JIHAD: Jurnal Ilmu Hukum dan Administrasi
Vol. 8 No. 3 September 2026
p-ISSN : 2745-9489, e-ISSNl 2746-3842
DOI: *10.36312/jihad.v8i2.11108/https://ejournal.mandalanursa.org/index.php/JIHAD/issue/archive*

Cybercrime Law Enforcement Reform: A Comparative Study of the Legal Systems of Indonesia, the United States, and Singapore

Muhammad Fu'ad Hasan[1], Andy Setiawan[2], Samsuhari[3], Isnawati Choiriyah[4], Moch. Eko Setiyo Budi Utomo[5], Dewi Putriani Yogosara Lodewijk[6]
Pascasarjana Magister Hukum Universitas Boyolali, Indonesia

Article Info

Article history:
Accepted: 26 June 2026
Publish: 1 September 2026

Keywords:
Cyber-Criminal Law;
Comparative Law;
Law Enforcement;
Cybercrime;
Legal Reform.

Abstract

The development of information and communication technology has increased the complexity of transnational cybercrime, posing new challenges for the criminal justice system in ensuring effective law enforcement. Although Indonesia has regulated various forms of cybercrime through the Electronic Information and Transactions Law and its amendments, the effective implementation of these regulations still faces various obstacles, particularly related to legal harmonization, enforcement capacity, and international cooperation. This study aims to analyze the characteristics of the cybercriminal legal systems in Indonesia, the United States, and Singapore, identify similarities and differences, evaluate the effectiveness of their implementation, and formulate a reform model relevant to Indonesia. The study uses a normative legal method with a comparative law approach, through an analysis of legislation, legal doctrine, court decisions, and national and international scientific literature. The results show that the United States implements a federal approach that emphasizes investigative capacity and inter-agency coordination through the Computer Fraud and Abuse Act, while Singapore prioritizes an integrated and responsive regulatory model through the Computer Misuse Act and a strong national cybersecurity strategy. Indonesia has a relatively comprehensive regulatory framework, but still faces challenges in enforcement, institutional coordination, and adaptation to evolving digital crime modes. The novelty of this research lies in the formulation of a cybercriminal law enforcement reform model based on regulatory integration, institutional capacity building, and increased international cooperation. These reforms are expected to improve the effectiveness of Indonesia's cybercriminal legal system in addressing the dynamics of global digital crime.

Corresponding Author:
Dewi Putriani Yogosara Lodewijk
Pascasarjana Magister Hukum Universitas Boyolali, Indonesia
Email Coresspondent: advisor.lodewijk@gmail.com

1. INTRODUCTION

The massive digital transformation that has taken place over the past two decades has transformed nearly every aspect of global society, from economic activity and government to education and social interaction. Advances in information and communication technology have created cyberspace as a new medium that enables the rapid exchange of data and information without regard to national jurisdictional boundaries (Brenner, 2022). Ideally, the development of digital technology should improve efficiency,

productivity, and public welfare through the safe use of technology protected by an adaptive legal system. The modern rule of law perspective positions law as an instrument that must be able to keep pace with technological developments through responsive regulations, effective law enforcement, and adequate international cooperation to ensure the security of the digital space and the protection of people's rights.

The reality, however, is different. The growth in internet usage has been accompanied by an increase in various forms of increasingly complex, organized, and transnational cybercrime. A report by the International Telecommunication Union (ITU) indicates that the number of global internet users will exceed 5.5 billion by 2025 (International Telecommunication Union (ITU), 2025), while developments in artificial intelligence, cloud computing, and digital transactions have also increased the potential for cybersecurity vulnerabilities. This phenomenon has resulted in an increase in various cybercrimes such as system hacking, personal data theft, online fraud, ransomware, attacks on critical infrastructure, and technology-based financial crimes. Cybersecurity Ventures data estimates that global economic losses due to cybercrime reach more than USD 10.5 trillion per year and continue to rise (Morgan, 2025a). The borderless nature of cybercrime often challenges national legal systems in the investigation, evidence-based investigation, prosecution, and enforcement of legal decisions.

Indonesia, as one of the countries with the highest digital economic growth in Southeast Asia, faces significant challenges in enforcing cybercrime. The large number of internet users, increasing electronic transactions, and the expansion of the digital platform-based economy have made Indonesia a prime target for various forms of cybercrime (Association of Indonesian Internet Service Providers (APJII), 2024). Various national reports indicate an increase in cases of personal data leaks, ransomware attacks on public and private institutions, digital-based fraud, and misuse of electronic systems. This situation demonstrates that the existence of regulations alone is not enough to ensure effective law enforcement if it is not accompanied by institutional capacity, quality human resources, digital forensic capabilities, and adequate international cooperation mechanisms (Fakhriah & Permata, 2024).

Normatively, Indonesia already has several legal instruments governing cybercrime, including Law Number 11 of 2008 concerning Electronic Information and Transactions and its amendments, Law Number 27 of 2022 concerning Personal Data Protection, the new Criminal Code, and various other sectoral regulations (Government of the Republic of Indonesia, 2022b, 2024b). However, various studies indicate that the implementation of these regulations still faces challenges in the form of overlapping regulations, limited inter-agency coordination, difficulties in digital evidence, and suboptimal cross-border cooperation in addressing transnational cybercrime (Redi & Tegnan, 2024). This situation indicates a gap between the available legal framework and the effectiveness of its enforcement in the field.

Many researchers have conducted studies on cybercriminal law. Some studies focus on the effectiveness of the Electronic Information and Transactions Law in addressing cybercrime in Indonesia (Fakhriah & Permata, 2024). Other studies highlight aspects of personal data protection, digital evidence, and the challenges of law enforcement against transnational criminals. Internationally, several studies have also discussed the success of the United States in developing a digital investigation system through a federal approach supported by the Computer Fraud and Abuse Act (CFAA) (Redi & Tegnan, 2024), as well as Singapore's effectiveness in establishing cybersecurity governance through the Computer Misuse Act and integrated national policies (Clough, 2022). However, most of this research

remains fragmented and isolated, with a limited focus on one country or a specific aspect of cybercrime.

Based on the literature review, several research gaps were identified that serve as an important basis for this research. First, there is an empirical gap in the form of differing research findings regarding the effectiveness of cybercrime regulations in Indonesia. Some studies assess that existing regulations are adequate, while others indicate weak implementation and enforcement. Second, there is a theoretical gap because most studies still use a conventional normative legal approach that fails to comprehensively explain the relationship between legal system design, institutional capacity, and the effectiveness of cybercrime law enforcement in a transnational context. Third, there is a methodological gap because previous research generally only compares Indonesia with one country or focuses solely on regulatory analysis, thus failing to produce a comprehensive reform model based on a comparison of legal systems from countries with different characteristics.

This study attempts to fill this gap through a comparative law approach by comparing the legal systems of Indonesia, the United States, and Singapore in handling cybercrime. The United States was chosen based on its position as a country with a federal legal system and extensive experience in developing cyber law and cyber enforcement. Meanwhile, Singapore was chosen because of its success in building an integrated cybersecurity system and is often used as a model for digital regulation in the Asian region. The comparison of these three countries is expected to provide a more comprehensive picture of the relationship between legal system design, institutional models, law enforcement strategies, and the effectiveness of cybercrime prevention.

The novelty of this research lies in its attempt to formulate a reform model for Indonesian cybercrime law enforcement that focuses not only on regulatory changes but also integrates institutional aspects, law enforcement capacity, national cybersecurity governance, and international cooperation mechanisms. Unlike previous research, which tends to examine the regulations sectorally, this study offers a multidimensional approach that combines legal, institutional, and law enforcement practice analysis through a comparative study of legal systems.

The urgency of this research is growing as the threat of cybercrime escalates, growing faster than the national legal system's ability to adapt. Failure to reform cybercriminal law has the potential to cause significant economic losses, weaken public trust in the national digital system, disrupt cybersecurity stability, and hinder digital transformation, a strategic development agenda for Indonesia. Therefore, a study of cybercriminal law enforcement reform through a comparative study of the legal systems of Indonesia, the United States, and Singapore is crucial to produce evidence-based and relevant recommendations for the development of the Indonesian legal system in the digital era.

Problem Formulation

Based on the background that has been described, the problem formulation in this research is:

1. What are the characteristics of the cyber-criminal law systems in Indonesia, the United States, and Singapore, and what are the similarities, differences, and effectiveness of their implementation in enforcing the law against cybercrime?
2. How can a relevant cybercrime law enforcement reform model be implemented in Indonesia based on the comparative results of the legal systems of Indonesia, the United States, and Singapore?

Writing purpose

This research aims to:

1. Analyze the characteristics of the cyber-criminal law system in Indonesia, the United States, and Singapore, including similarities, differences, and the effectiveness of law enforcement implementation in dealing with the development of cybercrime.
2. Formulating a model for cybercrime law enforcement reform that can be implemented in Indonesia based on the strengths and weaknesses of the legal systems developing in the United States and Singapore.

Benefits of research

1. Theoretical Benefits
   This research is expected to contribute to the development of legal science, particularly in the areas of cybercriminal law, information technology law, and comparative legal systems. Furthermore, it is expected to enrich academic studies on the relationship between legal system design, law enforcement effectiveness, and the challenges of transnational cybercrime.
2. Practical Benefits
   Practically, this research is expected to provide valuable information for lawmakers, law enforcement officials, and institutions authorized to handle cybersecurity issues, as they formulate more adaptive law enforcement policies and strategies to address digital technology developments. The findings are also expected to contribute to improved inter-agency coordination in handling cybercrime.
3. Academic and Social Benefits
   This research can serve as a reference for academics, students, and researchers in developing cybercriminal law and comparative law studies. From a social perspective, this research is expected to contribute to improving public protection from the threat of cybercrime by strengthening a more effective, responsive, and certainty-oriented legal system.

2. METHOD

This research uses an approach, **normative legal research, which** places law as a system of norms (*law in books*) with a focus on legal norms, legal principles, legal doctrines, and legal concepts related to cybercrime law enforcement. The research orientation is directed at analyzing positive law governing cybercrime in Indonesia, the United States, and Singapore to identify the characteristics of each legal system, the effectiveness of its implementation, and the possibility of developing a cybercrime law reform model relevant to Indonesia. The study was conducted without using primary field data, but rather relying on legal materials sourced from regulations, scientific literature, and legal documents relevant to the research object.

Efforts to answer the problem formulation are carried out through the integration of several complementary legal research approaches. **Statute approach used** to examine various regulations that form the basis for regulating cybercrime in each country, such as Law Number 11 of 2008 concerning Information and Electronic Transactions, as last amended by Law Number 1 of 2024, Law Number 27 of 2022 concerning Personal Data Protection, *Computer Fraud and Abuse Act in* the United States, as well as the *Computer Misuse Act* and *Cybersecurity Act in* Singapore. This approach is used to assess the normative construction and scope of cybercrime regulation in each of the legal systems being compared.

The study also uses a **conceptual approach** through the study of various relevant legal theories and doctrines, including Lawrence M. Friedman's Legal System Theory, Soerjono Soekanto's Law Enforcement Theory, Cyber Jurisdiction Theory (*Cyber Jurisdiction Theory*), and Theory *Modified Universalism.* These theories are used as analytical tools to understand the relationship between legal substance, institutional structure, legal culture, cross-border jurisdiction, and the effectiveness of law enforcement against cybercrime, which is increasingly developing transnationally.

In addition, this study uses a **case approach.** Through an analysis of several cybercrime cases that have significance for the development of cybercriminal law, both in Indonesia and in comparison, countries. Some of the cases studied include the ransomware attack on the Temporary National Data Center (PDNS) in Indonesia, the *Colonial Pipeline Ransomware Attack in* the United States, as well as data breach cases at *SingHealth* in Singapore. These cases were analyzed to understand the application of legal norms in practice, the effectiveness of institutional responses, and the various challenges that arise in law enforcement against cybercrime.

The main approach of this research is a **comparative law approach used** to compare the Indonesian cybercriminal legal system with those implemented in the United States and Singapore. Comparisons were made regarding regulatory aspects, institutional structure, digital investigation mechanisms, recognition of electronic evidence, international cooperation, and the effectiveness of legal implementation. Through this approach, the research seeks to identify similarities, differences, strengths, weaknesses, and best practices (*best practices*) which can be used as a reference in strengthening the Indonesian cyber-criminal law system.

Collection of legal materials is carried out through **library research** by utilizing primary, secondary, and tertiary legal materials. Primary legal materials include laws and regulations, international conventions, and official government documents. Secondary legal materials are obtained from books, reputable national and international journal articles, international organization reports, and relevant previous research results. Tertiary legal materials include legal dictionaries, legal encyclopedias, and other supporting sources that help explain the concepts used in the research.

Analysis of legal materials is carried out in a **qualitative** through the stage of identifying legal issues (*issue identification*), legal interpretation (*legal interpretation*), legal reasoning (*legal reasoning*), and comparative legal analysis (*comparative legal analysis.* The results of the analysis are then used to formulate prescriptive conclusions in the form of recommendations for a cybercrime law enforcement reform model that is adaptive to the development of digital technology, capable of responding to the challenges of transnational cybercrime, and still guaranteeing legal certainty and protecting Indonesia's national interests.

The characteristics of cybercrime, which transcend national boundaries, make jurisdictional issues a major challenge in enforcing cybercriminal law. In this context, **Cyber Jurisdiction Theory provides** a conceptual basis that the state's authority to prosecute cybercriminals can no longer be understood narrowly based on traditional territorial principles, but must instead consider the location of the legal impact, the harmed national interests, and the legal relationships arising from the use of cyberspace. This perspective is crucial for explaining the various obstacles Indonesia faces in addressing cybercrime involving perpetrators, victims, and digital infrastructure located in different jurisdictions.

3. LITERATURE REVIEW AND THEORETICAL FRAMEWORK

3.1 The Concept of Cybercrime Law

The development of information and communication technology has resulted in fundamental changes in the lifestyles of modern society, particularly in economic, social, political, and governmental aspects. The increasingly widespread use of the internet has created a digital space that enables various activities to occur without geographical boundaries or national jurisdiction (International Telecommunication Union (ITU), 2025). While this situation provides significant benefits in terms of efficiency and accelerated information exchange, it also presents new threats in the form of increasingly complex and difficult-to-control cybercrimes. This phenomenon poses serious challenges to conventional criminal law, as most traditional legal instruments are designed to address crimes occurring within a country's borders, while cybercrime is cross-border, anonymous, and high-tech (Brenner, 2022).

Recent literature shows that cybercrime has become a global security threat with significant economic, social, and political impacts. According to Yar & Steinmetz (2023), cybercrime is all forms of unlawful behavior that utilize computers, internet networks, or electronic systems as the primary means of committing crimes or as the target of the crime itself. These crimes include illegal access to electronic systems, personal data theft, malware distribution, ransomware, electronic fraud, digital money laundering, identity theft, and attacks on a country's strategic infrastructure.

Morgan's report (2025b) estimates that global economic losses due to cybercrime have reached over USD 10.5 trillion per year. This figure indicates that cybercrime has become one of the forms of crime with the greatest economic impact worldwide. This threat is increasing with the development of artificial intelligence, the Internet of Things (IoT), cloud computing, and digital financial services, which expand the attack surface for public and private information systems (Clough, 2022).

This situation means that cybercriminal law is no longer viewed simply as part of information technology law, but rather as a crucial instrument in maintaining national security, digital economic stability, and protecting human rights in the digital age (Wall, 2023). Therefore, a country's success in addressing cybercrime is largely determined by the ability of its legal system to adapt to rapid and dynamic technological developments.

3.2 Cyber Crime Law Enforcement

The existence of regulations governing cybercrime does not automatically guarantee effective law enforcement. Practical reality shows that the success of cybercrime prevention is greatly influenced by the quality of law enforcement institutions, digital investigative capabilities, forensic laboratory capacity, the availability of competent human resources, and the effectiveness of international cooperation (Europol, 2024). The complexity of cybercrime, which involves multiple national jurisdictions, requires a different approach to cybercriminal law enforcement than conventional criminal law enforcement.

This view aligns with research by Wall (2023), which asserts that the success of law enforcement against cybercrime is determined not only by the existence of legal regulations but also by the ability of state institutions to detect, investigate, identify perpetrators, collect electronic evidence, and conduct judicial proceedings in accordance with technological developments. In this context, the concept of digital evidence is one

of the most crucial elements because almost all cybercrimes produce evidence in the form of electronic data.

A study by Europol (2024) showed that the main challenges in enforcing cybercrime lie in differences in regulations between countries, limited access to data across jurisdictions, and low digital investigative capacity in developing countries (Europol, 2024). These obstacles often lead to delays in the investigation process, reducing the effectiveness of law enforcement efforts.

A modern legal perspective places cybercriminal law enforcement as part of cyber governance, which requires synergy between the government, the private sector, law enforcement agencies, academics, and international organizations. This approach, known as collaborative cybersecurity governance, is currently widely implemented by developed countries such as the United States, Singapore, the United Kingdom, and Australia (Cyber Security Agency of Singapore, 2025).

3.3 Comparative Law

Comparative legal studies is a method widely used in modern legal research to understand the variations in legal systems applied by different countries to regulate the same legal issue. This approach aims to identify similarities, differences, strengths, weaknesses, and potential best practices for implementation in national legal systems (Samuel, 2022).

According to Siems (2022), comparative law no longer merely serves as a means of comparing legal norms but has evolved into a legal policy analysis instrument that enables researchers to understand the relationship between legal culture, institutional structures, and the effectiveness of legal implementation in society (Siems, 2022). This perspective is particularly relevant in the context of cybercrime, as it is a global phenomenon that requires legal harmonization between countries.

The United States and Singapore are often cited as references in comparative studies of cybercriminal law because both countries have successfully developed relatively effective regulatory and institutional systems to address cyber threats (Tan, 2023). The experiences of these two countries provide an opportunity for Indonesia to identify best practices that can be adapted to the characteristics of its national legal system.

3.4 Lawrence M. Friedman's Legal System Theory

The success of a legal system in achieving its intended goals is not only determined by the quality of applicable laws and regulations, but also by the institutional structure and legal culture that develop within society. This perspective was put forward by Lawrence M. Friedman through his legal systems theory, which explains that legal effectiveness is determined by three main components: legal substance, legal structure, and legal culture (Friedman, 2016).

Legal substance refers to the overall legal norms that govern societal behavior. In the context of this research, legal substance encompasses various regulations regarding cybercrime in force in Indonesia, the United States, and Singapore. Legal structure relates to the institutions that carry out law enforcement functions, including the police, prosecutors, courts, and cybersecurity agencies. Legal culture refers to the attitudes, values, and level of societal compliance with the law.

Friedman's theoretical framework is used to analyze why the effectiveness of cybercrime law enforcement in the United States and Singapore is relatively higher than in Indonesia, even though all three countries have regulations governing cybercrime.

3.5 Soerjono Soekanto's Theory of Law Enforcement

Analysis of legal effectiveness cannot be separated from the law enforcement theory proposed by Soerjono Soekanto. According to this theory, the success of law enforcement is influenced by five main factors: legal factors, law enforcement officers, means and facilities, society, and legal culture (Soekanto, 2021).

In the context of cybercrime, resources and facilities are crucial because digital investigations require sophisticated technology and human resources with specialized competencies in digital forensics. The imbalance between the development of crime technology and the capabilities of law enforcement officials is often the cause of the ineffectiveness of cybercrime law enforcement in various developing countries.

3.6 Cyber Jurisdiction Theory

The transnational nature of cybercrime makes jurisdiction one of the most complex issues in cybercriminal law. The perpetrators, victims, servers, communication devices, and legal consequences are often located in different countries, giving rise to conflicts of authority between countries.

According to Svantesson (2024), modern cyber jurisdiction theory emphasizes the importance of an extraterritorial approach, allowing states to prosecute cybercriminals even if some elements of the crime occur outside their territory. This approach is becoming increasingly important in addressing the threats of ransomware, personal data theft, and attacks on strategic infrastructure, which are often carried out through cross-border networks.

4. RESULTS AND DISCUSSION

4.1 Characteristics of the Cyber Criminal Law System in Indonesia, the United States, and Singapore and the Similarities, Differences, and Effectiveness of Its Implementation in Law Enforcement against Cyber Crimes

The massive digital transformation that has taken place over the past two decades has transformed social, economic, and governmental relationships in nearly every country. Along with the increasing dependence on information technology, the threat of cybercrime has evolved into one of the most complex forms of crime, due to its cross-jurisdictional characteristics, exploiting the anonymity of perpetrators, and its ability to cause large-scale losses in a relatively short period of time. This situation has forced countries worldwide to develop cybercriminal legal systems that can provide effective legal protection for the public, public institutions, and the private sector.

From the perspective of Lawrence M. Friedman's Legal System Theory, the effectiveness of a legal system is not only determined by the quality of legal norms (legal substance), but is also influenced by institutional structure and legal culture (Friedman, 1975). Through this theoretical framework, the characteristics of the cybercriminal legal systems in Indonesia, the United States, and Singapore can be analyzed more comprehensively, thus demonstrating the relationship between regulatory design and the effectiveness of its implementation in practice.

1. Characteristics of the Indonesian Cyber Criminal Law System

The main characteristic of Indonesia's cybercriminal legal system lies in the dominance of the legislative approach as the primary instrument in regulating cybercrime. Indonesia's civil law tradition places statutes as the primary source of law, resulting in almost all forms of cybercrime being defined in writing through the Electronic Information and Transactions Law and the Personal Data Protection Law (Government of the Republic of Indonesia, 2022b, 2022a, 2024c, 2024a).

The existence of these two regulations demonstrates that, from a legal substantive perspective, Indonesia already has a relatively adequate legal basis. Regulations concerning illegal access to electronic systems, data theft, manipulation of electronic information, the spread of malware, online fraud, and personal data protection have gained fairly clear normative legitimacy.

The problem that arises lies in the legal structure. The authority to handle cybercrime remains dispersed across various institutions, including the Indonesian National Police, the National Cyber and Crypto Agency, the Ministry of Communication and Digital, the Attorney General's Office, and various other cybersecurity units. This institutional fragmentation often creates coordination issues in detection, investigation, mitigation, and law enforcement.

This phenomenon was clearly evident in the ransomware attack on the Temporary National Data Center (PDNS) in 2024 (National Cyber and Crypto Agency, 2024). The prolonged disruption to public services demonstrates that the existence of regulations has not been fully balanced by institutional readiness and incident response capacity.

2. Characteristics of the United States Cybercriminal Legal System

The characteristics of the United States legal system demonstrate a distinct pattern. The common law tradition and the federal system provide greater scope for legal development through court decisions and law enforcement practices. The Computer Fraud and Abuse Act (CFAA) is the primary instrument for addressing cybercrime, supported by various other sectoral regulations (Legal Information Institute (LLI), 1986).

The United States' primary advantage lies in its integration of regulation, technology, and institutional capacity. The Federal Bureau of Investigation (FBI), the Department of Justice (DOJ), and the Cybersecurity and Infrastructure Security Agency (CISA) have a relatively clear division of duties, enabling effective coordination in handling cybercrime.

Soerjono Soekanto's Law Enforcement Theory perspective demonstrates that law enforcement officers and supporting facilities play a crucial role in the success of law enforcement (Soekanto, 2021). This is reflected in the United States' digital investigative capabilities, particularly in handling ransomware and international data theft cases.

The 2021 Colonial Pipeline case illustrates the effectiveness of this system. Through collaboration between the FBI, the DOJ, and intelligence agencies, the United States government successfully traced the cryptocurrency transactions used by the perpetrators and recovered a portion of the ransom paid (U.S. Department of Justice (DOJ), 2021).

3. Characteristics of Singapore's Cybercriminal Law System

Singapore's success in managing cybersecurity is inextricably linked to its integrated governance approach. The Computer Misuse Act and Cybersecurity Act

serve not only as repressive instruments but also as a foundation for strengthening cyberthreat prevention and mitigation systems (Singapore, 2018, 2020).

The Cyber Security Agency of Singapore (CSA) serves as a national coordination center, connecting various stakeholders within a single cybersecurity policy framework (Cyber Security Agency of Singapore, 2025). This integration allows for rapid decision-making in the event of a security incident.

The SingHealth data breach, which involved approximately 1.5 million patients, sparked major reforms in Singapore's cybersecurity system (Ministry of Communications and Information (MCI) Singapore, 2019). The incident prompted the government to strengthen oversight, security audits, and continuously improve human resource capacity.

Table 1 Comparison of Characteristics of Cyber Criminal Law Systems

Aspect	Indonesia	United States of America	Singapore
Legal System	Civil Law	Common Law Federal	Common Law
Main Regulations	UU ITE and UU PDP	CFAA	CMA and Cybersecurity Act
Institutional Coordination	Separated	Integrated Federal	Centralized
Digital Forensics	Develop	Very Advanced	Proceed
International Cooperation	Currently	Very high	High
Incident Response	Currently	High	High

The most fundamental similarity is seen in the recognition that cybercrime poses a serious threat to national security and the stability of the digital economy. All three countries have criminalized illegal access to electronic systems, data theft, manipulation of electronic information, and various forms of attacks on digital infrastructure.

The existence of electronic evidence has also been recognized in the criminal evidence systems of all three countries. This recognition is crucial because almost all cybercrimes produce digital evidence.

The most significant differences lie in institutional aspects and implementation capacity. Indonesia remains oriented toward a regulatory approach, while the United States and Singapore have developed approaches that integrate regulation, technology, intelligence, and national security.

Table 2: Cybercrime in 2024

Country	Number of Cases	Loss
Indonesia	403 million traffic anomalies	Not yet measured nationally
United States of America	880,418 reports	USD 12.5 billion
Singapore	13,500 reports	SGD 660 million

Source: FBI IC3 Report 2024, BSSN 2024, Singapore Police Force 2024.

From a perspective of **Friedman's Theory, Indonesia's** weaknesses primarily lie in its legal structure and legal culture. Relatively adequate regulations have not been accompanied by strong institutional coordination and a mature digital security culture. In contrast, the United States and Singapore demonstrate a better balance between legal substance, legal structure, and legal culture, resulting in higher levels of effectiveness.

3.2 A Relevant Cyber Crime Law Enforcement Reform Model Implemented in Indonesia Based on Comparative Results of the Legal Systems of Indonesia, the United States, and Singapore

Research findings indicate that the main problem with cybercrime law enforcement in Indonesia is not solely related to a lack of regulation. The existence of various legal instruments governing cybercrime actually demonstrates that the greatest challenges lie in implementation, institutional coordination, and the technical capacity of law enforcement officials.

Perspective: Friedman's Legal System Theory. This demonstrates that legal reform cannot be achieved solely through changes to the substance of the law. Improvements must encompass both the legal structure and legal culture simultaneously. An imbalance between these three components will cause the law to lose its effectiveness in practice (Friedman, 2016).

Table 3: Indonesia's Implementation Gap

Aspect	Conditions in Indonesia	Ideal Conditions
Regulation	Relatively Complete	Integrated
Cyber HR	Limited	Nationally Certified
Forensic Laboratory	Limited	National Connected
Institutional Coordination	Fragmentatif	Integrated
International Cooperation	Not yet optimal	Proactive and Broad

3.3 Model Reformasi Integrated Cybercrime Law Enforcement System (ICLES)

The comparison shows that the most relevant model for Indonesia is not to completely imitate the systems of the United States or Singapore. The characteristics of Indonesia's legal politics, government structure, and legal culture demand an adaptive reform model.

Draft **Integrated Cybercrime Law Enforcement System (ICLES)**What is offered in this research is a synthesis between the United States federal model and Singapore's integrated governance model.

Table 4 ICLES Reform Model

Pillars of Reform	Strategic Program
Regulation	Harmonization of the ITE Law, the PDP Law, and the Criminal Code
Institutional	Cybercrime Coordination Center
HR	National Cyber Investigator Certification

Pillars of Reform	Strategic Program
Technology	National Digital Forensic Center
International Cooperation	ASEAN Cybersecurity Cooperation and MLA

Coordination issues are a major obstacle to enforcing Indonesia's cybercrime law. The United States' experience demonstrates that a clear division of duties between the FBI, DOJ, and CISA can expedite the response to cybersecurity incidents. Singapore's experience also demonstrates that having a single agency with coordinating authority can improve the effectiveness of national cybersecurity governance.

Based on these conditions, the establishment of a Cybercrime Coordination Center is a strategic necessity to integrate the National Cybersecurity Agency (BSSN), the Indonesian National Police (Polri), the Prosecutor's Office (Kejaksaan Prosecutor's Office), the Indonesian Digital Commission (Komdigi), and various related institutions into a single national coordination mechanism. The evolving modus operandi of cybercriminals, which utilizes artificial intelligence, cryptocurrency, and the dark web, has rendered conventional investigative capabilities increasingly inadequate. Colonial Pipeline's experience demonstrates that the success of an investigation is crucially determined by digital forensic capabilities.

The establishment of the National Digital Forensic Center is a relevant step to improve digital investigation and electronic evidence capabilities.

From Friedman's perspective, legal culture is just as important as regulations and institutions. Indonesia's relatively low level of digital literacy contributes to the continued prevalence of various forms of online fraud, phishing, and data theft. A national cybersecurity literacy program needs to be an integral part of cybercrime law reform so that cybercrime countermeasures focus not only on prosecution but also on prevention.

The novelty of this research lies in the formulation of the model. **Integrated Cybercrime Law Enforcement System (ICLES).** This combines the United States' digital investigation-based law enforcement approach with Singapore's integrated cybersecurity governance model. This formulation offers a reform paradigm that focuses not only on changing legal norms but also simultaneously strengthening institutional structures, technological capacity, and legal culture, making it more suited to the needs of the Indonesian legal system in addressing increasingly complex and transnational cybercrime.

5. CONCLUSION

The research results show that the cybercriminal legal systems in Indonesia, the United States, and Singapore have different characteristics as a consequence of differences in legal traditions, institutional structures, and law enforcement policies implemented by each country. Indonesia, which adheres to the cybercriminal legal system, *civil law. While* the United States has a relatively adequate regulatory framework through the Electronic Information and Transactions Law and the Personal Data Protection Law, its effective implementation still faces challenges such as institutional fragmentation, limited digital forensic capacity, and suboptimal inter-agency coordination. Conversely, the United States demonstrates greater effectiveness through its support for digital investigative capacity, integration between law enforcement and cybersecurity agencies, and strong international

cooperation. Singapore demonstrates success through its centralized and integrated cybersecurity governance, enabling it to generate rapid responses to various cyber threats. Similarities between the three countries are evident in the recognition of electronic evidence and the criminalization of various forms of cybercrime, while differences lie in the level of institutional integration, technological capacity, and the effectiveness of legal implementation in practice.

Based on these comparative results, a relevant cybercrime law enforcement reform model for Indonesia should not only focus on regulatory reform but also encompass strengthening institutional structures, increasing human resource capacity, developing digital forensic technology, and expanding international cooperation. *Integrated Cybercrime Law Enforcement System. The* ICLES (Census for Cyber Crimes) formulated in this study is a synthesis of the strengths of the United States and Singaporean systems, adapted to the characteristics of the Indonesian legal system. The integration of legal substance, legal structure, and legal culture, as proposed by Friedman, is a crucial factor in realizing an effective, adaptive, and responsive cybercriminal law enforcement system to the increasingly complex and transnational developments in cybercrime.

6. SUGGESTIONS

Efforts to strengthen Indonesia's cybercrime legal system need to be directed at establishing a national coordination mechanism capable of integrating the roles of the National Cyber and Crypto Agency, the Indonesian National Police, the Attorney General's Office, the Ministry of Communication and Digital, and other relevant institutions within a unified cybercrime handling framework. The development of a national digital forensics laboratory, improving the competence of law enforcement officers through certification programs and ongoing training, and harmonizing regulations related to cybersecurity and personal data protection are urgently needed to increase the effectiveness of law enforcement. Furthermore, strengthening public digital security literacy needs to be positioned as part of a prevention strategy to minimize the risk of cybercrime from the outset.

Expansion of international cooperation through mechanisms, such as *Mutual Legal Assistance*, the exchange of cyber intelligence information, and collaboration in cross-border investigations, also needs to be prioritized in national policy, given the inherently jurisdictional nature of cybercrime. Academics are advised to conduct further research to examine the effectiveness of the Personal Data Protection Law, the use of artificial intelligence in digital investigations, and the development of a cybersecurity governance model tailored to Indonesia's needs in the era of digital transformation. Empirical studies involving law enforcement data and periodic policy evaluations are expected to contribute more comprehensively to the establishment of a modern and sustainable cybercriminal legal system.

6. REFERENCES

Book

Brenner, Susan W. 2022. *Cybercrime and the Law: Challenges, Issues, and Outcomes*. New York: Routledge.

Clough, Jonathan. 2022. *Principles of Cybercrime*. 4th ed. Cambridge: Cambridge University Press.

Friedman, Lawrence M. 2016. *Impact: How Law Affects Behavior*. Cambridge: Harvard University Press.

Samuel, Geoffrey. 2022. *An Introduction to Comparative Law Theory and Method*. 2nd ed. Oxford: Hart Publishing.

Siems, Mathias M. 2022. *Comparative Law*. 3rd ed. Cambridge: Cambridge University Press.

Soekanto, Soerjono. 2021. *Faktor-Faktor yang Mempengaruhi Penegakan Hukum*. Depok: Rajawali Pers.

Svantesson, Dan Jerker B. 2024. *The Digitalisation of Private International Law*. Oxford: Hart Publishing.

Wall, David S. 2023. *Cybercrime: The Transformation of Crime in the Information Age*. Cambridge: Polity Press.

Yar, Majid, dan Kevin F. Steinmetz. 2023. *Cybercrime and Society*. 4th ed. London: Sage Publications.

Journal

Fakhriah, Efa Laela, dan Rika Ratna Permata. 2024. "Challenges of Cybercrime Law Enforcement in Indonesia." *Jurnal Hukum Ius Quia Iustum* 31, no. 2: 233–252.

Permata, Rika Ratna. 2024. "Efektivitas Penegakan Hukum Terhadap Tindak Pidana Siber di Indonesia." *Jurnal Rechtsvinding* 13, no. 1: 45–60.

Redi, Ahmad, dan Hilaire Tegnan. 2024. "Cyber Law Enforcement and Cross-Border Cybercrime Challenges in Indonesia." *Hasanuddin Law Review* 10, no. 1: 25–42.

Rustamaji, Muhammad. 2024. "Comparative Study of Cybercrime Regulation in Southeast Asia." *Yustisia* 13, no. 2: 201–219.

Tan, Eugene K. B. 2023. "Cybersecurity Governance in Singapore: Law, Policy and Institutional Framework." *Asian Journal of Comparative Law* 18, no. 1: 75–91.

Peraturan Perundang-Undangan

Indonesia. **Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik.** Lembaran Negara Republik Indonesia Tahun 2008 Nomor 58.

Indonesia. **Undang-Undang Nomor 19 Tahun 2016 tentang Perubahan atas Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik.** Lembaran Negara Republik Indonesia Tahun 2016 Nomor 251.

Indonesia. **Undang-Undang Nomor 1 Tahun 2023 tentang Kitab Undang-Undang Hukum Pidana.** Lembaran Negara Republik Indonesia Tahun 2023 Nomor 1.

Indonesia. **Undang-Undang Nomor 1 Tahun 2024 tentang Perubahan Kedua atas Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik.** Lembaran Negara Republik Indonesia Tahun 2024 Nomor 1.

Indonesia. **Undang-Undang Nomor 27 Tahun 2022 tentang Pelindungan Data Pribadi.** Lembaran Negara Republik Indonesia Tahun 2022 Nomor 196.

Singapore. **Computer Misuse Act 1993 (Revised Edition 2024).** Singapore Statutes Online.

Singapore. **Cybersecurity Act 2018 (Revised Edition 2024).** Singapore Statutes Online.

United States. **Computer Fraud and Abuse Act (18 U.S.C. §1030).** Amended 2024.

United States. **Cybersecurity Information Sharing Act of 2015.** Amended 2024.

Legislation

Indonesia. **Law Number 11 of 2008 concerning Electronic Information and Transactions.**State Gazette of the Republic of Indonesia 2008 Number 58.

Indonesia. **Law Number 19 of 2016 concerning Amendments to Law Number 11 of 2008 concerning Electronic Information and Transactions.**State Gazette of the Republic of Indonesia 2016 Number 251.

Indonesia. **Law Number 1 of 2023 concerning the Criminal Code.**State Gazette of the Republic of Indonesia 2023 Number 1.

Indonesia. **Law Number 1 of 2024 concerning the Second Amendment to Law Number 11 of 2008 concerning Electronic Information and Transactions.**State Gazette of the Republic of Indonesia 2024 Number 1.

Indonesia. **Law Number 27 of 2022 concerning Personal Data Protection.**State Gazette of the Republic of Indonesia 2022 Number 196.

Singapore. **Computer Misuse Act 1993 (Revised Edition 2024).** Singapore Statutes Online.

Singapore. **Cybersecurity Act 2018 (Revised Edition 2024).** Singapore Statutes Online.

United States. **Computer Fraud and Abuse Act (18 U.S.C. §1030).** Amended 2024.

United States. **Cybersecurity Information Sharing Act of 2015.** Amended 2024.

Official Reports and Documents

Indonesian Internet Service Providers Association (APJII). 2024.*Indonesia Internet Profile 2024*. Jakarta: APJII.

National Cyber and Crypto Agency. 2025.*Indonesia Cybersecurity Annual Report 2024*. Jakarta: BSSN.

Cyber Security Agency of Singapore. 2025. *Singapore Cyber Landscape 2024*. Singapore: CSA.

Europol. 2024. *Internet Organised Crime Threat Assessment (IOCTA) 2024*. The Hague: Europol.

Federal Bureau of Investigation. 2025. *Internet Crime Report 2024*. Washington, DC: FBI.

International Telecommunication Union. 2025. *Facts and Figures 2025*. Geneva: ITU.

Morgan, Steve. 2025. *Cybersecurity Ventures Annual Cybercrime Report 2025*. New York: Cybersecurity Ventures.

Singapore Police Force. 2025. *Annual Scams and Cybercrime Brief 2024*. Singapore: SPF.

U.S. Department of Justice. 2024. *Cyber Digital Task Force Report 2024*. Washington, DC: DOJ.