, and Article 447 regarding the surrender of a vessel to pirates, as well as Article 479, letter j concerning the unlawful control of aircraft, and Articles 479, letters l, m, n, and o concerning crimes that threaten civil aviation safety.

Law No. 11 of 2008 concerning Electronic Information and Transactions regulates the principle of jurisdiction in the application of legislation as follows:

Article 2: This law applies to any person who performs legal actions as regulated in this law, whether within the jurisdiction of Indonesia or outside the jurisdiction of Indonesia, provided that the actions have legal consequences within the jurisdiction of Indonesia and/or outside the jurisdiction of Indonesia and harm Indonesia's interests.

The explanation of this article states that this law has a jurisdictional scope that applies not only to legal actions within Indonesia or performed by Indonesian citizens, but also to legal actions performed outside the jurisdiction of Indonesia, whether by Indonesian citizens or

foreign nationals, or by Indonesian legal entities or foreign legal entities, provided such actions have legal consequences in Indonesia. This is in recognition of the fact that the use of Information Technology for Electronic Information and Electronic Transactions can be transnational or universal in nature.

It would be prudent for the author to also include the provisions of the latest law, Law No. 1 of 2023 concerning the Indonesian Criminal Code, even though this regulation has not yet come into effect as of the time this article was written. The law provides detailed provisions regarding jurisdiction.

Article 4: The criminal provisions in this law apply to every individual who commits: a) A criminal act within the territory of the Unitary State of the Republic of Indonesia; b) A criminal act aboard an Indonesian vessel or an Indonesian aircraft; or c) A criminal act in the field of information technology or other criminal acts whose consequences are experienced or occur within the territory of the Unitary State of the Republic of Indonesia or aboard an Indonesian vessel or an Indonesian aircraft. *(emphasis added by the author)*

Article 5: The criminal provisions in this law apply to any individual outside the territory of the Unitary State of the Republic of Indonesia who commits a criminal act affecting the interests of the Unitary State of the Republic of Indonesia, related to: a) National security or the processes of state governance; b) The dignity of the President, Vice President, and/or Indonesian officials abroad; c) The currency, seals, state stamps, or government-issued securities of the Republic of Indonesia, or credit cards issued by Indonesian banks; d) The economy, trade, and banking system of Indonesia; e) The safety or security of maritime and aviation activities; f) The safety or security of buildings, equipment, and national assets or properties of Indonesia; g) The safety or security of the electronic communication system; h) The national interests of Indonesia as stipulated in the law; or i) Indonesian citizens, in accordance with international agreements with the country where the criminal act occurred.

Article 6: The criminal provisions in this law apply to any individual outside the territory of the Unitary State of the Republic of Indonesia who commits a crime under international law that has been designated as a criminal offense under this law.

Article 7: The criminal provisions in this law apply to any individual who commits a criminal offense outside the territory of the Unitary State of the Republic of Indonesia, where prosecution is taken over by the Government of Indonesia based on an international agreement granting the Government of Indonesia the authority to prosecute the offense.

Article 8:

1. The criminal provisions in this law apply to every Indonesian citizen who commits a criminal act outside the territory of the Unitary State of the Republic of Indonesia.

2. The provisions referred to in paragraph (1) apply if the act in question is also considered a criminal offense in the country where the crime was committed.
3. The provisions referred to in paragraph (1) do not apply to criminal offenses punishable by a fine not exceeding category III.
4. Prosecution for criminal acts referred to in paragraph (1) may be carried out even if the suspect becomes an Indonesian citizen after the criminal act was committed, provided that the act constitutes a criminal offense in the country where it occurred.
5. Indonesian citizens outside the territory of the Unitary State of the Republic of Indonesia who commit the criminal acts referred to in paragraph (1) may not be sentenced to the death penalty if such acts, under the laws of the country where the crime was committed, are not punishable by the death penalty.

2. Criminal Regulatory Policies Related To Cybercrime In Indonesia That Threaten State Sovereignty

Cybercrimes committed by Indonesian citizens or foreign nationals outside the territory of the Republic of Indonesia must be enforced. This is closely related to national sovereignty. It is conceivable that confidential and critical data of a country could be easily hacked without optimal law enforcement efforts from that country.

Sovereignty is a fundamental right of every nation, serving as a prerequisite for the implementation of a legal system within its territory to ensure the continuity of life for its residents (Paris, 2020). Jean Bodin proposed the doctrine that sovereignty is the primary source for establishing law. Sovereignty represents the source of authority and is positioned as the highest principle in the legal hierarchy. It is a concept of paramount importance within both domestic and international legal orders, serving as the point of intersection between these two systems. National sovereignty is one of the foundational norms within the international legal system (Riyanto, 2012).

Criminal law plays a vital role in ensuring the sovereignty of the state. This is reflected in the function of criminal law, which is to protect legal interests. The protection extends not only to individual interests but also to the interests of the state and society (Mochtar & Hiariej, 2021). The breach of personal data in the case at hand constitutes a violation of human rights. Law No. 27 of 2022 on Personal Data Protection explicitly states in its considerations that personal data protection is a fundamental human right, which is part of the protection of personal security. Therefore, it is essential to provide a legal foundation to ensure the security of personal data (Lestari et al., 2024).

Article 4, letter E of the Electronic Information and Transactions Law explicitly states that the utilization of Information Technology and Electronic Transactions is carried out with the aim of providing a sense of security, justice, and legal certainty for users and organizers of Information Technology.

Quoting the legal system theory from Friedman, it is stated that the legal system consists of law substance, law structure, and law culture (Stinchcombe, 2024). Using Friedman's analysis, it can be concluded that, in terms of substance, there are regulations that support the enforcement of the law outside the territory of the Republic of Indonesia.

The law is merely a text if there is no institution to enforce it. This is what is meant by the law structure. In the context of law enforcement related to cyberlaw, the author urges law enforcement agencies, especially the Indonesian National Police, to promptly formulate the necessary technical aspects for enforcement.

Article 2 of Law No. 20 of 2002 concerning the Indonesian National Police explains that the function of the Police is one of the state's governmental functions in maintaining public security and order, law enforcement, protection, fostering, and providing services to the community.

Regarding the interpretation in Article 4 of this law, which pertains to achieving domestic security, it illustrates that the Indonesian National Police (Polri) holds significant responsibility for security. Although the causes of insecurity may originate from abroad, the resulting impact affects national security. Therefore, it is essential for Polri to be the frontline institution in handling cybercrime.

There are several methods that the Indonesian National Police can employ in handling cases outside the territory of the Republic of Indonesia, including the following:

1. Extradition: As defined in Black's Law Dictionary, extradition is "the official surrender of an alleged criminal by one state or nation to another having jurisdiction over the crime charged." Remmelink defines extradition as the transfer of a suspect, defendant, or convict by the state where the individual is located to another state that seeks to prosecute the individual or enforce a judgment issued by the court of the requested state. International extradition refers to a request by one government to another country for the surrender of an individual to face prosecution or to serve a sentence (Hiariej, 2016).
2. Mutual Legal Assistance: Mutual legal assistance is an international cooperation system in the field of crime prevention and eradication, particularly concerning transnational crimes (Joutsen, 2019). In 2006, Indonesia enacted Law No. 1 of 2006 on Mutual Legal Assistance in Criminal Matters. According to Article 5 of this law, mutual legal assistance in criminal matters may be provided based on an agreement. However, if no such agreement exists, mutual assistance may still be possible based on friendly relations and the principle of reciprocity. Indonesia has entered into mutual legal assistance agreements with the following countries (Hartono & Hapsari, 2019):
    - Australia, on October 27, 1995, ratified by Law No. 1 of 1999;

- China, on July 24, 2000, ratified by Law No. 8 of 2006;
- South Korea, on March 30, 2002 (currently in the process of ratification);
- Hong Kong SAR, on April 3, 2008 (currently in the process of ratification);
- India, on January 25, 2011 (currently in the process of ratification).

3. **Police-to-Police Cooperation**: This represents a form of High-Level Diplomacy (HLD), utilizing a law enforcement approach.

The author believes that, in enforcing the law against cybercrime offenses occurring outside the jurisdiction of the Republic of Indonesia, the "police-to-police" approach is the most efficient and effective among the three available methods for law enforcement agencies, particularly the Indonesian National Police. This approach is preferred because it does not involve numerous institutions, thus avoiding the complexities of bureaucratic procedures.

This view is supported by the success of the police in apprehending perpetrators of extraordinary crimes, such as corruption and drug trafficking, through this approach. The Indonesian National Police successfully apprehended Djoko S. Tjandra, a fugitive involved in the Bali Bank Cessie corruption case (Prasetyo, 2020). Additionally, cooperation related to narcotics cases involving international networks has also been facilitated through the police-to-police approach.

D. CONCLUSION

Based on the results of this study, it is concluded that criminal law, as a branch of science, has a responsibility to respond to societal changes, particularly in the protection of citizens, as it is closely related to state sovereignty. Cybercrime, a relatively new issue, is widely discussed in both academic and non-academic circles. This crime disrupts citizens' peace and threatens state sovereignty, such as through the hijacking of Indonesian citizens' data. The conclusion of this study is that more technical regulations are needed regarding the handling of cybercrime committed outside the territory of the Unitary State of the Republic of Indonesia, one of which could be the concept of police-to-police cooperation. This approach is expected to serve as an alternative for the government to address these issues and create more efficient and effective laws.

REFERENCES

JOURNALS

Alam, S. (2020) Optimalisasi Sanksi Pidana Terhadap Pelanggaran Baku Mutu Lingkungan Dari Limbah. *Jurnal Penelitian Hukum De Jure,* Vol.20, (No.01), pp.137-151. https://doi.org/10.30641/dejure.2020.v20.137-151.

Arisandy, Yogi O. (2020). Penegakan Hukum Terhadap Cyber Crime Hacker. *Indonesian Journal of Criminal Law and Crimonology*, Vol.1,(No.3),pp.162–69. https://doi.org/10.18196/ijclc.v1i3.11264

Arnell, Paul., & Faturoti, Bukola. (2022). The prosecution of cybercrime – why transnational and extraterritorial jurisdiction should be resisted. *International Review of Law, Computers and Technology*, Vol.37*,* (No.1),pp.29–51. https://doi.org/10.1080/13600869.2022.2061888.

Arquilla, John., & Ronfeldt, David. (1993). Cyberwar Is Coming. *Comparative Strategy,* Vol.12, (No.02), pp.23-60. https://www.rand.org/content/dam/rand/pubs/reprints/2007/RAND_RP223.pdf

Benuf, Kornelius., & Azhar, Muhammad. (2020). Metodologi Penelitian Hukum Sebagai Instrumen Mengurai Permasalahan Hukum Kontemporer. *Gema Keadilan,* Vol.07, (No.01),pp.20-33. https://doi.org/10.14710/gk.2020.7504

Chatinakrob, T. (2024). Interplay of International Law and Cyberspace: State Sovereignty Violation, Extraterritorial Effects, and the Paradigm of Cyber Sovereignty. *Chinese Journal of International Law*, Vol.23, (No.1), pp.25–72. https://doi.org/10.1093/chinesejil/jmae005.

Djanggih, H. (2018). Konsepsi Perlindungan Hukum Bagi Anak Sebagai Korban Kejahatan Siber Melalui Pendekatan Penal Dan Non-Penal. *Mimbar Hukum*, Vol.30, (No.2),pp.316–30. https://doi.org/10.22146/jmh.32017.

Dupont, Benoit., Fortin, Francis. & Leukfeldt, Eric Rutger. (2024). Broadening our understanding of cybercrime and its evolution. *Journal of Crime and Justice*, Vol.47,(No.4),pp.435–439.DOI:10.1080/0735648X.2024.2323872.

Fuady, Muhammad E. (2005). Cybercrime, Fenomena Kejahatan Melalui Internet Di Indonesia. *Mediator Journal,* Vol.06, (No.02),pp.255-264. https://doi.org/10.29313/mediator.v6i2.1194

Hartono, Bambang., & Hapsari, Recca Ayu. (2019). Mutual Legal Assitance Pada Pemberantasn Cyber Crime Lintas Yurisdiksi Di Indonesia. *Jurnal SASI,* Vol.25,(No.01),pp.59-71. https://doi.org/10.47268/sasi.v25i1.136.

Irawan, Benny., Firdaus, Firdaus., Jaya, Belardo Prasetya Mega., Taufiqurrohman, A.H Asri., Sari, Siti Wulan., & Furqoni, Sarah. (2024). State Responsibility and Strategy in Preventing and Protecting Indonesian Fisheries Crews Working on Foreign Fishing Vessels from Modern Slavery. *Australian Journal of Maritime and Ocean Affairs*,pp.1-21. https://doi.org/10.1080/18366503.2024.2333107

Jaya, Belardo Prasetya Mega., Ridwan, Ridwan., Mucharom, Rully Syahrul., Wibowo,Dwi Edi., Aisah, Siti Nur., Sulastri, Sulastri., & Alifvia, Novia Bella. (2023). Criticising the Implementation of the ACTIP in Southeast Asia. *Sriwijaya Law Review* Vol.7,(No.2), pp.355-373.

https://doi.org/10.28946/slrev.Vol7.Iss2.2542.pp350-367

Jaya, Belardo Prasetya Mega., Sidiq, Permana., Fasyehhudin, Mohamad., & Solapari, Nuryati. (2024). Republic of Indonesia Sovereign Right in North Natuna Sea according to United Nations Convention on the Law of the Sea 1982. *Australian Journal of Maritime & Ocean Affairs*, Vol.16,(No.1),pp.127–140. https://doi.org/10.1080/18366503.2023.2206261

Joutsen, M. (2019). Extradition and Mutual Legal Assistance. *International and Transnational Crime and Justice*, pp.293–298. https://doi.org/10.1017/9781108597296.049.

Lestari, Ahdiana Yuni., Misran, Trisno Raharjo., Annas, Muhammad., Riskanita, Dinda, Prabandari., & Prabandari, Adya Paramita. (2024). Improving Healthcare Patient Data Security: An Integrated Framework Model for Electronic Health Records from A Legal Perspective. *Law Reform,* Vol.20, (No.2), pp.329-352. https://doi.org/10.14710/lr.v20i2.56986

Pansariadi, Rafi Septia Budianto., & Soekorini, Noenik. (2023). Tindak Pidana Cyber Crime Dan Penegakan Hukumnya. *Bina Mulia Hukum,* Vol. 12, (No.2), pp. 287–298. doi:https://doi.org/10.37893/jbh.v12i2.605.

Paris, R. (2020). The Right to Dominate: How Old Ideas About Sovereignty Pose New Challenges for World Order. *International Organization*,Vol.74,(No.3),pp.453–489. DOI:10.1017/S0020818320000077.

Riyanto, S. (2012). Kedaulatan Negara Dalam Kerangka Hukum Internasional Kontemporer. *Yustisia*, Vol.1, (No.3), pp.49-71. https://doi.org/10.20961/yustisia.v1i3.10074

Ryngaert, C. (2023). Extraterritorial Enforcement Jurisdiction in Cyberspace: Normative Shifts. *German Law Journal,* Vol.24, (No.3),pp.537–550. https://doi.org/10.1017/glj.2023.24.

Setiyono, Joko., Azhar, Muhamad., Solechan, Solechan., Trihastuti, Nanik., & Hakim, Arif R. (2020). Justification of the ship-sinking policy in the territorial jurisdiction of Indonesia. *AACL Bioflux*, Vol.13,(No.5), pp.2610–2618. https://bioflux.com.ro/docs/2020.2610-2618.pdf

Stinchcombe, Arthur L. (2024). Lawrence M. Friedman, The Legal System Donald Black, The Behavior of Law. *Law and Society Review*,Vol.12,(No.1),pp.129–131. DOI:10.1017/S0023921600024324.

Subagyo, A. (2015). Sinergi Dalam Menghadapi Ancaman Cyber Warfare. *Jurnal Pertahanan dan Bela Negara,* Vol.5,(No.1),pp.89-108.DOI:10.33172/jpbh.v5i1.350

CONFERENCE

Soponyono, Eko., & Bernadhi, Brav Deva. (2016). Formulation of Policy for Cyber Crime in

Criminal Law Revision Concept of Bill Book of Criminal Law (A New Penal Code). In IOP Conference Series: Materials Science and Engineering (Vol.190). IAES International Conference on Electrical Engineering, Computer Science and Informatics 23–25 November 2016, Semarang,Indonesia. https://doi.org/10.1088/1757-899X/190/1/012050

BOOKS

Adolf, H. (1991). *Aspek-Aspek Negara Dalam Hukum Internasional.* Jakarta: Raja Grafindo Persada.

Arief, Barda N. (2007). *Masalah Penegakan Hukum dan Kebijakan Hukum Pidana Dalam Penangulangan Kejahatan*. Jakarta: Prenadia Media Group.

Bachtiar. (2018). *Metode Penelitian Hukum*. Tangerang Selatan: Unpam Press.

Chazawi, A. (2007). *Pelajaran Hukum Pidana 1*. Jakarta: Grafindo Persada.

Hiariej, Edward Omar S. (2016). *Prinsip-Prinsip Hukum Pidana*. Yogyakarta: Cahaya Atma Pustaka.

Mochtar, Zainal Arifin., & Hiariej, Edward Omar Sharif. (2021). *Dasar-Dasar Ilmu Hukum*. Jakarta: Red & White Publishing.

Situmeang, Sahat M. (2020). *Cyber Law*. Bandung: Penerbit Cakra.

Widodo. (2013). *Hukum Pidana Di Bidang Teknologi Informasi (Cybercrime Law): Telaah Teoritik dan Bedah Kampus*. Yogyakarta: Aswaja Pressindo.

ONLINE SOURCES

Farid, A. (2022). 14 Kasus Cyber Crime Di Indonesia Yang Menggemparkan Warganet. Retrieved from: https://www.exabytes.co.id/blog/kasus-cyber-crime-di-indonesia/.

Prasetyo, A. (2020). Mengenal Diplomasi Police to Police Yang Mengakhiri Pelarian Djoko Tjandra. Retrieved from: https://www.hukumonline.com/berita/a/mengenal-diplomasi-police-to-police-yang-mengakhiri-pelarian-djoko-tjandra-lt5f280c3b8aa56/?page=1.