COMPARATIVE STUDIES ON TRENDS AND STRATEGIES FOR COMBATING CYBERCRIME BETWEEN INDONESIA AND DEVELOPED COUNTRIES

Muhammad Ahfadh Fazlurrohman[1*], Surya Nita[2], Muhammad Erza Aminanto[3]
[1,2]Police Science Study Program, School of Strategic and Global Studies, Universitas Indonesia, Depok, Indonesia
[3]Cyber Security Program, Monash University Indonesia
E-mail: [1)] fazlurrohman.af@gmail.com, [2)] suryanita.sksgui@gmail.com, [3)] erza.aminanto@monash.edu

Abstract
Cybercrime has become a significant global threat, targeting individuals, organizations, and governments with increasing sophistication. This study aims to conduct a comparative analysis of cybercrime trends, patterns, and mitigation strategies between Indonesia and developed countries. Using a Systematic Literature Review (SLR) method, this research highlights the dominance of phishing and ransomware in Indonesia, often exploiting weak digital literacy and regulatory gaps. Conversely, advanced threats like Advanced Persistent Threats (APT) and AI-based malware are prevalent in developed countries, supported by robust cybersecurity infrastructure and international regulations such as the Budapest Convention. The findings emphasize the urgent need for Indonesia to enhance its cybersecurity readiness through technology adoption, legal framework improvement, and public education. This study offers valuable insights into bridging the cybersecurity gap between developing and developed nations, promoting international collaboration for a safer digital ecosystem. Adopting more modern strategies can be an opportunity for Indonesia to enhance its cyber resilience.

Keywords: *Comparative Study, Cybercrime, Cybersecurity, Cyber Threat, Indonesia*

1. INTRODUCTION

Cybercrime refers to all forms of illegal activities conducted through the use of computer technologies and the internet, aiming to harm, steal, or gain unauthorized access to data and systems. This phenomenon encompasses various activities, such as identity theft, system hacking, malware distribution, and ransomware attacks. These actions have evolved significantly due to advancements in technology, with global costs of data breaches reaching $4.45 million on average in 2023 (Global Cybersecurity Index, 2024). Asia, as a rapidly developing region in digital adoption, has seen significant growth in cybercrime alongside internet proliferation, with countries like China, India, and Indonesia experiencing over tenfold increases in internet users since 2002. This digital expansion, while beneficial for economic and social growth, has opened vulnerabilities that cybercriminals exploit, particularly in jurisdictions with weaker cybersecurity frameworks (Broadhurst & Chang, 2012). The rapid evolution of crime-ware and exploit toolkits further exacerbates these challenges, enabling even non-technical actors to execute sophisticated attacks, such as botnets and malware intrusions (Broadhurst & Chang, 2012).

The expanding presence of the internet worldwide has created vast opportunities for innovation and digital transformation. However, this growth has also opened new avenues for cybercriminals to exploit existing security gaps (Broadhurst & Chang, 2012).

Cybercrime not only results in direct financial losses but also damages organizational reputations, threatens individual privacy, and impacts political stability across nations (Zhuravel, 2020). For instance, INTERPOL reports that cyberattacks such as ransomware and phishing are primary methods employed by criminals to target sensitive data and corporate systems in the Asia-Pacific region.

This phenomenon is exacerbated by advancements in sophisticated technologies that equip cybercriminals with tools to expand the reach and impact of their attacks. Ransomware, for instance, has emerged as a global threat, targeting major institutions such as hospitals, educational systems, and governments, with recovery costs increasing annually (Interpol, 2024). On the other hand, the capacity of law enforcement to combat cybercrime often lags behind the rapid evolution of these threats, particularly in developing countries that lack the infrastructure and resources to manage cybersecurity risks effectively (Imran, 2023).

Advancements in information and communication technology (ICT) have created significant opportunities for broader connectivity and efficiency across various sectors, including education, healthcare, and public services. This digital transformation enables faster information exchange, easier access to digital services, and increased economic productivity worldwide (Broadhurst & Chang, 2012). However, the acceleration of digitalization also presents major challenges, such as the heightened risk of cybercrime. Phishing, ransomware, data theft, and Distributed Denial of Service (DDoS) attacks are increasingly frequent threats faced by internet users, both individuals and organizations (Zhuravel, 2020).

One of the most prominent threats is ransomware attacks. These attacks function by encrypting victims' data and demanding a ransom to restore access. The Sophos Research Team (2022) reported that ransomware has become one of the most financially damaging forms of cybercrime. For instance, the "WannaCry" ransomware attack in 2017 crippled hospital systems, businesses, and government institutions in over 150 countries, causing global losses amounting to billions of US dollars. Its impact extended beyond direct financial losses, endangering human lives as critical systems, such as healthcare services, were disrupted (Zhuravel, 2020). The growing prevalence of ransomware has been exacerbated by the widespread adoption of cloud-based technologies, which, while improving efficiency, have also introduced new vulnerabilities that cybercriminals exploit (Imran, 2023). In Indonesia, the complexity of ransomware attacks is amplified by inadequate cybersecurity measures, including insufficient legislation and a lack of skilled cybersecurity professionals, which have created regulatory gaps (Suarmita & Purnomo, 2024). Furthermore, data from the Ministry of Communication and Information Technology highlights that Indonesia remains highly vulnerable, with an alarming rate of cyberattacks directed at critical infrastructure, including the healthcare and financial sectors (Suartana et al., 2022).

In Indonesia, ransomware threats have also been on the rise, particularly with the rapid adoption of digital technology in the public and private sectors. Recent reports from INTERPOL indicate that Indonesia is among the primary targets of phishing and ransomware attacks in the Asia-Pacific region, with high vulnerability stemming from low cybersecurity awareness among internet users (Zhuravel, 2020). Additionally, data theft poses another significant challenge, where sensitive personal and corporate data is often exploited for financial gain or used in subsequent crimes, such as identity fraud (Fauzi et al., 2024).

Given the increasing scale and frequency of threats, the acceleration of digitalization necessitates a more holistic approach to addressing cybersecurity risks. Collaboration between governments, the private sector, and society is essential to enhance awareness and implement more effective digital security systems. Without proactive measures, advancements in ICT risk becoming a double-edged sword, creating even greater opportunities for cybercriminals (Ghelerter et al., 2022).

Globalization and cyber connectivity have created extraordinary opportunities for information exchange and cross-border collaboration. However, the darker side of this phenomenon lies in the expanded scale of cross-border cybercrime. Attacks that were once localized can now easily target victims in other countries, enabled by increasingly interconnected digital infrastructures worldwide (Broadhurst & Chang, 2012). Cybercriminals exploit vulnerabilities in varying security systems across countries, facilitating more complex and harder-to-trace attacks.

In Asia, the surge in internet users over the last decade has significantly increased cybercrime cases. Countries such as Indonesia, China, and India face growing threats due to rapid digital technology adoption unaccompanied by sufficient security improvements (Fauzi et al., 2024). This increase is driven by the use of cloud-based technologies and mobile applications, which are primary targets for phishing, malware, and ransomware attacks (Zhuravel, 2020).

The gap between developed and developing countries in terms of cybersecurity further exacerbates the situation. Developed nations typically possess stronger security infrastructures and more comprehensive regulations. In contrast, developing countries often lack the resources, technical capacity, and adequate regulations needed to address these threats (Ghelerter et al., 2022). For instance, in Southeast Asia, differences in regulations among countries create significant barriers to cross-border collaboration in combating cybercrime (Broadhurst & Chang, 2012).

This phenomenon highlights that globalization not only fosters international collaboration but also creates new opportunities for cybercriminals to exploit regulatory and technological gaps in different countries. Therefore, a more coordinated international approach is essential to reduce cybersecurity disparities and strengthen defenses against cross-border threats (Zhuravel, 2020).

The impact of cybercrime extends beyond direct financial losses, reaching into social and political realms. Cyberattacks can disrupt essential services, erode public trust, and contribute to political instability. In Indonesia, vulnerabilities to cyber threats have affected various sectors, including government institutions, businesses, and the general public. Research by Imran (2023) indicates that data theft and system breaches are frequent issues, hindering the operations and reputations of critical institutions.

These vulnerabilities are increasingly apparent in the digital transformation era, where personal and corporate data have become prime targets. For instance, attacks on government systems have led to the leakage of sensitive data, threatening individual privacy and weakening public trust in governmental institutions (Fauzi et al., 2024). In the business context, ransomware attacks and customer data theft have resulted in significant financial losses and decreased customer loyalty, particularly in trust-dependent sectors such as banking and e-commerce (Interpol, 2024).

Globally, cybercrime has evolved into a political tool, used to intimidate specific groups and perpetuate authoritarian government control. For example, in Azerbaijan, spear-phishing attacks targeting human rights activists and journalists have allowed the

government to access personal information, which was then used to suppress political opposition (Zhuravel, 2020). A similar case occurred in Vietnam, where government-linked hacking groups launched spyware attacks on local human rights activists and the diaspora, aiming to silence criticism of the regime (Zhuravel, 2020).

The social impact of cybercrime also includes a decline in trust in the digital ecosystem. People are becoming increasingly wary of using risky online services, hindering the potential growth of the digital economy in many developing countries. Therefore, collective efforts are needed not only to strengthen digital security but also to raise public awareness of cyber threats and their impacts (Ghelerter et al., 2022). In Indonesia, cybercrime continues to evolve into a serious threat, with various types of attacks frequently occurring, such as data theft, phishing, and malware attacks. Data theft from individuals and institutions has become the most prominent threat, where cybercriminals exploit security gaps in digital systems to access sensitive information. Phishing, one of the most common cybercrime methods, involves deceiving users through fake emails or websites to steal their credentials (Fauzi et al., 2024). Additionally, malware or malicious software is often used to damage systems or steal data without the user's knowledge.

However, the biggest challenge in combating cybercrime in Indonesia lies in the limitations of digital security infrastructure and regulations. Although the Electronic Information and Transactions Law (UU ITE) serves as the primary legal framework for addressing cybercrime, it is often deemed insufficient in dealing with the complexities of modern cyber threats. For instance, UU ITE does not adequately address the development of new security technologies and fails to fully cover cross-border cyberattacks (Fauzi et al., 2024). Law enforcement also faces significant challenges due to limited resources and technical capacity. Many law enforcement officers lack adequate training to handle complex cybercrime cases, hampering investigation and prosecution efforts. Additionally, low digital literacy among the population exacerbates the situation, with internet users often unaware of the risks they face when using digital services (Imran, 2023).

Furthermore, Indonesia's fragmented regulatory framework and the absence of a centralized national cybersecurity agency weaken its ability to respond to evolving threats effectively (Suarmita & Purnomo, 2024). Studies show that the lack of collaboration between government agencies and private sectors hampers the implementation of comprehensive cybersecurity strategies (Tropina et al., 2015). For example, Indonesia’s critical infrastructure, including the banking and healthcare sectors, frequently faces ransomware attacks due to inadequate cybersecurity protocols and insufficient investment in robust defense systems (Suartana et al., 2022). Additionally, cross-border cybercrime investigations are hindered by inconsistent international cooperation and insufficient legal frameworks to prosecute foreign perpetrators (Broadhurst & Chang, 2012). Addressing these gaps requires not only updating legal instruments like UU ITE but also fostering public-private partnerships, increasing international collaboration, and investing in digital literacy programs to create a resilient digital ecosystem in Indonesia (Siregar et al., 2024).

The urgent need to strengthen digital security infrastructure and enhance law enforcement capacity has become increasingly critical. Steps such as specialized training for law enforcement officers, regulatory strengthening through updates to UU ITE, and improving the digital literacy of the public can form part of a sustainable solution. With

a more proactive approach, Indonesia can reduce the risks and impacts of the growing cybercrime threats.

Globally, cybercrime trends continue to show significant increases in line with the development of digital technology and the adoption of internet-based services. Cybercrime has now become a major threat faced by governments, the private sector, and individuals worldwide. Ransomware attacks, one of the most damaging types of cybercrime, have grown rapidly over the past decade. According to research conducted by Zhuravel (2020), the global rate of ransomware attacks has increased by more than 50%, causing financial losses amounting to billions of dollars annually. These attacks not only disrupt operations but also put immense pressure on organizations to pay ransoms to recover their encrypted data. In addition to ransomware, phishing and Distributed Denial of Service (DDoS) attacks have become increasingly common, targeting critical infrastructure and financial institutions, particularly in the Asia-Pacific region (Broadhurst & Chang, 2012).

The COVID-19 pandemic further amplified the frequency and scale of cyberattacks globally, as the rapid shift to remote work and increased online activities introduced new vulnerabilities (Suarmita & Purnomo, 2024). In Indonesia, the adoption of cloud-based services and digital banking has made financial systems a primary target for cybercriminals. A 2023 report by Indonesia's Ministry of Communication and Information Technology highlighted that ransomware and phishing attacks were responsible for nearly 60% of the reported cybersecurity incidents, underscoring the urgent need for robust security measures (Suartana et al., 2022). Despite growing awareness of these threats, many small and medium-sized enterprises (SMEs) lack the resources and expertise to implement effective cybersecurity strategies, leaving them highly vulnerable to sophisticated attacks (Tropina et al., 2015).

To combat these rising threats, international collaboration and the adoption of advanced technologies, such as artificial intelligence (AI) for threat detection and blockchain for securing data, have been recommended as critical strategies (Zhuravel, 2020). However, without sufficient investment in cybersecurity training and awareness, organizations and individuals remain susceptible to evolving cybercrime tactics, which are increasingly leveraging automation and artificial intelligence to scale attacks (Siregar et al., 2024).

In the Asia-Pacific region, cybercrime threats exhibit unique characteristics. Reports from INTERPOL Asia Pacific (Zhuravel, 2020) reveal that phishing and ransomware are the most frequently reported types of cybercrime in this region. Phishing, often conducted through fake emails or websites, targets individuals and organizations to steal sensitive information such as login credentials and financial data. Ransomware, on the other hand, is frequently used to attack critical infrastructure, such as the healthcare and energy sectors, causing devastating impacts.

Additionally, countries in the Asia-Pacific region are often prime targets for cyberattacks due to their high rates of technology adoption and vulnerabilities in digital security systems. In this region, cybercriminals frequently exploit users' lack of awareness about digital security risks and gaps in cybersecurity regulations, which vary significantly between countries (Broadhurst & Chang, 2012). This situation further exacerbates the inability of developing nations in the region to protect their digital systems from increasingly complex attacks.

The global increase in the number and scale of cyberattacks underscores the need for a more coordinated international digital security strategy. Cross-border cooperation, sharing information about threats, and strengthening cybersecurity regulations are critical steps to mitigating the impacts of these growing trends (Fauzi et al., 2024). With a holistic approach, countries can build better digital resilience to counter increasingly complex threats in the modern era.

Comparisons of cyberattack patterns between developed and developing countries show significant differences in the types of threats they face. Developed nations tend to be targets of complex threats, such as advanced persistent threats (APT), which are long-term attacks designed to steal sensitive data or disrupt critical infrastructure. APTs typically involve sophisticated technologies and organized actors, such as state-sponsored hacking groups, targeting government institutions, multinational corporations, and strategic infrastructure (Broadhurst & Chang, 2012). These attacks are often difficult to detect as perpetrators use stealth techniques and advanced methods to evade detection.

Conversely, developing countries like Indonesia are more frequently targeted by high-volume attacks, such as mass phishing, malware, and large-scale ransomware. This is largely due to low levels of digital literacy and inadequate cybersecurity infrastructure (Fauzi et al., 2024). In mass phishing attacks, perpetrators send fake emails or messages to a large number of users, hoping that some will fall victim and disclose sensitive information such as passwords or banking details. The lack of awareness about how to recognize and avoid these threats has resulted in many internet users in Indonesia becoming victims.

Indonesia faces unique challenges stemming from a combination of low digital literacy levels and gaps in security infrastructure. Many internet users in Indonesia lack adequate understanding of the importance of protecting personal data or recognizing cyber threats (Fauzi et al., 2024). Additionally, security systems in many organizations are often not equipped with the latest technologies to defend against cyber threats, enabling cybercriminals to exploit existing vulnerabilities.

These differences highlight the need for tailored approaches to addressing cyber threats in each country. Developed nations require strategies to detect and counter advanced attacks such as Advanced Persistent Threats (APTs), whereas developing nations must focus on improving digital literacy, raising public awareness, and investing in basic security infrastructure. Collaborative approaches involving the sharing of technology and best practices between countries can help reduce the global cybersecurity gap (Zhuravel, 2020).

Studies on global cybercrime trends indicate that the motivations of cybercriminals vary, but financial gain remains the primary driver. Many attacks are designed to steal sensitive data, financial information, or disrupt systems to obtain economic benefits. For example, ransomware has become a key tool used by perpetrators to extort individuals and large organizations. The Sophos Research Team (2022) reported that ransomware attacks in recent years have caused global financial losses amounting to billions of dollars, with recovery costs rising steadily each year.

Beyond financial motivations, politically driven cybercrime is also on the rise, particularly in regions experiencing geopolitical tensions. For instance, targeted attacks on human rights activists in Azerbaijan and Vietnam have employed spear-phishing and spyware techniques to intimidate and silence criticism against the government (Zhuravel, 2020). In Europe, research shows that politically motivated attacks are often carried out

by state-sponsored hacking groups aiming to disrupt stability or influence the policies of other countries (Reep-van den Bergh & Junger, 2018).

Research in Europe highlights the importance of cross-border collaboration in addressing threats that transcend geographical boundaries. Cybercrime knows no borders, making individual efforts by a single country often insufficient to combat organized criminal networks. Initiatives like the Budapest Convention serve as essential frameworks to promote international cooperation in law enforcement against cybercrime (Buçaj & Idrizaj, 2024). Through cross-border collaboration, information sharing, and regulatory harmonization, nations can strengthen collective responses to increasingly complex threats.

Furthermore, a multi-sectoral approach involving governments, the private sector, and civil society is key to effectively mitigating the impact of cybercrime. This includes investing in security technologies, raising public awareness about cyber threats, and developing law enforcement capacities to handle cross-border cybercrime. With these combined strategies, countries worldwide can better address the growing and diverse landscape of cyber threats (Interpol, 2024).

Research in Indonesia indicates that the implementation of cybersecurity regulations still faces numerous challenges. One of the primary issues is the effectiveness of regulations, which often fail to match the complexity of modern cybercrime threats. Although the Electronic Information and Transactions Law (UU ITE) serves as the main legal framework, its implementation is often hindered by inconsistent interpretations and a lack of robust enforcement mechanisms (Fauzi et al., 2024). Additionally, UU ITE does not fully address new forms of cyber threats, such as advanced persistent threats (APTs) or artificial intelligence-based attacks, leaving the regulation lagging behind technological developments (Fauzi et al., 2024).

The lack of resources for law enforcement further exacerbates the situation. Many law enforcement officers in Indonesia lack adequate training to handle complex cybercrime cases. This includes limited understanding of digital investigation techniques, cyber forensic analysis, and methods for addressing cross-border attacks involving international networks (Imran, 2023). As a result, investigations often take longer, and cybercriminals are difficult to prosecute.

Moreover, many law enforcement agencies lack advanced technological infrastructure to detect and prevent cyber threats. This technological gap makes institutions in Indonesia less competitive against hacking groups that employ sophisticated tools and methods to conduct their attacks (Zhuravel, 2020). The situation is further worsened by low levels of digital literacy among the public, who often fall victim to phishing or data theft due to a lack of awareness about the risks they face.

To address these challenges, strategic measures must be implemented, including intensive training for law enforcement officers. This training should cover modern cyber investigation techniques, the use of digital forensic tools, and collaborative approaches to handling cross-border threats. Additionally, significant investment in developing digital security infrastructure is necessary to enhance institutional capacity to combat cybercrime. With these measures, Indonesia can improve the effectiveness of its regulations and response to the ever-evolving cybercrime threats (Broadhurst & Chang, 2012).

Globally, proposed solutions to tackle cybercrime threats include a range of strategic measures, from strengthening regulations to adopting technology-driven

approaches. Regulatory enhancements, such as the enactment of more comprehensive laws and the harmonization of cross-border policies, are essential first steps. For example, the Budapest Convention has served as a key framework for promoting international collaboration in addressing cybercrime, though its implementation remains limited in many developing countries (Buçaj & Idrizaj, 2024). Strong regulations help create a clear legal framework to prosecute cybercriminals while improving coordination among nations.

The implementation of advanced security technologies has also been proposed as a crucial solution. Technologies such as data encryption, artificial intelligence (AI), and machine learning-based threat detection systems are now being adopted to protect digital infrastructure and detect attacks at earlier stages (Zhuravel, 2020). In the Asia-Pacific region, for example, many organizations have started adopting AI-based solutions to analyze attack patterns and identify threats before they cause damage (Zhuravel, 2020). These technologies enable faster and more effective responses to increasingly sophisticated cyber threats.

Moreover, improving public digital literacy is a key element of cybersecurity solutions. Many cyberattacks, such as phishing and ransomware, succeed due to a lack of user awareness about risks and how to avoid such attacks (Fauzi et al., 2024). Therefore, education and public campaigns about the importance of cybersecurity must be conducted extensively to reduce individual and organizational vulnerabilities to attacks.

Collaboration among governments, the private sector, and society is essential to effectively mitigate cybercrime risks. Governments can play a role in establishing policies and regulations, while the private sector has a critical role in developing security technologies. At the same time, society must be engaged through education and awareness initiatives about the importance of safeguarding personal data (Broadhurst & Chang, 2013). With close cooperation among these parties, countries worldwide can build a safer and more resilient digital ecosystem against cyber threats.

Although numerous studies have been conducted to map trends and solutions for cybercrime, there remains a significant gap in comparative analysis between developing and developed countries. Developed nations, such as the United States and European countries, often have stronger cybersecurity infrastructure, well-established regulations, and high levels of public awareness. In contrast, developing countries, including Indonesia, face major challenges, such as limited technological capacity, less comprehensive regulations, and low levels of digital literacy (Fauzi et al., 2024). These differences create a deep gap in the ability of countries to address cybercrime threats.

A comparative approach is essential to understand how countries like Indonesia can learn from global best practices. For example, the Budapest Convention has provided an effective framework for European countries to address cross-border cybercrime. Meanwhile, developed nations have leveraged technologies like AI and blockchain to enhance data security and detect threats more quickly (Zhuravel, 2020). Analyzing the success of these approaches can offer guidance for Indonesia in developing its cybersecurity strategies.

Through a comparison of attack patterns, mitigation strategies, and policy effectiveness, this study aims to provide relevant and in-depth insights. For instance, developed countries face complex threats such as advanced persistent threats (APTs), whereas developing countries are more frequently targeted by high-volume attacks such as mass phishing (Broadhurst & Chang, 2012). By analyzing these patterns, Indonesia

can tailor its strategic actions to focus on the most relevant threats. Furthermore, an evaluation of the effectiveness of global policies can help Indonesia identify regulatory gaps that need to be addressed to strengthen its digital security.

Specifically, Indonesia can learn from the regulatory frameworks and technological advancements of developed countries. For instance, the implementation of comprehensive data protection laws, such as the European Union's General Data Protection Regulation (GDPR), demonstrates the importance of establishing robust legal frameworks to protect sensitive information and enforce accountability (Suartana et al., 2022). Additionally, the adoption of artificial intelligence (AI)-powered threat detection systems, as seen in countries like the United States, highlights the role of technology in enhancing proactive cybersecurity measures (Zhuravel, 2020).

Moreover, developed nations have demonstrated the value of international collaboration in addressing cross-border cybercrime. Initiatives like the Budapest Convention facilitate the sharing of intelligence and harmonization of legal approaches, which could serve as a model for Indonesia to strengthen its cooperation with neighboring countries and global partners (Buçaj & Idrizaj, 2024). By adopting such practices, Indonesia could enhance its capacity to counteract sophisticated cyber threats and build a more resilient digital ecosystem

This approach can also open opportunities for cross-country collaboration, where Indonesia can leverage the experiences and technologies of developed nations to accelerate the development of its digital security infrastructure. By doing so, the cybersecurity gap between developing and developed countries can be narrowed, while simultaneously strengthening global digital resilience (Zhuravel, 2020).

This study aims to conduct a comprehensive comparative analysis of trends, patterns, and approaches to combating cybercrime in Indonesia and globally. By considering differences in social, economic, and digital security infrastructure conditions, the research seeks to uncover how cybercrime characteristics evolve in two distinct contexts: developing countries like Indonesia and developed countries with more integrated cybersecurity systems. This analysis is crucial for understanding how these differences influence the ways countries respond to cybercrime threats.

2. LITERATURE REVIEW

2.1. Introduction to Cybercrime and Cybersecurity

Cybercrime, defined as illegal activities executed through digital technologies and the internet, encompasses threats such as identity theft, ransomware, phishing, and Distributed Denial of Service (DDoS) attacks. These crimes jeopardize not only individuals and organizations but also critical infrastructures, impacting societal, economic, and political stability globally (Zhuravel, 2020). The rapid pace of technological advancement, while enhancing efficiency and connectivity, has simultaneously amplified the sophistication and prevalence of cybercrime, particularly in developing nations where cybersecurity frameworks are often underdeveloped (Broadhurst & Chang, 2012).

In Indonesia, the digital transformation has outpaced the implementation of robust cybersecurity measures. Increased internet penetration, driven by socio-economic initiatives, has inadvertently widened the attack surface for cybercriminals (Suartana et al., 2022). Public skepticism regarding data security, exacerbated by high-profile

incidents such as the e-KTP breach, further highlights the challenges in safeguarding sensitive information (Imran et al., 2024). This contrasts sharply with developed nations that invest significantly in proactive and adaptive cybersecurity strategies, including real-time threat detection and cross-border cooperation (Reda et al., 2023). Addressing this disparity requires understanding the nuanced challenges faced by developing nations and learning from the advanced approaches implemented in developed countries.

2.2. Understanding Cybercrime and Cybersecurity Trends

Global cybercrime trends highlight the escalating sophistication and prevalence of cyber threats, driven by rapid technological advancements. Incidents like the 2017 WannaCry ransomware attack have demonstrated the global scale and impact of these threats, disrupting critical infrastructures in over 150 countries and causing billions of dollars in damages (Zhuravel, 2020). Phishing schemes leveraging social engineering tactics also remain significant, targeting both individuals and organizations. Developed nations have shown greater resilience to such threats due to investments in comprehensive cybersecurity frameworks and strategic technological advancements (Global Cybersecurity Index, 2024). The integration of emerging technologies such as AI and machine learning has bolstered global cybersecurity efforts, enabling predictive analytics and real-time threat detection systems. However, the proliferation of IoT devices and cloud services has expanded the attack surface, highlighting the dual-edged nature of technological innovation and vulnerabilities.

Developed nations have built robust cybersecurity ecosystems supported by advanced technologies and comprehensive regulations. The European Union's General Data Protection Regulation (GDPR) exemplifies global standards for data protection and privacy, while international agreements such as the Budapest Convention foster transnational cooperation to address the complexities of cross-border cybercrime (Buçaj & Idrizaj, 2024). Advanced tools like AI-driven threat detection systems and blockchain technologies provide predictive threat modeling, real-time analytics, and secure data management, reducing risks of fraud and breaches (Reda et al., 2023). Public-private partnerships further enhance these systems. For instance, initiatives like the National Cybersecurity Alliance in the United States demonstrate the impact of coordinated awareness campaigns and innovative solutions. These collaborative efforts, combined with robust technological frameworks, underscore the importance of integrated regulatory, technological, and cooperative measures in achieving comprehensive cyber resilience.

In Indonesia, the fight against cybercrime is fraught with challenges stemming from systemic weaknesses in digital infrastructure, low digital literacy, and limited resources. Sectors such as finance, healthcare, and government are particularly vulnerable, frequently targeted by ransomware and phishing attacks. For example, recent studies show that 69.8% of Indonesian governmental organizations avoid using cloud computing services due to concerns over data security (Imran et al., 2024). The COVID-19 pandemic further exposed these vulnerabilities, accelerating the digital transition across sectors without sufficient investment in robust cybersecurity defenses. Indonesia's regulatory framework, primarily centered on the Electronic Information and Transactions Law (UU ITE), has been criticized for its narrow scope and lack of alignment with international standards. Insufficient cross-border cooperation and inconsistent enforcement further hinder effective responses to transnational cyber threats. Additionally, public distrust in

the security of government-managed data highlights the pressing need for systemic reforms to strengthen Indonesia's cybersecurity resilience (KIC & Ministry of Communication and Information, 2022).

2.3. Previous Research

Indonesia's legal framework, primarily anchored in the Electronic Information and Transactions Law (UU ITE), has been criticized for its inadequacy in addressing advanced cyber threats. The law lacks provisions for managing cross-border incidents and struggles with inconsistent enforcement, further hampered by the limited capacity of law enforcement agencies (Suarmita & Purnomo, 2024). These gaps leave significant vulnerabilities in the nation's cybersecurity defenses. Furthermore, inconsistencies in interpreting and applying existing regulations hinder their effectiveness, highlighting the urgent need for a more comprehensive legal framework that aligns with global standards to combat sophisticated cyber threats.

Technological innovation plays a critical role in mitigating cyber risks, yet Indonesia faces significant barriers to adopting advanced solutions like AI-driven threat detection systems and blockchain technologies. Limited financial resources, a lack of skilled cybersecurity professionals, and inadequate infrastructure restrict the nation's ability to deploy these tools effectively. High implementation costs exacerbate the problem, leaving critical sectors such as finance and healthcare particularly exposed to cyberattacks (Suarmita & Purnomo, 2024). In contrast, developed countries have leveraged these technologies to transform their cybersecurity ecosystems. AI, for instance, enables real-time threat analysis and predictive risk assessments, while blockchain ensures data integrity and reduces vulnerabilities to fraud. Case studies from the United States and Europe highlight the effectiveness of these tools in reducing operational risks and enhancing security (Reda et al., 2023; Zhuravel, 2020).

Collaboration between public and private sectors is equally crucial in addressing the multifaceted nature of cybercrime. However, in Indonesia, limited public-private partnerships and a lack of coordinated efforts hinder the development of effective cybersecurity measures. Building multi-sectoral alliances and fostering international agreements are necessary steps to enhance the nation's ability to combat complex cyber threats (Zhuravel, 2020). Developed nations exemplify the power of collaborative efforts, showcasing initiatives like public awareness campaigns, industry partnerships, and participation in frameworks such as the Budapest Convention. These approaches not only strengthen domestic cybersecurity but also contribute to coordinated global responses against transnational cyber threats. Indonesia's active participation in such initiatives could significantly bolster its capability to address increasingly sophisticated and cross-border challenges.

2.4. Emerging Technologies in Cybersecurity

Emerging technologies, including AI, machine learning, and blockchain, are transforming the landscape of cybersecurity. These technologies enable real-time threat detection, data integrity through decentralized systems, and predictive analytics to preemptively identify vulnerabilities (Reda et al., 2023). Despite their potential, implementing these innovations in resource-constrained environments like Indonesia presents significant challenges.

In Indonesia, barriers such as limited financial resources, a shortage of skilled professionals, and fragmented digital infrastructure hinder the widespread adoption of emerging cybersecurity technologies (Suarmita & Purnomo, 2024). High implementation costs and inadequate training opportunities further exacerbate these issues, limiting the accessibility of advanced solutions like AI-driven threat detection and blockchain-based secure systems.

Addressing these challenges requires coordinated efforts to bridge the resource gap. Strategies such as public-private partnerships, international collaboration, and targeted investments in education and training are crucial. Additionally, fostering local innovation and promoting technology-sharing initiatives can accelerate the integration of emerging technologies, helping Indonesia strengthen its cybersecurity framework.

2.5. Key Insights from Comparative Studies

The comparative analysis of cybersecurity strategies between developed and developing nations reveals critical lessons for Indonesia. Developed nations' emphasis on proactive approaches, such as the integration of AI and robust regulatory frameworks, highlights the importance of forward-looking strategies in mitigating cyber risks. Public-private partnerships and international collaboration further underscore the value of coordinated efforts in addressing global cyber threats (Buçaj & Idrizaj, 2024).

For Indonesia, the key insights include the necessity of aligning national policies with global standards, investing in advanced technologies, and fostering multi-sectoral collaboration. Strengthening digital literacy and public awareness is equally important for building a resilient cybersecurity ecosystem. By learning from the experiences of developed nations, Indonesia can enhance its capabilities to address the unique challenges posed by cybercrime.

3. RESEARCH METHODS

This study employs a qualitative approach using the Systematic Literature Review (SLR) method. This approach aims to identify, analyze, and compare trends, patterns, and cybercrime mitigation strategies in Indonesia and globally, based on relevant literature sources. The method was chosen as it allows for in-depth analysis of various perspectives presented in the literature while providing a systematic foundation to compare global and Indonesian contexts.

3.1. Data Sources

The study relies on secondary data obtained from various sources, including:

1. Scientific journal articles.
2. Reports from international organizations, such as INTERPOL and the World Economic Forum.
3. Policy documents related to cybersecurity.
4. Case studies from various countries, including Indonesia.

The criteria for selecting sources include articles or reports published within the last five years (2018–2023) to ensure they remain relevant to current conditions. The selected studies must explicitly address trends, patterns, or strategies for combating cybercrime.

Additionally, the focus should cover both Indonesian and global contexts to ensure the findings are comparable and align with the research objectives.

3.2. Data Collection Techniques

Data collection was carried out through the following stages:

1. Identification: Articles and reports were searched using keywords like "cybercrime trends," "cybersecurity in Indonesia," and "global cybercrime solutions" in databases such as Scopus, IEEE Xplore, and Google Scholar.
2. Selection: Relevant articles and reports were chosen based on abstracts, keywords, and their relation to the research theme.
3. Classification: Selected literature was categorized into topics such as cybercrime trends, attack patterns, and mitigation strategies.

3.3. Data Analysis Techniques

Thematic analysis was used to identify key themes relevant to the research objectives. Steps in the analysis included:

1. Information Extraction: Extracting key data from the literature, such as types of cybercrime, attack patterns, and mitigation strategies.
2. Systematic Comparison: Highlighting similarities and differences in trends, patterns, and cybercrime mitigation strategies between Indonesia and other countries.
3. Interpretation: Interpreting the results to address research objectives, provide policy recommendations, and contribute to scientific literature.

4. RESULTS AND DISCUSSION

4.1. Research Results

4.1.1. Cybercrime Trends in Indonesia and Globally

Cybercrime is an escalating global issue, with both Indonesia and developed countries witnessing a surge in cyberattacks. The nature of these attacks and the sectors most affected, however, differ significantly between the two regions. In Indonesia, the most prevalent forms of cybercrime include phishing and ransomware. Phishing attacks typically target individuals and organizations in both the public and private sectors, exploiting human vulnerabilities to gain unauthorized access to sensitive information. Ransomware attacks, on the other hand, have become increasingly sophisticated, often disrupting business operations, particularly in the e-commerce sector. These attacks, while impactful, generally involve lower levels of complexity compared to those seen in more developed nations (Interpol, 2023).

In contrast, developed countries, such as the United States, Germany, and others in Europe, face more advanced and targeted forms of cyber threats. These include Advanced Persistent Threats (APTs), which are usually carried out by highly skilled threat actors, often state-sponsored, with the objective of infiltrating critical infrastructure systems. These threats tend to focus on sectors such as energy and healthcare, where the stakes are higher, and the potential damage from a breach can be catastrophic. Moreover, the rise of AI-based malware has added a new dimension to cyberattacks, enabling cybercriminals to execute more adaptive, stealthy, and effective attacks (WEF, 2024).

The financial impact of cybercrime is significant in both regions. In Indonesia, the average financial loss per cyberattack is approximately $4.5 million. While this figure is substantial, it pales in comparison to the losses incurred by developed nations, where the average loss per attack reaches $8.5 million. This disparity highlights the difference in the scale of attacks and the nature of targeted industries, with critical sectors in developed countries bearing a larger financial burden from these attacks (Interpol, 2023; WEF, 2024).

4.1.2. Cybercrime Patterns

In Indonesia, cybercrime often manifests in high-volume, short-term attacks that have immediate and widespread effects. One of the most common forms of these attacks is mass phishing campaigns, where cybercriminals send out thousands or even millions of deceptive emails, hoping to trick recipients into clicking on malicious links or revealing sensitive information. These campaigns are usually less targeted, relying on sheer volume to exploit unsuspecting victims. The success of such attacks in Indonesia can be attributed to several factors, including low public awareness of cybersecurity risks and significant regulatory gaps. The general lack of digital literacy and insufficient security measures among individuals and small businesses make them prime targets for these types of attacks (Cybercrime Atlas, 2024). Additionally, the regulatory framework in Indonesia, although improving, still faces challenges in enforcement and updating laws to keep pace with evolving cyber threats. As a result, cybercriminals often exploit these vulnerabilities to execute mass-scale attacks with minimal repercussions (Cybercrime Atlas, 2024).

In contrast, developed countries experience more sophisticated, targeted cyberattacks, often characterized by Advanced Persistent Threats (APTs). These attacks are designed to be stealthy and to remain undetected within systems for extended periods. APTs are typically carried out by highly skilled attackers, sometimes with state-sponsored backing, and they focus on infiltrating critical infrastructure sectors such as energy, healthcare, and finance. The goal of an APT is not just to cause immediate damage, but to gain long-term access to sensitive data or systems for espionage, financial gain, or disruption. These attacks often employ advanced technologies such as artificial intelligence (AI), which allows cybercriminals to dynamically adapt their tactics to evade detection by conventional security measures. By using AI, attackers can create malware that evolves in real-time, making it more difficult for security systems to identify and neutralize the threat (WEF, 2024).

The contrasting patterns of cybercrime in Indonesia and developed countries highlight the difference in attack complexity, as well as the varying degrees of vulnerability in different regions. While Indonesia is more susceptible to large-scale, low-tech attacks due to systemic issues in digital literacy and regulation, developed countries face more complex, targeted threats that require advanced defense mechanisms and constant adaptation to keep pace with the evolving tactics of cybercriminals (Cybercrime Atlas, 2024; WEF, 2024).

4.1.3. Mitigation Strategies

Developed countries tend to adopt advanced, proactive mitigation strategies that leverage cutting-edge technologies to stay ahead of evolving cyber threats. One of the key strategies employed is the use of Artificial Intelligence (AI)-based technologies, which enhance the ability to detect and respond to cyber threats in real-time. AI allows

security systems to analyze vast amounts of data, identify anomalies, and predict potential cyberattacks before they occur. Additionally, developed nations increasingly implement Zero Trust Architecture (ZTA), a security model that assumes no entity, inside or outside of the network, can be trusted by default. This approach requires continuous authentication and authorization of all users and devices trying to access the system, thus minimizing the risk of breaches. These technologies provide an adaptive, comprehensive defense mechanism that is crucial in a landscape where cyber threats are constantly evolving (WEF, 2024).

In contrast, Indonesia's cybersecurity efforts are still heavily focused on regulatory measures, such as the Information and Electronic Transactions Law (UU ITE). This law aims to create a legal framework for addressing cybercrime, particularly in the areas of digital fraud, privacy violations, and online content regulation. While the UU ITE has been instrumental in establishing a foundational legal framework for cyberspace, its implementation faces significant challenges. One of the main issues is the technical capacity to effectively enforce these regulations, as many law enforcement agencies lack the necessary tools and expertise to address advanced cyber threats. Furthermore, there are concerns about coordination between various government agencies, which sometimes leads to inefficiencies in responding to cybercrimes. Despite these challenges, Indonesia's regulatory approach provides an essential starting point for improving cybersecurity in the country, though more resources and strategic coordination will be needed to enhance its effectiveness (Interpol, 2023).

The following table highlights a comparison of cybersecurity strategies and infrastructure between Indonesia and developed countries, offering a clearer view of the different approaches to mitigating cyber threats.

Table 1. Comparison of Cybersecurity Strategies and Infrastructure Between Indonesia and Developed Countries

No.	Aspect	Indonesia	Developed Countries
1	Dominant Attack Types	Phishing, Ransomware	APT, AI-based Malware
2	Most Affected Sectors	Public and E-commerce	Critical: Energy, Healthcare
3	Financial Loss (USD)	Average $4.5 million per attack	Average $8.5 million per attack
4	Detection Technology	Limited, reliant on the ITE Law	AI, Zero Trust Architecture
5	Main Regulations	ITE Law (2008, revised 2016)	Budapest Convention, GDPR

4.1.4. Comparison of Infrastructure and Regulations

Developed countries exhibit significant advantages in digital security infrastructure. Most organizations in these countries have adopted cutting-edge technologies such as artificial intelligence (AI)-based detection systems and machine learning (ML) to proactively detect and respond to threats. The 2024 Global Cybersecurity Outlook report notes that over 70% of companies in countries like the United States and Germany use AI solutions to detect anomaly patterns indicating malicious cyber activity. In contrast, in Indonesia, the adoption of similar technologies

remains limited. Most organizations still rely on manual solutions or technologies that are less effective in addressing modern cyber threats. This imbalance is due to resource constraints, such as budget and skilled personnel shortages, as well as a lack of investment in cybersecurity training and professional development (WEF, 2024).

In terms of regulation, developed countries have ratified the Budapest Convention, which provides a comprehensive legal framework for handling cross-border cybercrime. This regulation covers aspects such as law enforcement, cyber incident reporting, and international cooperation. Meanwhile, although Indonesia has not ratified the Budapest Convention, several of its principles have been adopted in the Information and Electronic Transactions Law (UU ITE) of 2008, with revisions in 2016. However, the scope of UU ITE remains limited and unable to address more complex cyber threats. Furthermore, developed countries enforce additional regulations, such as the General Data Protection Regulation (GDPR) in the European Union, which not only protects personal data but also mandates that companies report data breaches within 72 hours. On the other hand, the enforcement of UU ITE in Indonesia still faces challenges in terms of consistent implementation and coordination among law enforcement agencies (Interpol, 2023).

Indonesia has significant opportunities to strengthen its infrastructure and regulations by learning from the approaches of developed countries. Adjusting local regulations to address more complex cyber threats, increasing digital literacy, and investing in AI-based detection technologies are strategic steps that can be taken. Additionally, international cooperation, such as active participation in the Budapest Convention or regional alliances like ASEAN CERT, can help Indonesia accelerate the development of a more robust cybersecurity framework. With the right strategies, Indonesia can reduce the gap in infrastructure and regulation, while also enhancing its digital resilience to meet increasingly complex cyber threats (Interpol, 2023; WEF, 2024).

4.2. Discussion

Cybercrime shows significantly different patterns between Indonesia and developed countries. In Indonesia, phishing and ransomware attacks dominate, primarily due to low public digital literacy and the lack of advanced detection technology. In contrast, developed countries such as the United States and Germany face more complex threats like Advanced Persistent Threats (APT) and AI-based malware, which target critical infrastructures such as the energy and healthcare sectors. This difference not only reflects the high dependence of developed countries on digital technology but also their ability to deal with more strategic cyber threats. Meanwhile, Indonesia often faces high-volume attacks that exploit regulatory gaps and low user awareness.

The cybercrime pattern in Indonesia tends to focus on mass attacks like phishing, which are easy to execute and target large numbers of victims. Perpetrators exploit social engineering techniques to deceive victims, often through fraudulent emails or fake websites. In contrast, in developed countries, the attack patterns tend to be more targeted and designed to remain within systems for extended periods. For example, APTs involve well-organized actors who use technologies like AI to avoid detection and modify their attacks according to the security systems they encounter. These patterns show that developing countries are more vulnerable to easy-to-execute attacks, while developed countries become targets of more strategic attacks with broader impacts.

Mitigation strategies in developed countries also show fundamental differences compared to Indonesia. Developed countries tend to adopt advanced technologies like

Artificial Intelligence (AI) to detect and prevent threats early. Approaches like Zero Trust Architecture allow for quick anomaly detection and proactive responses to threats. On the other hand, Indonesia still relies on regulations like the Information and Electronic Transactions Law (UU ITE), which, although important, has limitations in dealing with modern threats. The implementation of strategies in Indonesia is often hindered by a lack of technical resources and coordination between agencies. To bridge this gap, Indonesia needs to integrate more advanced detection technologies while also improving workforce training in the cybersecurity sector.

The difference in digital security infrastructure is also striking between Indonesia and developed countries. Most organizations in developed countries have adopted AI-based systems to detect cyber threats, with over 70% of companies in Europe and the United States using them extensively. In contrast, in Indonesia, the adoption of such technologies is still limited, with many organizations relying on manual detection methods. In terms of regulations, developed countries have ratified the Budapest Convention, which covers cross-border cybercrime. This regulation supports international coordination and consistent incident reporting. Conversely, UU ITE in Indonesia, although having adopted some principles from the Budapest Convention, still faces challenges in coverage and implementation.

Indonesia has a significant opportunity to strengthen its infrastructure and regulations by learning from the approaches of developed countries. The adoption of advanced technologies and the strengthening of international cooperation, such as through ASEAN CERT, can help improve national cybersecurity resilience. Additionally, investment in professional training and increasing digital literacy among the public are key to reducing vulnerabilities to cyber threats. With the right strategies, Indonesia can close the gap with developed countries and strengthen its position in addressing the increasingly complex global cyber threats.

5. CONCLUSION

Cybercrime is an evolving threat with different patterns and impacts between Indonesia and developed countries. In Indonesia, attacks such as phishing and ransomware dominate, while developed countries more often face complex threats like Advanced Persistent Threats (APT) and AI-based malware. This difference reflects gaps in digital literacy, infrastructure readiness, and cybersecurity regulations. The low adoption of advanced technologies and limited technical capacity are major challenges for Indonesia in enhancing resilience to cyber threats.

Developed countries have demonstrated the effectiveness of their strategies through the use of AI-based detection technologies, the Zero Trust Architecture approach, and international regulatory frameworks such as the Budapest Convention. In contrast, Indonesia still relies on regulations like UU ITE, which, while important, has limited coverage in addressing modern cyber threats. To reduce this gap, Indonesia needs to invest more in security technologies, strengthen international cooperation, and promote digital literacy across all levels of society. Through the adoption of more proactive and modern strategies, Indonesia has a significant opportunity to improve its digital resilience. Measures such as strengthening regulations, training the workforce, and fostering cross-border cooperation can help Indonesia address the increasingly complex cyber threats, while also contributing to global efforts to create a secure and resilient digital ecosystem.

REFERENCES

Broadhurst, R., & Chang, L. Y. C. (2012). Cybercrime in Asia: trends and challenges. Handbook of Asian Criminology, 49–63.

Buçaj, E., & Idrizaj, K. (2024). The need for cybercrime regulation on a global scale by the international law and cyber convention. Multidisciplinary Reviews, 8(1), 2025024.

Fauzi, E., Citra, H., Marwenny, E., & Alfitrianti, N. (2024). Control of Personal Data and Cyber Space by Global Digital Platforms in Relation to Indonesia's Digital Sovereignty. Jurnal Ilmiah Ekotrans & Erudisi, 4(1), 149–157.

Ghelerter, D. A., Wilson, J. E., Welch, N. L., & Rusk, J.-D. (2022). Cybercrime in the Developing World.

Imran, M. F. (2023). Cyber Criminology: An analysis of the Indonesian and the United States Police Perception. International Journal of Cyber Criminology, 17(2), 250–261.

Reda, H. T., Anwar, A., Mahmood, A. N., & Tari, Z. (2023). A taxonomy of cyber defence strategies against false data attacks in smart grids. ACM Computing Surveys, 55(14s), 1–37.

Reep-van den Bergh, C. M. M., & Junger, M. (2018). Victims of cybercrime in Europe: a review of victim surveys. Crime Science, 7(1), 1–15.

Siregar, L. H., Fahmi, T., Nasution, I. R., Rozi, F., Harahap, M. T., & Putra, T. D. (2024). Strategi Aman Bertransaksi Digital: Mengedukasi Generasi Milenial Di Era Digital (PKM Desa Medan Krio Kabupaten Deli Serang). Journal Of Human And Education (JAHE), 4(3), 690–695.

Suarmita, I. G. N. A., & Purnomo, H. (2024). Challenges of Hybrid Policing in Countering Online Fraud Networks: A Case Study from Sidrap Regency. Al-Ishlah: Jurnal Ilmiah Hukum, 27(1), 17–30.

Suartana, I. M., Putra, R. E., Bisma, R., & Prapanca, A. (2022). Pengenalan pentingnya cyber security awareness pada umkm. Jurnal Abadimas Adi Buana, 5(02), 197–204.

Tropina, T., Callanan, C., & Tropina, T. (2015). Public–private collaboration: Cybercrime, cybersecurity and national security. Self-and Co-Regulation in Cybercrime, Cybersecurity and National Security, 1–41.

Zhuravel, M. V. (2020). Increasing Your Cybersecurity Awareness: Understanding Cybercrime And Finding Ways To Fight It.

Copyrights