International Law Discourse in Southeast Asia

Volume 4 Issue 1 (June 2025), pp. 1-39
ISSN: 2830-0297 (Print) 2829-9655 (Online)
https://doi.org/10.15294/ildisea.v4i1.20147
Published biannually by the Faculty of Law, Universitas Negeri Semarang, Indonesia and managed by Southeast Asian Studies Center, Universitas Negeri Semarang, INDONESIA

Available online since June 30, 2025

Cyber Victimology and Legal Gaps in Southeast Asia

Zico Junius Fernando✉
Fakultas Hukum Universitas Bengkulu, Bengkulu, Indonesia

Anis Widyawati
Fakultas Hukum Universitas Negeri Semarang, Semarang, Indonesia

Kasmanto Rinaldi
Universitas Islam Riau

✉Corresponding Email: zjfernando@unib.ac.id

ABSTRACT: Cybercrime is escalating in Southeast Asia alongside rapid digital growth, yet the region still lacks a unified legal and victim-centered approach. While most studies focus on perpetrators and cybersecurity, this research addresses a critical gap by exploring Cyber Victimology as a framework to understand and strengthen victim protection in ASEAN countries. Using a normative legal method with comparative and conceptual approaches, this study examines legal disparities, weak law enforcement, limited victim support, and low digital literacy, particularly among children and the elderly. Findings show that ASEAN lacks harmonized regulations, adequate cyber policing, and psychological-legal support infrastructure. For instance, Singapore's robust Personal Data Protection Act contrasts with minimal protection in Cambodia and Laos. The study proposes concrete policy responses, including regional legal harmonization modeled on the Budapest Convention and the GDPR, enhanced law enforcement capacity, national crisis centers, and targeted digital literacy programs. Integrating Cyber Victimology into policy will help ASEAN establish a more inclusive, victim-responsive digital governance system.

KEYWORDS: *Cybercrime, Cyber Victimology, Southeast Asia, Legal Frameworks, Digital Literacy.*

I. INTRODUCTION

The advancement of information and communication technology has brought significant changes to various aspects of global society.[1] Amid the rapidly evolving era of digitalization, cybercrime has emerged as a significant challenge faced by communities, particularly in Southeast Asia. This region, known as one of the fastest-growing areas for internet users globally, had over 400 million internet users in 2024, according to the Digital 2024 Southeast Asia.[2] The high internet penetration rates, reaching 75% in countries like Singapore, Malaysia, and Thailand, present substantial opportunities for digital economic growth while simultaneously increasing the risks of cybercrime.

Cybercrime, encompassing offenses such as hacking, online fraud, identity theft, cyber harassment, and online child sexual exploitation, has become a serious threat in the region. Data from Interpol indicates that during the COVID-19 pandemic, cyberattacks in Southeast Asia increased by more than 50%. Crimes such as phishing, ransomware, and online child exploitation were the most prevalent.[3] This phenomenon demonstrates that Southeast Asia is not only a target for cybercrime but also a region with a growing number of victims. However, attention to the protection of cybercrime victims remains relatively limited compared to efforts to prosecute offenders. This

---

1 Ayu Puspita and Anik Nur Handayani, "Dampak Teknologi Digital Terhadap Perilaku Sosial Masyarakat 5.0," *Jurnal Inovasi Teknologi Dan Edukasi Teknik* 2, no. 10 (2022): 446–51, https://doi.org/10.17977/um068v2i102022p446-451.

2 Statista, "Internet Usage in Southeast Asia - Statistics & Facts," www.statista.com, 2024.

3 Abdul Hanief Amarullah, Arthur Josias Simon Runturambi, and Bondan Widiawan, "Analisis Ancaman Kejahatan Siber Bagi Keamanan Nasional Pada Masa Pandemi COVID-19," *Jurnal Kajian Stratejik Ketahanan Nasional* 4, no. 2 (2021): 17–28, https://doi.org/10.7454/jkskn.v4i2.10052.

highlights the relevance of Cyber Victimology as a branch of study to be developed in Southeast Asia, with a focus on victims' rights.[4]

The main challenge in protecting cybercrime victims in Southeast Asia lies in the legal and policy gaps among countries in the region. Some countries, such as Singapore, have relatively advanced legal frameworks, such as the Personal Data Protection Act (PDPA), which protects citizens' personal data.[5] On the other hand, countries like Cambodia and Laos have inadequate regulations to address cybercrime, leaving victims often without proper justice. These regulatory disparities create gaps in victim protection and hinder regional efforts to combat cybercrime effectively.

Furthermore, the lack of regional harmonization poses a significant obstacle to cross-border collaboration in protecting victims. While ASEAN has initiated frameworks such as the ASEAN Cybersecurity Cooperation Strategy, the implementation of these policies is hampered by inconsistent priorities and technical capacities among member states. For example, in cross-border crimes like online child trafficking, the lack of coordination among ASEAN countries often makes it difficult to trace perpetrators and provide adequate recovery for victims.

Law enforcement in the region also faces significant challenges. Many countries in Southeast Asia, such as Myanmar and the Philippines, lack adequately trained cyber police units and sufficient technical infrastructure. A report by UNODC highlights that limited human

---

[4] K Jaishankar, "Cyber Victimology: A New Sub-Discipline of the Twenty-First Century Victimology BT - An International Perspective on Contemporary Developments in Victimology: A Festschrift in Honor of Marc Groenhuijsen," in *An International Perspective on Contemporary Developments in Victimology*, ed. Janice Joseph and Stacie Jergenson (Cham: Springer International Publishing, 2020), 3–19, https://doi.org/10.1007/978-3-030-41622-5_1.

[5] Nadine Tong and Emma Leung, "An Analysis of the Amendments to Singapore's Personal Data Protection Act," www.durhamasianlawjournal.com, 2022.

and technological resources are significant obstacles in identifying, investigating, and prosecuting cybercriminals. This directly impacts the legal system's inability to deliver justice to victims. For instance, cases of online harassment in Indonesia often go unaddressed due to a lack of sufficient technical evidence, leaving victims with deep psychological trauma. Another significant challenge is the lack of psychological and legal support for cybercrime victims. Many victims feel neglected by the legal system due to slow court processes and the difficulty of proving cyber offenses. A study by Singapore's Cyber Security Agency (CSA) found that over 40% of online harassment victims were reluctant to report their cases due to a lack of support from authorities. This demonstrates that victims' needs are often overlooked in efforts to address cybercrime.

In this context, integrated and comprehensive solutions are crucial to overcoming the challenges of protecting cybercrime victims in Southeast Asia. One step is to enhance national and regional regulations. Southeast Asian countries need to develop more specific legal frameworks to address cybercrime and protect victims. For example, adopting strict data protection principles, as implemented by the European Union's General Data Protection Regulation (GDPR), could serve as a model for countries in the region.[6]

Regional harmonization is also a strategic step that must be pursued. ASEAN can play a key role in drafting standardized regional regulations for protecting cybercrime victims. The Budapest Convention on Cybercrime can serve as a reference for establishing

[6] Sebastian Weise, Franziska Rinke, and Aishwarya Natarajan, "Dawn of a New Era of Global Data Protection?," *Völkerrechtsblog*, March 2021, 1–3, https://doi.org/10.17176/20210302-153629-0.

an effective regional legal framework.[7] Additionally, training law enforcement officers in digital forensics and cyber analysis should be improved. Collaboration among ASEAN countries in sharing resources and technology can also enhance the region's law enforcement capacity.

On the other hand, psychological and legal support for victims must be strengthened. Each country should establish mechanisms to assist cybercrime victims, including psychological counseling services, free legal aid, and online reporting centers. Singapore, with its Cyber Security Agency (CSA), can serve as an example of providing accessible support for victims.[8] Moreover, digital literacy campaigns and education on cybercrime risks should be promoted, particularly among vulnerable users such as children and the elderly. This is essential for raising public awareness of digital risks and promoting more effective preventive measures.

By understanding these challenges and adopting integrated solutions, Southeast Asia has a significant opportunity to create a more just and effective legal system for protecting cybercrime victims. A Cyber Victimology-based approach not only emphasizes victims' rights but also promotes strengthening a legal system that is more responsive to the development of digital technology. Close collaboration among ASEAN countries, increased law enforcement capacity, and enhanced support for victims can be key to addressing

---

[7] Karpagapriya, "An Evaluation of the Jurisdictional Aspects of Cyber Crimes Under the Regional Agreements with Special Emphasis on the Budapest Convention," *IJFMR - International Journal For Multidisciplinary Research* 5, no. 6 (November 2023): 1–6, https://doi.org/10.36948/IJFMR.2023.V05I06.9365.

[8] Fabio Cristiano, "Singapore : A Leading Actor in ASEAN Cybersecurity," in Routledge Companion to Global Cyber-Security Strategy (Routledge, 2021), 381–91, https://doi.org/10.4324/9780429399718-35.

these challenges and creating a safer digital environment for the people of Southeast Asia.

The urgency of addressing cybercrime in Southeast Asia cannot be overstated. The region stands at a critical juncture where increasing internet penetration is not matched by adequate legal protection for victims, resulting in a widening gap in justice. Previous studies have primarily concentrated on cybersecurity threats, digital infrastructure, or offender profiling, with limited focus on the victim's experience within legal systems. For example, Jaishankar (2020) emphasized the need for a new sub-discipline, Cyber Victimology, to understand the unique vulnerabilities of digital victims.[9] Scott N. Romaniuk (2021) highlighted how victims of online abuse often fall through legal loopholes in developing countries.[10] Meanwhile, Smith (2024) identified the challenge of legal harmonization in Southeast Asia but lacked a victim-centered perspective.[11] This study advances the discourse by applying a Cyber Victimology lens to examine not only the legal gaps but also the systemic weaknesses in law enforcement, victim support, and digital literacy across ASEAN. Its contribution lies in offering an integrated analysis and concrete policy proposals rooted in both regional dynamics and global best practices. Specifically, this research seeks to

---

[9] K. Jaishankar, "Cyber Victimology: A New Sub-Discipline of the Twenty-First Century Victimology," *An International Perspective on Contemporary Developments in Victimology: A Festschrift in Honor of Marc Groenhuijsen*, January 2020, 3–19, https://doi.org/10.1007/978-3-030-41622-5_1.

[10] Scott N. Romaniuk and Mary Manjikian, "Routledge Companion to Global Cyber-Security Strategy," *Routledge Companion to Global Cyber-Security Strategy*, January 2021, 1–632, https://doi.org/10.4324/9780429399718/ROUTLEDGE-COMPANION-GLOBAL-CYBER-SECURITY-STRATEGY-MARY-MANJIKIAN-SCOTT-ROMANIUK/RIGHTS-AND-PERMISSIONS.

[11] Robert Brian Smith, "Complexity of Legal Harmonisation in Southeast Asia: A Diversity of Legal Systems & Languages," *Athens Journal of Law* 10, no. 2 (April 2024): 233–54, https://doi.org/10.30958/AJL.10-2-4.

answer: (1) What legal and institutional gaps hinder the protection of cybercrime victims in Southeast Asia? (2) How can regional harmonization and a Cyber Victimology framework be utilized to improve victim protection and digital resilience? Through these questions, the study aims to contribute to the development of a more inclusive and responsive legal system for digital society in Southeast Asia.

II. METHODS

This study adopts a normative legal research method combined with comparative and conceptual approaches to examine the protection of cybercrime victims in Southeast Asia.[12] The normative approach is used to analyze the content of existing legal norms, statutes, and regulatory frameworks related to cybercrime and victim protection, particularly in countries such as Singapore, Malaysia, Indonesia, Thailand, Cambodia, and Laos. The comparative approach enables the study to contrast the legal frameworks of these ASEAN member states with international standards such as the Budapest Convention on Cybercrime and the European Union's General Data Protection Regulation (GDPR), to identify legal disparities and draw out best practices suitable for regional harmonization. Furthermore, the conceptual approach is applied to explore the theoretical underpinnings of Cyber Victimology, which serves as an analytical lens for understanding the socio-legal positioning of cybercrime victims, especially those from vulnerable groups. All data used in this study were obtained through desk research, consisting of legal texts, international reports (e.g., from UNODC, Interpol, ASEAN),

[12] Zico Junius Fernando, Kiki Kristanto, and Ariesta Wibisono Anditya, "Knitting Democracy, Separating Restraints: Legal Reform and a Critical Analysis of Article 256 of the New Criminal Code and Its Impact on Freedom of Speech," *Journal of Law and Legal Reform* 5, no. 2 (April 2024): 555–86, https://doi.org/10.15294/JLLR.VOL5I2.1670.

academic publications, and documented case studies. This study does not employ empirical methods such as interviews, surveys, or field observations. As such, its findings are based entirely on secondary sources and doctrinal legal analysis. While this limits the research in terms of direct stakeholder perspectives or quantitative victim data, it allows for a focused legal and theoretical evaluation of how Southeast Asian countries regulate and respond to cybercrime from a victim-centered perspective.

III. LEGAL GAPS IN THE PROTECTION OF CYBERCRIME VICTIMS

Legal disparities among Southeast Asian countries pose a significant barrier to protecting cybercrime victims. Some countries, such as Singapore, have adopted comprehensive legal frameworks like the Personal Data Protection Act (PDPA).[13] However, countries like Laos and Cambodia lag behind in terms of cyber regulations, leaving many victims without adequate protection. Additionally, differing legal definitions of cybercrime across countries complicate law enforcement processes, particularly in cross-border cases. For instance, online child trafficking cases in Indonesia involving international networks are often hindered by a lack of legal harmonization with other countries.

These legal gaps in Southeast Asia stem from varying legislative approaches to protecting cybercrime victims. Countries like Singapore and Malaysia have made significant progress by introducing laws specifically targeting cyber threats and victim protection. Singapore, through the Cybersecurity Act 2018 and the

[13] Vijaykumar Shrikrushna et al Chowbe, "Beyond Borders : Addressing the Legal Quagmire of Jurisdiction in Cyberspace," *IJFMR - International Journal For Multidisciplinary Research* 6, no. 6 (November 2024): 1–19, https://doi.org/10.36948/IJFMR.2024.V06I06.30051.

PDPA, has implemented stringent data protection standards, providing greater security to individuals and organizations affected by cybercrimes. In contrast, countries like Laos and Cambodia are still in the early stages of developing legal frameworks to address cybercrime. This discrepancy creates a considerable gap in the capacity of countries within the region to combat cyber threats effectively.

These differences become even more pronounced when examining the issue of cybercrime definitions. In many cases, the lack of uniformity in definitions among Southeast Asian countries leads to confusion in law enforcement, particularly for cross-border crimes. For example, what may be classified as a data breach in one country might not be considered a serious offense in another. This inconsistency creates legal loopholes that cybercriminals often exploit to evade arrest and prosecution.

For example, a report from ECPAT Indonesia covering the period from 2020 to 2022 highlights a significant increase in cases of online sexual exploitation of children. These cases involve various forms of crimes, such as the distribution of Child Sexual Abuse Material (CSAM), child trafficking for sexual purposes, and sexual harassment conducted via digital platforms, including social media, messaging apps, and specific websites. The "Disrupting Harm" study, released in 2022, provides additional data on this phenomenon, revealing that 2% of internet users aged 12–17 in Indonesia have been victims of serious cases of online exploitation and sexual harassment. This research underscores the various methods used by perpetrators, ranging from manipulation to coercion through digital platforms, targeting this vulnerable age group.[14] The Indonesian Child

[14] ECPAT, "Catatan Akhir Tahun ECPAT Indonesia 2023 : Keberlanjutan Perlindungan Anak Dari Eksploitasi Seksual," ecpatindonesia.org, 2023.

Protection Commission (Komisi Perlindungan Anak Indonesia, KPAI) recorded 481 reported cases of online prostitution or online exploitation during the 2021–2023 period. These cases highlight the prevalence of such crimes, yet they are believed to represent only a fraction of the true scale of the issue. This phenomenon is often referred to as the "tip of the iceberg," as many cases remain unreported, reflecting the significant challenges in detecting and addressing online exploitation comprehensively.[15] These findings illustrate the complexity of online child sexual exploitation in Indonesia without drawing specific conclusions regarding solutions or impacts. The case of online child trafficking in Indonesia further demonstrates how legal gaps can hinder the pursuit of justice. In such cases, international networks involved in the sexual exploitation of children utilize digital platforms to carry out their actions. However, the lack of legal coordination with other countries within these networks causes delays in law enforcement processes. Despite having relatively strict laws on child protection, Indonesia faces significant challenges in extraditing perpetrators operating from countries with weak cyber regulations.

Additionally, legal gaps significantly affect the protection of cybercrime victims. Victims often fail to receive adequate remedies due to the insufficiency of existing legal frameworks in addressing their needs. In countries with weak cyber regulations, victims frequently lack access to legal mechanisms that could facilitate justice or recovery. This creates barriers for victims in seeking redress or protection. Conversely, in countries like Singapore, the legal framework includes efficient reporting mechanisms and provides

[15] M. Iqbal Al Machmudi, "481 Kasus Eksploitasi Anak Secara Daring, Transaksi Dengan Kripto," mediaindonesia.com, 2024.

comprehensive support for victims. These supports range from psychological counseling to legal assistance, ensuring that victims have access to the resources needed to address their circumstances. This disparity highlights how the strength or weakness of cyber regulations in different countries directly influences the level of protection and assistance available to victims.

The lack of legal harmonization is a significant obstacle to regional efforts in addressing cybercrime in Southeast Asia. ASEAN, as a regional organization, has attempted to tackle this challenge through initiatives such as the ASEAN Cybersecurity Cooperation Strategy, aimed at enhancing cooperation among member states to counter cyber threats.[16] However, the implementation of this framework continues to face various challenges, particularly differences in national priorities and technical capacities among member states. Some countries in the region have more advanced regulations and infrastructure, while others lag in developing cyber laws and technical resources. These disparities hinder effective collaboration, especially in addressing cross-border cybercrime. Legal harmonization among countries in the region is crucial to ensure that cybercrime can be addressed collectively, perpetrators can be prosecuted without jurisdictional barriers, and victims receive equal protection across Southeast Asia.

IV. LACK OF LAW ENFORCEMENT CAPACITY IN SOUTHEAST ASIA

Law enforcement in Southeast Asia faces significant challenges in combating cybercrime. One of the primary issues is the lack of trained cyber police units and adequate technical infrastructure. According

[16] Smith, "Complexity of Legal Harmonisation in Southeast Asia: A Diversity of Legal Systems & Languages."

to a report by the United Nations Office on Drugs and Crime (UNODC), criminal groups in the region are increasingly leveraging advanced technologies such as artificial intelligence (AI) and deepfakes in their operations, resulting in financial losses of up to USD 37 billion (approximately IDR 575 trillion) in 2023.[17] Furthermore, data from the National Cyber Security Index (NCSI) indicates that several countries in Southeast Asia rank low in terms of cybersecurity. For instance, Indonesia ranks 6th in Southeast Asia and 83rd globally out of 160 countries assessed.[18] These limitations result in many cybercrime cases remaining unresolved, allowing perpetrators to frequently evade justice. The low level of cybersecurity also leaves countries in the region vulnerable to increasingly sophisticated cyberattacks, while law enforcement capacity struggles to keep pace with the technological advancements utilized by cybercriminals.

Myanmar and the Philippines serve as two examples of countries facing significant challenges in this regard. Myanmar is still in the early stages of developing its cyber police capacity, with limited resources and expertise dedicated to addressing cybercrime. In contrast, the Philippines has established some cyber police units; however, these units often struggle to handle cases involving advanced technologies such as ransomware or botnet-based attacks. The primary factor contributing to these difficulties is the limited technical infrastructure available in both countries, which hinders their ability to investigate and respond to complex cyber threats effectively.

---

[17] kumparanNEWS, "Penipuan Sindikat Kriminal Asia Tenggara Gencar Pakai AI, Bisa Raup Rp 575 T," kumparan.com, 2024.

[18] Vika Azkiya Dihni, "Keamanan Siber Indonesia Peringkat Ke-6 Di Asia Tenggara," databoks.katadata.co.id, 2022.

In 2023, Malaysia experienced a significant increase in cyberattacks targeting various sectors. A report by Ensign InfoSecurity revealed that nearly 40% of cyberattacks in Malaysia involved the manufacturing and government sectors, with manufacturing accounting for 20% and government 18.2% of the incidents.[19] Additionally, a study by Palo Alto Networks indicated that 78.4% of Malaysian companies experienced at least one cyberattack in the past year, with over 55% facing attacks on a monthly or weekly basis.[20] In these cases, hackers successfully stole sensitive data from several major companies, including customer data and financial information. Although the Malaysian government attempted to address the incidents, the lack of digital forensic capabilities caused the investigations to progress slowly, allowing the perpetrators to escape without leaving sufficient traces for further pursuit. In 2023, Cambodia garnered significant attention due to the surge in online scam cases involving Indonesian citizens (WNI). Many Indonesians were enticed by job offers promising high salaries as customer service operators or call center agents in Cambodia. However, upon arrival, they were coerced into working as scammers, defrauding fellow Indonesians through various online fraud schemes.[21]

Southeast Asia continues to face profound challenges in combating cybercrime, primarily due to the limited capacity of its law enforcement institutions. A critical obstacle lies in the insufficient training of law enforcement personnel in handling cyber-related offenses. Many officers across ASEAN member states lack the

[19] Astro Awani, "Hampir 40 Peratus Serangan Siber Di Malaysia Libatkan Akaun Pembuatan, Sektor Kerajaan Pada 2023," www.astroawani.com, 2024.
[20] Astro Awani, "Majoriti Syarikat Malaysia Alami Serangan Siber Pada 2023," astroawani.com, 2024.
[21] Danu Damarjati, "11 WNI Di Kamboja: Dipaksa Scamming Tipu Sesama Hingga Dijemput Polisi," news.detik.com, 2023.

technical expertise required to investigate complex cybercrimes, such as ransomware attacks, phishing schemes, and cryptocurrency-related fraud. Existing training programs, where available, often provide only basic information technology knowledge, without a specialized curriculum in digital forensic science or cyber investigation methods. This results in many cases being mishandled or left unresolved, directly impacting victims who are denied access to justice, restitution, or protection from re-victimization. The problem is further compounded by the lack of regional cooperation. Although ASEAN has introduced frameworks aimed at fostering cross-border collaboration, such as the ASEAN Cybersecurity Cooperation Strategy, implementation has been weak due to political sensitivities, capacity disparities, and a lack of resource-sharing protocols. This has made it exceedingly difficult to conduct coordinated responses to transnational cybercrime cases, especially those involving online human trafficking, financial scams, and data breaches. For example, the 2023 online fraud cases in Cambodia involving dozens of Indonesian citizens exposed the inability of local law enforcement to act promptly, due to a lack of cross-border legal mechanisms and digital forensic infrastructure. Victims who were lured with fake job offers and later forced to operate cyber scams were often left without institutional support or proper mechanisms for rescue and repatriation.

To address these gaps, strategic reforms must be adopted both at the national and regional levels. First, ASEAN countries must develop mandatory and standardized training programs for law enforcement personnel, focusing on digital forensics, evidence preservation, blockchain analysis, and cyber-investigation protocols. This training should be coordinated regionally, under the ASEAN Secretariat, with

technical support from international bodies like INTERPOL, UNODC, and EUROPOL to ensure consistency and mutual recognition of skills. Second, governments must establish specialized cybercrime units within their national police forces. These units should be equipped with modern investigative tools, including data recovery systems, encrypted storage facilities, and cyber threat intelligence platforms.

Moreover, investment in infrastructure is essential. Each country should build national digital forensic laboratories, set up 24/7 online complaint platforms for victims, and develop secure inter-agency communication channels for real-time information exchange. Singapore, which has demonstrated leadership in the region through its Cyber Security Agency (CSA) and robust implementation of the Personal Data Protection Act (PDPA), can play a mentoring role in supporting less-equipped countries such as Laos, Myanmar, and Cambodia. Finally, ASEAN must develop and implement binding protocols for cybercrime response, enabling joint investigations and facilitating rapid mutual legal assistance. Without these institutional, legal, and technological reforms, Southeast Asia will remain highly vulnerable to escalating cyber threats. More importantly, victims, especially from vulnerable groups such as women, children, and migrant workers, will continue to suffer without adequate legal recourse, protection, or support.

V. LACK OF PSYCHOLOGICAL AND LEGAL SUPPORT FOR VICTIMS

Many victims of cybercrime in Southeast Asia feel neglected by the legal system. The slow judicial process and the challenges in proving online offenses often deter victims from reporting their cases. A study conducted by SG Her Empowerment (SHE) in Singapore revealed that 38% of respondents had personally experienced some form of

online harm. Among those who encountered harmful online content or conduct, 26% faced sexual harassment or cyberbullying. This indicates a significant gap in victim support systems, both in terms of legal assistance and psychological rehabilitation.[22] In response to these challenges, Singapore has announced plans to establish a dedicated government agency to support victims of online harms and enhance online safety.[23] This agency aims to provide timely relief for victims and promote responsible behavior online. These findings highlight the need for more effective support mechanisms to encourage victims to come forward and seek the help they need.

The lack of legal support often stems from the insufficient availability of legal aid services provided by governments or non-governmental organizations in many Southeast Asian countries. In numerous cases, victims are unaware of their rights or how to effectively report their cases. Additionally, the lengthy and complex court processes leave many victims feeling frustrated, leading them to abandon their cases. From a psychological perspective, many victims of cybercrime experience deep trauma resulting from incidents such as online harassment, identity theft, or the unauthorized dissemination of private content. However, psychological support services for cybercrime victims remain highly limited in most Southeast Asian countries. Many nations lack crisis centers or specialized counseling services for cybercrime victims. As a result, victims are often left to cope with the psychological impact of these crimes on their own.

For example, in Indonesia, although there are some organizations providing assistance services for victims, their numbers remain very

[22] SG Her Empowerment, "SHE Study Reveals Majority of Online Users Have Experienced Online Harms," www.she.org.sg, 2023.
[23] MDDI, "New Agency for Online Safety and Assurance," www.mddi.gov.sg, 2024.

limited compared to the existing needs. Moreover, these services are often only available in major cities, leaving victims in rural or remote areas without access to the support they require. Similarly, in the Philippines, the availability of support services for cybercrime victims is largely concentrated in metropolitan areas such as Manila and Cebu. This urban-centric distribution means that individuals in provincial regions may struggle to find accessible legal and psychological assistance. The lack of nationwide infrastructure to support victims exacerbates the challenges faced by those affected by cybercrime. These examples highlight a broader regional issue where support systems for cybercrime victims are insufficiently developed, particularly outside of major cities, underscoring the need for more comprehensive and accessible victim support services across Southeast Asia.

On the other hand, Singapore stands out as a relatively better example of providing psychological and legal support for cybercrime victims. The Cyber Security Agency (CSA) of Singapore has implemented an online reporting service that simplifies the process for victims to report their cases. This platform aims to ensure that victims can seek help quickly and efficiently, addressing a key barrier to reporting cybercrime. Furthermore, the Singapore government offers counseling services specifically designed for cybercrime victims, helping them cope with the psychological impacts of these incidents. Despite these efforts, it is acknowledged that the number of reported cases remains lower than the actual number of incidents, suggesting that underreporting and barriers to accessing support still persist. This highlights Singapore's progress while also emphasizing the need for continuous improvement in victim support mechanisms.

This lack of support also reflects the public's limited awareness of the importance of reporting cybercrime cases and seeking help. Broader

digital literacy campaigns are needed to educate people about the risks of cybercrime and how to protect themselves online. Additionally, governments in Southeast Asia must invest more in developing legal and psychological infrastructures that support the recovery of cybercrime victims.

VI. LACK OF DIGITAL LITERACY AMONG VULNERABLE USERS

Low digital literacy among internet users, particularly children and the elderly, is a significant factor contributing to the high rates of cybercrime in Southeast Asia. This lack of awareness makes many users easy targets for cybercriminals who exploit their limited understanding of online risks. A 2022 report by the DQ Institute revealed that almost three in four (73%) children and adolescents aged 8-18 worldwide experienced at least one cyber risk in the 12 months leading up to September 2022. These risks include cyberbullying, exposure to violent and sexual content, and unwanted sexual contact.[24]

Vulnerable users, such as children, are often victims of online sexual exploitation and cyberbullying. A study conducted by ECPAT International in 2023 showed that Southeast Asia is one of the regions with the highest incidents of online child sexual exploitation in the world. Children who lack an understanding of online safety tend to share photos, videos, or personal information without realizing the potential dangers lurking. As a result, many of them become victims of sexual exploitation or cyberbullying, which has long-term impacts on their mental and emotional health.

[24] DQ institute, "Three in Four Children Worldwide Experienced at Least One Cyber-Risk in 2022," www.dqinstitute.org, 2023.

Meanwhile, the elderly face different challenges in digital literacy. As relatively new internet users, many older adults do not understand how to protect their personal information online. Online scams and identity theft often target elderly people in Southeast Asia. According to an AARP report in 2022, 78% of adults over the age of 65 experienced at least one scam incident, an increase from 69% in 2021[25] Online scammers often exploit the trust and lack of technological understanding among the elderly to carry out fraudulent activities, such as asking for money or banking information. In the Philippines, for example, there was a major case in 2022 where hundreds of elderly individuals fell victim to an online scam that posed as a government social assistance program.

Digital literacy campaigns initiated by governments in Southeast Asia remain uneven. Countries such as Singapore and Malaysia have launched comprehensive digital literacy programs, such as Singapore's Digital for Life Movement, which aims to enhance digital literacy among internet users of various age groups. However, in countries such as Laos and Myanmar, efforts to improve digital literacy remain very limited. The lack of access to digital literacy education in rural areas exacerbates this situation. For example, in Laos, only about 20% of the rural population has access to the internet, and very few of them receive training on digital security.

Another factor exacerbating the low digital literacy in Southeast Asia is the lack of integration of digital literacy education into school curricula. Children who should be taught about online safety in schools often do not receive such lessons. A survey conducted by the ASEAN Cybersecurity Forum in 2023 revealed that only 40% of schools in the region include digital literacy as part of their

[25] Hamim Septian, "Mengatasi Ancaman Penipuan Terhadap Lansia: Panduan Komprehensif 2024," Jurno.id, 2024.

curriculum. This creates a significant knowledge gap among the younger generation, many of whom spend much of their time online without understanding the risks involved.

The lack of digital literacy also impacts migrant workers, another vulnerable group in Southeast Asia. Migrant workers often use the internet to stay connected with their families, but their lack of understanding about online security makes them easy targets for online scams. In Malaysia, for example, thousands of migrant workers became victims of an online investment scam in 2021, resulting in significant financial losses. To address this issue, several non-governmental organizations (NGOs) have launched local initiatives to improve digital literacy among vulnerable users. In Thailand, programs like CyberSafe Thailand have been introduced to provide digital literacy training to children and the elderly. However, these programs often face funding limitations and limited coverage, making it difficult to reach the entire population in need. One of the main obstacles to improving digital literacy is the lack of collaboration between the government, private sector, and civil society. Most digital literacy programs are still sporadic and poorly coordinated. Additionally, the lack of awareness at the community level about the importance of digital literacy means that many initiatives do not receive enough attention. In Vietnam, for example, although the government has launched the Be Smart Online campaign to raise awareness about online safety, public participation in this campaign remains low.

This problem is further exacerbated by infrastructure limitations in several Southeast Asian countries. In countries like Cambodia and Timor Leste, slow and expensive internet access prevents many people from having the opportunity to learn about digital literacy.

Moreover, language becomes another barrier in digital literacy programs, especially in countries with low literacy rates or communities that speak local languages other than the national official language. Many digital literacy materials are only available in English or the national language, making them difficult to access for certain segments of society. Despite these challenges, the potential for improving digital literacy in Southeast Asia is vast. With a large youth population and rapid technology adoption, the region has the opportunity to become a model for promoting inclusive digital literacy. Collaborative efforts between the government, private sector, and civil society are essential to creating effective and sustainable digital literacy programs.

The first step that can be taken is to integrate digital literacy into the school curriculum comprehensively. Countries in the region can also learn from best practices implemented in developed countries, such as the Digital Citizenship Education program in South Korea, which has successfully raised awareness about online safety among school students. Additionally, digital literacy campaigns need to be amplified through the use of social media and other digital platforms. Since most internet users in Southeast Asia are active on social media, well-designed campaigns can reach a larger audience and raise awareness about the importance of digital literacy. For example, the #ThinkBeforeYouClick campaign in the Philippines has successfully raised awareness about online safety among the younger generation. Governments in Southeast Asia also need to collaborate with the private sector to provide more affordable internet access and digital literacy training. Corporate social responsibility (CSR) programs from technology companies can be leveraged to fund digital literacy initiatives in remote areas. Moreover, investing in digital infrastructure, such as providing wider and faster internet access, is

crucial to ensuring that everyone has the opportunity to learn about online security. By addressing these challenges, Southeast Asia can enhance digital literacy among vulnerable users and create a society that is better prepared to face the threats of cybercrime. Better digital literacy will not only protect individuals from online risks but also strengthen the rapidly growing digital economy in the region.

VII. STRATEGIC SOLUTIONS FOR ENHANCING CYBERCRIME VICTIM PROTECTION AND DIGITAL LITERACY IN SOUTHEAST ASIA: LESSONS FROM GLOBAL PRACTICES

To address the legal gaps in the protection of cybercrime victims and improve digital literacy, several practical solutions can be implemented by drawing on the experiences of developed countries outside of Southeast Asia. Below are strategic steps along with comparative analysis from several countries:

1. Harmonization of Laws Between Countries

   Harmonizing laws between countries is a crucial step in addressing legal gaps in Southeast Asia. Countries in the region should adopt international standards such as the Budapest Convention on Cybercrime, which has proven effective in establishing a unified legal framework for handling cross-border cybercrimes.[26] ASEAN, as a regional organization, can play a key role by encouraging the formation of a regional task force dedicated to managing transnational cybercrime cases. Moreover, the development of a uniform legal definition of

[26] Dr. Chat Le Nguyen and Dr. Wilfred Golman, "Diffusion of the Budapest Convention on Cybercrime and the Development of Cybercrime Legislation in Pacific Island Countries: 'Law on the Books' vs 'Law in Action,'" *Computer Law & Security Review* 40 (2021): 1–7, https://doi.org/https://doi.org/10.1016/j.clsr.2020.105521.

cybercrime is essential to reduce ambiguities in law enforcement. The European Union's success with the General Data Protection Regulation (GDPR) serves as an example, where the harmonization of data privacy policies has facilitated legal collaboration among member states.[27] Such an approach can be adapted by ASEAN to enhance the effectiveness of law enforcement and victim protection. From a jurisprudential perspective, the harmonization of legal norms across jurisdictions reflects the concept of a "shared legal culture." The Budapest Convention, for instance, serves as a framework for countries to align their cybercrime laws, thereby reducing legal conflicts and jurisdictional ambiguities. This harmonization can be analyzed through H.L.A. Hart's concept of a legal system as a union of primary and secondary rules.[28] A uniform definition of cybercrime functions as a primary rule (obligation), while regional agreements like the proposed ASEAN task force operate as secondary rules (rules about rules) that ensure consistency and enforcement. Philosophically, this approach also aligns with Kantian ideals of universal legal norms that transcend individual states, fostering global cooperation and the rule of law in cyberspace.[29]

2. Enhancing Law Enforcement Capacity

---

[27] Alexander Wodi, "The EU General Data Protection Regulation (GDPR): Five Years After and the Future of Data Privacy Protection in Review," *SSRN Electronic Journal*, 2023, 1–22, https://doi.org/10.2139/SSRN.4601142.

[28] David Lefkowitz, "H.L.A. Hart: Social Rules, Officials, and International Law," in *Philosophy and International Law: A Critical Introduction*, ed. David Lefkowitz, Cambridge Introductions to Philosophy and Law (Cambridge: Cambridge University Press, 2020), 20–39, https://doi.org/DOI: 10.1017/9781316481653.003.

[29] Øystein Lundestad and Kjartan Koch Mikalsen, "The Institutionalisation of International Law: On Habermas' Reformulation of the Kantian Project," *Journal of International Political Theory* 7, no. 1 (April 2011): 40–62, https://doi.org/10.3366/jipt.2011.0005.

Enhancing law enforcement capacity is essential to address the complexity of cybercrimes in Southeast Asia. Intensive training programs for law enforcement officers should focus on digital forensic investigation techniques and the use of advanced technology to trace online criminal activities. Moreover, investment in developing digital forensic infrastructure, such as forensic centers equipped with modern hardware and software, is critical to support investigative processes. International collaboration is also key, with countries like Germany and Israel serving as strategic partners for sharing expertise and technology. Germany's experience in establishing specialized cyber police units with advanced technology and continuous training offers valuable lessons for nations in the region. The need for more sophisticated law enforcement mechanisms, including digital forensic capabilities, aligns with the functionalist theory of law, which views legal institutions as tools to maintain social order and respond to new forms of deviance. By integrating advanced forensic technology and international partnerships, legal systems can adapt to the evolving nature of cyber threats. From a philosophical perspective, such efforts reflect John Rawls' principle of justice: ensuring that law enforcement institutions have equal capacity to protect individuals' digital rights and freedoms.[30] Investment in specialized training and infrastructure can also be seen as fulfilling the social contract, as theorized by Rousseau, wherein the state must provide security and justice to its citizens in exchange for their compliance and trust.

[30] David M Douglas, "Towards a Just and Fair Internet: Applying Rawls' Principles of Justice to Internet Regulation," *Ethics and Information Technology* 17, no. 1 (2015): 57–64, https://doi.org/10.1007/s10676-015-9361-1.

3. Psychological and Legal Support for Victims

   Psychological and legal support for cybercrime victims is often overlooked in Southeast Asia. To address this issue, each country needs to establish crisis centers that provide free psychological counseling and legal assistance. Additionally, developing online applications for case reporting can make it easier for victims to seek help. Community programs should also be involved, with non-governmental organizations playing a crucial role in offering both legal and psychological support. Sweden and Australia serve as good examples, with their national programs offering efficient counseling and legal services. Community-based approaches, such as those in Sweden, can be adapted by engaging local actors and civil society organizations in Southeast Asia. Providing psychological and legal support to cybercrime victims reflects a shift toward a victim-centered approach in the criminal justice system, similar to restorative justice models that emphasize healing and rehabilitation over mere punishment. Theoretically, this approach aligns with Lon Fuller's integrative jurisprudence, which highlights the role of law in facilitating constructive human interactions.[31] Philosophically, the emphasis on victim support resonates with Martha Nussbaum's capabilities approach, which argues that a just legal system should enhance individuals' ability to live with dignity and security. By addressing the psychological impact of cybercrime and ensuring victims have access to counseling and legal assistance, the legal framework fulfills its moral duty to uphold the dignity and well-being of those harmed.

[31] Shyamkrishna Balganesh, "Interactional Ordering: Reconstructing Lon Fuller's Theory of Private Law," *SSRN Electronic Journal*, June 2024, 1–37, https://doi.org/10.2139/SSRN.4888472.

4. Improving Digital Literacy

   Digital literacy must become a priority in addressing the vulnerabilities of internet users in Southeast Asia. One effective step is integrating digital literacy into school curricula, enabling younger generations to understand the importance of protecting their privacy and online security. Digital literacy campaigns on social media should also be expanded to reach users across different age groups. Additionally, collaboration with the private sector can help provide more affordable internet access and digital literacy training. South Korea serves as a relevant example, with its Digital Citizenship Education program training students on online ethics and security.[32] This approach can inspire Southeast Asia to create a society better prepared to face cyber threats. Integrating digital literacy into educational curricula and community initiatives can be understood through the framework of legal pluralism, which acknowledges multiple sources of normative order. By incorporating educational policies that promote safe online behavior, countries recognize that the law is not the sole regulator of conduct education and social norms also play a crucial role. Philosophically, this strategy reflects Aristotle's concept of cultivating virtues through education.[33] By teaching individuals how to safeguard their digital identities, the state not only enforces legal compliance but also encourages responsible digital citizenship, thus contributing to the common good.

---

[32] Jongsur Park et al., "디지털 사회로의 전환과 시민 교육," 글로벌교육연구 14, no. 3 (September 2022): 5–32, https://doi.org/10.19037/AGSE.14.3.01.

[33] Thomas L. Pangle, "The Rhetorical Strategy Governing Aristotle's Political Teaching," *The Journal of Politics* 73, no. 1 (January 2011): 84–96, https://doi.org/10.1017/S0022381610000885.

5. Regional and International Collaboration

   Regional and international collaboration is a strategic step in addressing cybercrime challenges in Southeast Asia. ASEAN needs to establish a cybercrime committee tasked with overseeing the implementation of cybersecurity policies in each member state. In addition, data and technology exchange among countries should be enhanced to expedite cross-border cybercrime investigations. The European Union's experience with Europol, which serves as a platform for cross-border law enforcement information and technology sharing, can provide a useful reference. Beyond this, multilateral cooperation through forums such as the INTERPOL Global Cybercrime Program can help Southeast Asia access advanced resources and technologies to increase the effectiveness of cybercrime handling in the region. Regional and international collaboration in tackling cybercrime reflects the concept of transnational legal orders (TLOs), which arise when several countries agree on legal frameworks to address cross-border issues.[34] The establishment of an ASEAN cybercrime committee mirrors the European Union's harmonization efforts under GDPR and Europol, providing legal infrastructure for cooperation and information exchange. From a philosophical standpoint, such collaboration embodies the cosmopolitan ideal of global justice. Drawing on Habermas's discourse ethics, such international initiatives can be viewed as a rational, deliberative process by which countries agree on shared principles to address cyber

[34] Pushpanathan Sundram, "ASEAN Cooperation to Combat Transnational Crime: Progress, Perils, and Prospects," *Frontiers in Political Science* 6 (February 15, 2024): 1–6, https://doi.org/10.3389/FPOS.2024.1304828/BIBTEX.

threats, ensuring that legal responses are not only effective but also legitimate and ethically grounded.[35]

VIII. STRATEGIC SOLUTIONS FOR ENHANCING CYBERCRIME VICTIM PROTECTION AND DIGITAL LITERACY IN SOUTHEAST ASIA: A CYBER VICTIMOLOGY CONCEPTUAL APPROACH

In the context of Southeast Asia, the rise of cybercrimes such as online fraud, identity theft, cyberbullying, and data breaches has raised significant concerns about the protection of victims and the need for comprehensive digital literacy programs. Cyber victimology, as an interdisciplinary field, focuses on understanding the experiences of victims in the digital space, the nature of cybercrimes, and the effectiveness of responses in mitigating harm.[36] By applying this conceptual framework, several strategic solutions can be proposed to enhance victim protection and digital literacy.

1. Understanding Cyber Victimology and Its Relevance
   Cyber victimology explores the dynamics between offenders, victims, and the digital environment in which cybercrimes occur. Unlike traditional criminology, it focuses on the unique aspects of victimization in the digital era, where anonymity and global reach complicate the identification and assistance of victims. In Southeast Asia, where internet penetration is high and diverse, understanding these dynamics is critical for formulating effective victim protection strategies. Cyber victimology helps to identify patterns of vulnerability, such as

[35] Jens Steffek, "The Legitimation of International Governance: A Discourse Approach," *European Journal of International Relations* 9, no. 2 (June 2003): 249–75, https://doi.org/10.1177/1354066103009002004.

[36] Debarati Halder, *Cyber Victimology : Decoding Cyber-Crime Victimisation*, *Cyber Victimology* (Routledge, 2021), https://doi.org/10.4324/9781315155685.

socio-economic factors, gender, age, and digital literacy, which influence individuals' susceptibility to cybercrimes. It highlights the importance of understanding victimization not just as a consequence of criminal behavior but also in terms of its socio-legal and psychological impacts on the victim.

2. Developing Robust Legal Frameworks for Cyber Victim Protection

   One of the first steps in protecting victims is the establishment and reinforcement of legal frameworks that specifically address the needs of cybercrime victims. In Southeast Asia, countries like Singapore, Malaysia, and Thailand have implemented cybercrime laws that criminalize a range of online offenses. However, there is often a gap in these laws regarding the direct provision of victim protection, compensation, and support mechanisms. From a cyber victimology perspective, legal responses should go beyond punishment for offenders to include restorative justice elements that prioritize victim needs. This might include:

   a. Clear definitions and classification of cybercrimes

      Laws must be specific to the types of cybercrimes that affect different groups of victims, such as children, the elderly, or marginalized communities.

   b. Victim compensation and support

      Implementing systems to provide financial, psychological, and social support to victims, ensuring that they are not left alone in recovering from the impact of the crime.

   c. Cross-border legal cooperation

      Since cybercrimes often transcend national borders, regional cooperation in legal matters is essential to ensure victims

have access to justice, even if offenders are in a different jurisdiction.

3. Expanding Digital Literacy Programs

   Digital literacy is a cornerstone of cybercrime prevention and victim protection. The concept of digital literacy goes beyond simply teaching individuals how to use technology it encompasses the ability to recognize threats, understand privacy settings, and make informed decisions online. In Southeast Asia, there is a significant disparity in digital literacy levels between urban and rural areas, as well as among different age groups and socio-economic classes. To address this, comprehensive digital literacy programs should be developed, focusing on:

   a. Awareness of online risks

      Educating individuals on the various types of cybercrimes, including phishing, social engineering, and scams, which are prevalent in the region.

   b. Promoting safe online behaviors

      Encouraging best practices such as using strong passwords, enabling two-factor authentication, and being cautious with personal information.

   c. Targeted programs for vulnerable groups

      Developing programs specifically for vulnerable populations such as children, women, the elderly, and those in rural or underserved communities who are at greater risk of exploitation and victimization.

   d. School-based curricula

Introducing cyber hygiene and security topics into educational systems, from elementary to tertiary levels, so that digital literacy becomes part of lifelong learning.

4. Creating Support Systems for Victims

   Another crucial aspect of victim protection is the creation of support systems that provide immediate assistance and long-term recovery. These systems should be designed to support victims emotionally, financially, and legally, ensuring that they have access to resources to navigate the complexities of cybercrime victimization. In Southeast Asia, the following measures could be considered:

   a. Hotlines and reporting platforms

      Establishing anonymous reporting systems that allow victims to report cybercrimes without fear of retribution. These platforms should be easy to use, multi-lingual, and accessible on various digital platforms.

   b. Psychological support

      Offering counseling services to victims who suffer from the psychological impacts of cybercrimes, such as stress, anxiety, or depression.

   c. Legal assistance

      Providing pro bono legal support to victims to help them understand their rights, pursue justice, and recover damages.

   d. Community support networks

      Building community-driven victim support networks that offer peer-to-peer assistance, especially in regions where formal systems may be less accessible or trusted.

5. Enhancing Public-Private Partnerships

   Collaboration between the government, law enforcement agencies, non-governmental organizations (NGOs), and the private sector is critical in addressing the complexities of cybercrime. The private sector, particularly technology companies and service providers, plays a pivotal role in detecting, reporting, and preventing cybercrimes.

   a. Data protection initiatives

      Companies must be held accountable for safeguarding users' data and for cooperating with law enforcement when incidents occur.

   b. Public-private dialogues

      Regular dialogues between stakeholders can help develop strategies for protecting victims, creating safer online environments, and ensuring that the interests of victims are prioritized.

   c. Corporate social responsibility

      Encouraging companies to invest in digital literacy and victim support programs as part of their social responsibility to the community.

6. Advocating for a Holistic Approach to Cybercrime Prevention

   Cybercrime prevention requires more than just reactive measures it demands a proactive, holistic approach that incorporates the principles of cyber victimology. This approach recognizes that technology can be both a tool for crime and a means for prevention. By understanding the patterns and characteristics of cybercrime victimization, strategies can be developed to minimize risks, prevent crimes before they occur,

and reduce the impact on victims. Southeast Asia, with its diverse legal, social, and cultural contexts, requires regional coordination to effectively address cybercrime. Efforts should be made to harmonize legal frameworks, share best practices, and cooperate on cross-border investigations. Initiatives such as the ASEAN Cybersecurity Cooperation and partnerships with international bodies like INTERPOL can foster stronger collaboration in protecting cybercrime victims.

V. CONCLUSION

This study demonstrates that Southeast Asia is contending with complex and multifaceted challenges in safeguarding victims of cybercrime. Key structural issues persist, including substantial legal inconsistencies among ASEAN member states, limited institutional capacity within law enforcement agencies, low levels of digital literacy among high-risk populations, and the absence of a holistic, rights-based framework for legal and psychosocial victim support. The lack of regulatory harmonization has contributed to a fragmented regional response, thereby allowing cyber offenders to exploit jurisdictional loopholes with relative impunity. Consequently, victims, particularly those from vulnerable demographics such as women, children, the elderly, and transnational labor migrants, remain susceptible to repeated victimization, further exacerbated by limited access to justice and insufficient institutional redress mechanisms. This research also underscores the disparity in institutional readiness across the region, highlighting countries such as Singapore that have developed robust cybersecurity infrastructures, while others, including Cambodia, Laos, and Myanmar, continue to face serious regulatory and operational deficits. Moreover, law enforcement agencies across the region frequently lack specialized training in digital forensic science and

cyber-investigative methodologies, with cross-border cooperation remaining nascent and underutilized. In response to these critical findings, the study proposes five interrelated policy interventions. First, ASEAN must advance legal harmonization across member states by aligning national cybercrime laws with internationally recognized standards, such as those articulated in the Budapest Convention on Cybercrime. Second, it is imperative to institutionalize region-wide, certified training programs in digital forensics and cyber-investigation for law enforcement personnel, supported through coordinated regional platforms for knowledge exchange and capacity development. Third, national governments must adopt victim-centered frameworks that establish crisis intervention centers, digital reporting mechanisms, and trauma-informed legal aid systems, particularly those that address gender-based vulnerabilities and intersectional harm. Fourth, ASEAN should launch large-scale, inclusive digital literacy initiatives targeting educational institutions, elderly populations, and rural communities to strengthen digital resilience. Fifth, the creation of a dedicated ASEAN Cyber Victimology Task Force is recommended to monitor policy implementation, facilitate regional data-sharing, and bridge capacity gaps among member states. Through the systematic integration of cyber victimology principles into regional policy discourse and practice, ASEAN can work toward constructing a secure, equitable, and inclusive digital environment, one that affirms and protects the rights, dignity, and agency of all digital citizens.

ACKNOWLEDGMENTS

With profound gratitude, the author expresses heartfelt thanks to all individuals and institutions that have supported and contributed to the completion of this journal. Special appreciation is extended to

academic institutions, mentors, and colleagues whose invaluable feedback and moral encouragement have been instrumental throughout the research process. The author is also deeply thankful to family and friends for their unwavering prayers, support, and motivation. Acknowledgment is due to the foundational works of prior researchers, whose insights and findings have significantly inspired this study on addressing the legal gaps in cybercrime victim protection across Southeast Asia. Their contributions have paved the way for exploring innovative solutions, such as harmonizing laws, enhancing digital literacy, and strengthening regional cooperation. It is the author's sincere hope that this journal will serve as a meaningful contribution to advancing justice and sustainability within the digital sphere, fostering a more secure and equitable environment for all.

COMPETING INTEREST

None

REFERENCES

Amarullah, Abdul Hanief, Arthur Josias Simon Runturambi, and Bondan Widiawan. "Analisis Ancaman Kejahatan Siber Bagi Keamanan Nasional Pada Masa Pandemi COVID-19." *Jurnal Kajian Stratejik Ketahanan Nasional* 4, no. 2 (2021): 17–28. https://doi.org/10.7454/jkskn.v4i2.10052.

Astro Awani. "Hampir 40 Peratus Serangan Siber Di Malaysia Libatkan Akaun Pembuatan, Sektor Kerajaan Pada 2023." www.astroawani.com, 2024.

———. "Majoriti Syarikat Malaysia Alami Serangan Siber Pada 2023." astroawani.com, 2024.

Balganesh, Shyamkrishna. "Interactional Ordering: Reconstructing Lon Fuller's Theory of Private Law." *SSRN Electronic Journal*, June

2024, 1–37. https://doi.org/10.2139/SSRN.4888472.

Cristiano, Fabio. "Singapore : A Leading Actor in ASEAN Cybersecurity." In *Routledge Companion to Global Cyber-Security Strategy*, 381–91. Routledge, 2021. https://doi.org/10.4324/9780429399718-35.

Damarjati, Danu. "11 WNI Di Kamboja: Dipaksa Scamming Tipu Sesama Hingga Dijemput Polisi." news.detik.com, 2023.

David Lefkowitz. "H.L.A. Hart: Social Rules, Officials, and International Law." In *Philosophy and International Law: A Critical Introduction*, edited by David Lefkowitz, 20–39. Cambridge Introductions to Philosophy and Law. Cambridge: Cambridge University Press, 2020. https://doi.org/DOI: 10.1017/9781316481653.003.

Douglas, David M. "Towards a Just and Fair Internet: Applying Rawls' Principles of Justice to Internet Regulation." *Ethics and Information Technology* 17, no. 1 (2015): 57–64. https://doi.org/10.1007/s10676-015-9361-1.

DQ institute. "Three in Four Children Worldwide Experienced at Least One Cyber-Risk in 2022." www.dqinstitute.org, 2023.

ECPAT. "Catatan Akhir Tahun ECPAT Indonesia 2023 : Keberlanjutan Perlindungan Anak Dari Eksploitasi Seksual." ecpatindonesia.org, 2023.

Fernando, Zico Junius, Kiki Kristanto, and Ariesta Wibisono Anditya. "Knitting Democracy, Separating Restraints: Legal Reform and a Critical Analysis of Article 256 of the New Criminal Code and Its Impact on Freedom of Speech." *Journal of Law and Legal Reform* 5, no. 2 (April 2024): 555–86. https://doi.org/10.15294/JLLR.VOL5I2.1670.

Halder, Debarati. *Cyber Victimology : Decoding Cyber-Crime Victimisation*. *Cyber Victimology*. Routledge, 2021. https://doi.org/10.4324/9781315155685.

Jaishankar, K. "Cyber Victimology: A New Sub-Discipline of the Twenty-First Century Victimology." *An International Perspective on Contemporary Developments in Victimology: A Festschrift in Honor*

of Marc Groenhuijsen, January 2020, 3–19. https://doi.org/10.1007/978-3-030-41622-5_1.

Jaishankar, K. "Cyber Victimology: A New Sub-Discipline of the Twenty-First Century Victimology BT - An International Perspective on Contemporary Developments in Victimology: A Festschrift in Honor of Marc Groenhuijsen." In *An International Perspective on Contemporary Developments in Victimology*, edited by Janice Joseph and Stacie Jergenson, 3–19. Cham: Springer International Publishing, 2020. https://doi.org/10.1007/978-3-030-41622-5_1.

Karpagapriya. "An Evaluation of the Jurisdictional Aspects of Cyber Crimes Under the Regional Agreements with Special Emphasis on the Budapest Convention." *IJFMR - International Journal For Multidisciplinary Research* 5, no. 6 (November 2023): 1–6. https://doi.org/10.36948/IJFMR.2023.V05I06.9365.

kumparanNEWS. "Penipuan Sindikat Kriminal Asia Tenggara Gencar Pakai AI, Bisa Raup Rp 575 T." kumparan.com, 2024.

Lundestad, Øystein, and Kjartan Koch Mikalsen. "The Institutionalisation of International Law: On Habermas' Reformulation of the Kantian Project." *Journal of International Political Theory* 7, no. 1 (April 2011): 40–62. https://doi.org/10.3366/jipt.2011.0005.

Machmudi, M. Iqbal Al. "481 Kasus Eksploitasi Anak Secara Daring, Transaksi Dengan Kripto." mediaindonesia.com, 2024.

MDDI. "New Agency for Online Safety and Assurance." www.mddi.gov.sg, 2024.

Nadine Tong and Emma Leung. "An Analysis of the Amendments to Singapore's Personal Data Protection Act." www.durhamasianlawjournal.com, 2022.

Nguyen, Dr. Chat Le, and Dr. Wilfred Golman. "Diffusion of the Budapest Convention on Cybercrime and the Development of Cybercrime Legislation in Pacific Island Countries: 'Law on the Books' vs 'Law in Action.'" *Computer Law & Security Review* 40 (2021): 1–7. https://doi.org/https://doi.org/10.1016/j.clsr.2020.105521.

Pangle, Thomas L. "The Rhetorical Strategy Governing Aristotle's Political Teaching." *The Journal of Politics* 73, no. 1 (January 2011): 84–96. https://doi.org/10.1017/S0022381610000885.

Park, Jongsur, Seunghwa Jeon, Yoon Lee, and Yunhee Choi. "디지털 사회로의 전환과 시민 교육." 글로벌교육연구 14, no. 3 (September 2022): 5–32. https://doi.org/10.19037/AGSE.14.3.01.

Puspita, Ayu, and Anik Nur Handayani. "Dampak Teknologi Digital Terhadap Perilaku Sosial Masyarakat 5.0." *Jurnal Inovasi Teknologi Dan Edukasi Teknik* 2, no. 10 (2022): 446–51. https://doi.org/10.17977/um068v2i102022p446-451.

Romaniuk, Scott N., and Mary Manjikian. "Routledge Companion to Global Cyber-Security Strategy." *Routledge Companion to Global Cyber-Security Strategy*, January 2021, 1–632. https://doi.org/10.4324/9780429399718/ROUTLEDGE-COMPANION-GLOBAL-CYBER-SECURITY-STRATEGY-MARY-MANJIKIAN-SCOTT-ROMANIUK/RIGHTS-AND-PERMISSIONS.

Septian, Hamim. "Mengatasi Ancaman Penipuan Terhadap Lansia: Panduan Komprehensif 2024." Jurno.id, 2024.

SG Her Empowerment. "SHE Study Reveals Majority of Online Users Have Experienced Online Harms." www.she.org.sg, 2023.

Smith, Robert Brian. "Complexity of Legal Harmonisation in Southeast Asia: A Diversity of Legal Systems & Languages." *Athens Journal of Law* 10, no. 2 (April 2024): 233–54. https://doi.org/10.30958/AJL.10-2-4.

Statista. "Internet Usage in Southeast Asia - Statistics & Facts." www.statista.com, 2024.

Steffek, Jens. "The Legitimation of International Governance: A Discourse Approach." *European Journal of International Relations* 9, no. 2 (June 2003): 249–75. https://doi.org/10.1177/1354066103009002004.

Sundram, Pushpanathan. "ASEAN Cooperation to Combat Transnational Crime: Progress, Perils, and Prospects." *Frontiers in Political Science* 6 (February 2024): 1–6.

https://doi.org/10.3389/FPOS.2024.1304828/BIBTEX.

Vijaykumar Shrikrushna et al Chowbe. "Beyond Borders : Addressing the Legal Quagmire of Jurisdiction in Cyberspace." *IJFMR - International Journal For Multidisciplinary Research* 6, no. 6 (November 2024): 1–19. https://doi.org/10.36948/IJFMR.2024.V06I06.30051.

Vika Azkiya Dihni. "Keamanan Siber Indonesia Peringkat Ke-6 Di Asia Tenggara." databoks.katadata.co.id, 2022.

Weise, Sebastian, Franziska Rinke, and Aishwarya Natarajan. "Dawn of a New Era of Global Data Protection?" *Völkerrechtsblog*, March 2021, 1–3. https://doi.org/10.17176/20210302-153629-0.

Wodi, Alexander. "The EU General Data Protection Regulation (GDPR): Five Years After and the Future of Data Privacy Protection in Review." *SSRN Electronic Journal*, 2023, 1–22. https://doi.org/10.2139/SSRN.4601142.

***

HISTORY OF ARTICLE

Submitted : January 21, 2025

Revised : June 1, 2025

Accepted : June 8, 2025

Published : June 30, 2025