AKCF ASEAN-KOREA COOPERATION FUND 한-아세안 협력기금

Forging and Fostering Peace
ASEAN Institute for Peace and Reconciliation

ASEAN-IPR CYBERSECURITY YOUTH ESSAY COMPETITION

2024

2025

ASEAN-IPR Publication of
ASEAN-IPR Cybersecurity Youth Essay Competition 2024

Editor:
Bayu Wicaksono
Patricia (Kesumahadi)

Editing support:
Deni Prasetya Mulya
Theodora Alyssa Ysabel

"ASEAN-IPR Publication of ASEAN-IPR Cybersecurity Youth Essay Competition 2024 is published by the ASEAN Institute for Peace and Reconciliation (ASEAN-IPR)

The ASEAN-IPR accepts no responsibility for views expressed or content plagiarised from other sources. Responsibility rests exclusively with the individual author.

Copyright of this publication is held by the ASEAN-IPR
No part of this publication may be reproduced in any form without permission."

ASEAN-IPR CYBERSECURITY YOUTH ESSAY COMPETITION

AN OVERVIEW

This essay compilation book features the winning entries from the ASEAN-IPR Cybersecurity Youth Essay Competition 2024, held as an integral part of the **ASEAN-IPR Regional Conference on Cybersecurity and the Role of Information Technology in Fostering a Culture of Peace in ASEAN**. The competition aimed to promote meaningful youth participation and identify individuals from ASEAN Member States and Timor-Leste with a strong understanding of cybersecurity and peacebuilding. By providing a platform for young people to showcase their knowledge and perspectives, the competition fostered a deeper understanding of the critical intersection between cybersecurity and human security.

The essays delve into critical sub-themes such as the impact of cyber threats on human security, the role of technology in fostering peace and trust, balancing privacy and security in cyberspace, and youth engagement in addressing online radicalization and political polarization. Written by young individuals aged 21-35, they offer unique perspectives and innovative policy recommendations for enhancing cybersecurity and peacebuilding in the region. These essays represent a valuable contribution to the ongoing regional discussions on cybersecurity and serve as a testament to the youth's commitment to shaping a secure and peaceful digital future for ASEAN.

ASEAN-IPR extends its gratitude to the Government of the Republic of Korea for their support through the ASEAN-Korea Cooperation Fund (AKCF), which made this essay publication possible.

AKCF ASEAN-KOREA COOPERATION FUND 한 - 아세안 협력기금

TABLE OF **CONTENTS**

PSYBERSECURITY: EMPOWERING YOUTH TO DEFEND DATA IN A DIGITAL WORLD

ABSTRACT

The prompt digitization of ASEAN has revealed its weaknesses, with cyberattacks pointing out serious shortcomings in data management, governance, and privacy protection. This essay examines instances such as the SIM Registration Act of the Philippines and significant security breaches in Singapore and Indonesia to demonstrate how inadequate protections not only jeopardize security but also cause psychological harm. The analysis, which uses the panopticon as a model, shows how ongoing surveillance, whether actual or imagined, erodes public trust in digital systems by fostering fear, acquiescence, and mistrust. In order to resolve these problems, ASEAN has to implement transparent and moral cybersecurity frameworks that are modeled after Singapore's and Qatar's best practices. Digital literacy should be a top priority for regional changes, bridging generational divides to protect people from exploitation and fraud. Furthermore, privacy can be preserved while security is maintained by a unified legal framework that prioritizes justice, accountability, and proportionality. ASEAN can establish a shared culture of accountability and adaptability by encouraging cross-border cooperation and using young people as digital ambassadors. It is not only a technical problem but also a moral requirement to strike a balance between innovation and human rights. At this juncture, ASEAN can guarantee a safe and inclusive digital future for all its citizens by taking decisive action.

Keywords: Digital Literacy; Panopticon; Cybersecurity; Privacy, and Human Rights

AUTHOR:

HAMMIL RAINARD D. DISTOR

(PHILIPPINES)

Introduction

In the age of digital information, privacy, security and human rights tend to be placed at risk as we work towards digital innovation. Is it necessary to have a compromise?

Months after the Philippine government passed the SIM Card Registration Act of 2022 into a law, a surge in scams has been reported.The SIM Card Registration Act was encouraged by the Senate with the promise to eliminate text scams and fraud, aiming to eliminate phishing (Janvic, 2024). With the rise of POGOs[1] (Abalos, 2024), it has become a Trojan horse, enabling scammers to exploit registered identities while law-abiding citizens face bigger risks of privacy breaches. Instead of making it impenetrable for scammers, the passing of the law has ironically made it easier for them to access the classified information of those registered.

THIS IS NOT AN ISOLATED CASE. AcrossASEAN, similar alternatives aimed at enhancing cybersecurity clash with the region's collective goals of safeguarding privacy and human rights.The challenge for ASEAN is clear: How can we implement and develop cybersecurity measures that balance security, privacy, and human rights amid rising digital threats and rapidly evolving technologies?

The Cybersecurity Landscape in ASEAN

At the core of Southeast Asia's digital revolution, the threats online have become unseen, quietly shapingSoutheast Asia's securitylandscape. A starkexample is the silent call center scams in 2023 that targeted vulnerable people in Thailand, especially the elderly, with their fraudulent schemes. The authorities report that over 360,000 cybercrime cases in less than two years highlighting the alarming presence and devastating impact of such scams. Hence, some victims overwhelmed by losses, even attempted or committed suicide (Karnjanatawe, 2023). In Singapore, the worst cyber-attack was in 2018 with the SingHealth data breach, which exposed the personal data of around 1.5 million patients including the Prime Minister, which triggered widespread questioning of Singapore's healthcare cybersecurity measures (Tham, 2021).

[1] Philippine Offshore Gaming Operators (POGOs) are entities licensed by the Philippine Amusement and Gaming Corporation (PAGCOR) to offer online gaming services to players outside the Philippines. Established in 2016, POGOs aim to tap into the global online gaming market, generating significant revenue through regulatory fees and taxes. However, their operations have sparked debates due to concerns over illegal activities, security risks, and economic implications. Critics highlight issues such as unregulated operations, potential involvement in criminal activities.

In September 2024, the Indonesian government also encountered a massive data breachof taxpayers' information. This breach, along with the ransomware attackthat paralyzed government services last June, underscores Indonesia's on-going battle against cybersecurity measures and inadequate data protection ("Indonesia's tax agency probes alleged Personal Data Breach," 2024).

Furthermore, the SIM Registration Act of the Philippines has further damaged public trust by raising worries about privacy and data exploitation although it was designed to stop mobile fraud. The necessity for ASEAN countries to harmonize their legislation with a focus on data protection, openness, and inclusive implementation is reflected in this circumstance. The fundamental structural problem is reflected in the inability to identify fraud in real time and protectagainst cyber-attacks. To coerce victimsinto complying, scammers take advantage of human psychology by playing on feelings of urgency, fear, and trust. People are left susceptible by inadequate safeguards and lack of digital knowledge, increasing the psychological impact of these breaches. Stronger cybersecurity frameworks, improvedfraud detection systems,and stricter restrictions are necessary to safeguard sensitive data and national security in the ASEAN cyberspace landscape.

The "Panopticon" in Cyberspace

In the digital era, the mind is like an open book. Knowing this, cybercriminals skillfully take advantage of our wants—cognitive shortcuts that we frequently take without even realizing it. Anchoring effects,such as a misleading headlineor an offer that seems too good to be true, cause us to believe the first piece of information we come across. Whether it's a concerning email or an overly fancy social media advertisement, "the shortcut" forces us to respondrapidly to what is most easily accessible. Because of these biases, we tend to behave hastilywithout thoroughly considering the risks or motivations, which makes it simpler for scam artists to take advantage of us. There is a "digital panopticon (Foucault, 1979)[2]" at work when scammers take advantage of these mental vulnerabilities: the threat is always there, watching, but we never know where it will strike next.

[2] The panopticon is a concept introduced by philosopher Michel Foucault (1979) in his work Discipline and Punish. It was originally designed as a model for prisons, where a central tower allowed guards to observe prisoners without them knowing when they were being watched. This constant, unseen surveillance led to self-regulation as prisoners adjusted their behavior to avoid punishment. In the digital age, the panopticon translates into the feeling of being perpetually watched online. We may not always know when we're being observed or manipulated, but we adjust our actions as if we are. This constant awareness of potential surveillance impacts how we behave and interact in cyberspace.

Nowadays, people are always trying to sell us something in today's digital world-- a product, a concept, or even a way of life. The purpose of this never-ending flow of data is to induce FOMO, or the fear of missing out. We are susceptible to manipulation because of our craving for connection and our rapid trust in digital encounters. We navigate the digital world without knowing if the next notification or message is a real opportunity or a trap, much as in the panopticon, where everyone is being watched but nobody is aware that they are beingwatched at any given time.In the cyberspace, we do not always see the whole picture, and have tendencies to make judgments based more on FOMO than logic.

To combat this, digital literacy is the first piece of mental armor needed to resist digital risks. Thinking critically before clicking, challenging what we consume, and examining the motivations behind it are all ways to become resilient. We may protect ourselves from these dangersby being awareof what we are doing and double-checking every pop-upnotification of its legitimacy and truthfulness. This goes beyondawareness; it involves takingintentional action, turningthe powerlessness of continual monitoring into empowerment, and learning to outsmart the mechanisms that intend to rule us.

Balancing Privacy,Security, and Human Rights

The digital revolution in ASEAN has spurred serious discussions about data privacy and data gathering ethics. Managing personal data ethically has grown more important as artificial intelligence (AI) becomes more powerful (“AI, Privacy, and Data Protection: Legal Considerations in Southeast Asia,” 2023). Because of this, ASEAN nations must take strong action; finding a balance between promoting innovation and defending individual rights is no longer an option.

There are serious ethical questions raised by AI's capacity to handle enormous volumes of personal data. Singapore and Malaysia are two ASEAN nations that have taken significant action to control data privacy. Others fall behind, resulting in an unbalanced legal environment with enforcement gaps (“AI, Privacy, and Data Protection: Legal Considerations in Southeast Asia,” 2023). In the absence of unified regulations, improper data handling can compromise privacy, weaken public belief, and erode trust in digital networks. To make sure that technological advancement doesn't come at the expense of individual liberties, ASEAN must give ethical data collection top priority. Public trust is further tested by the creeping expansion of surveillance.

Many people are left feelingcautious and anxiousbecause they have no understanding of how their data is gathered, much less how it is used. Widespread, deceptive monitoring by various parties undermines public confidence in digital networks and their regulators. In addition to undermining individual liberties, this mistrust preventsthe digital economyfrom expanding as consumers stop utilizing services, they no longer feel safe using (ASEAN, 2024).

Education is the first step toward the solution. It is not only our duty to educate citizens about their digitalrights; it is also essential to restore confidence and encouraging openness in the handling of data. Therefore, ASEAN countries must simultaneously manage the challenge of striking a balance between privacy and security. Governments have passed broad national security legislation in response to growing cyberthreats, but these frequently put the interests of the state ahead of individual liberties. Such actions run the potential of infringing on freedom of expression and privacy in the absence of sufficient control. This trade-off must be reconsidered by policymakers to build a secure, democratic society.Creating laws that safeguard both security and privacy requiresopen governance and genuine cooperation with civil society.

Human rights are another hot spot for cyberspace. Legislation is being used as a tool to suppress dissent and limit free expression online. For example, Thailand's lèse- majesté laws make it illegalto criticize the monarchy, which can resultin incarceration for posts made on social media (ILGA Asia, 2024). These acts call for persistent campaigning and international pressure to protect the right to free speech online. Strong data protection regulations and unambiguous guidelines regarding the storage and use of data are necessary. It is essential that security shouldn'thave to come at the expense of privacy (Dela Cruz, et.al., 2024).

Bridging Generations for a Secure and Inclusive DigitalFuture in ASEAN

To create ASEAN a safer cybersecurity environment, a bold,united approach that combines education, data protection, balanced legislation, and regional cooperation is required. These policies must consider ASEAN's particular possibilities and difficulties, even thoughthey are influenced by international standards. Important foundations for this endeavor include developing appropriate cybersecurity regulations, protecting personal data through transparency, and enhancing digitalliteracy for all generations. A robust and inclusive digital ecosystem is further ensured by empowering young people as digital advocates and encouraging cross-border collaborations.

By giving these stepstop priority, ASEAN can create a digital ecosystembased on sharedresponsibility, trust, and security while simultaneously safeguarding its population from changing cyber threats.

The foundation of ASEAN's cybersecurity education plan should, first and foremost, be gamification and certification, giving participants of all ages access to interactive learning platforms and certifications that are regionally specific. Real-world cyberthreats can be simulated using gamified courses,which can make learning exciting and approachable while developing important skills. Singapore's Cybersecurity Skills Framework (“Data and Privacy Protection in ASEAN,” 2018), which successfully builds trained workforces through certifications and public-private partnerships, likewise adheres to these principles. To provide a proactive, inclusive approach to addressing digital risks, ASEAN may build on this by including gamified cybersecurity simulations into community projects and educational courses.

ASEAN's data protection systemcan be strengthened by requiring frequent audits of data controllers and incorporating cutting-edge privacy-enhancing technologies like blockchain and encryption, which will guarantee compliance and transparency. By addressing privacy issuesand promoting confidence in digital systems,these steps lower implementation risks. In a similar vein, the Cybercrime Prevention Law of Qatar lays out explicit punishments for illegal data access and tampering, reflecting these concepts. By establishing cross-border cybercrime units with common resources and knowledge, ASEAN may build on these models and facilitate cooperative efforts to address transnational cyberthreats more successfully and unified.

Furthermore, it is equally critical that ASEAN close the generational divide by providing adults and children with the cybersecurity information they need. Leading this campaign should be digital educators and advocates who use youth-driven initiatives to educate people about the dangers and obligations of cyberspace. These initiatives can include publicawareness campaigns that highlight the risks of cybercrime, digitalhygiene, and responsible online conduct, as well as online safety training in schools. ASEAN should also support youth-led projects that advance digital literacy and incorporate cybersecurity into school curricula. Young people can also act as educators for the elderly, especially those who are more susceptible to internet fraud and false information. Through age-appropriate digital literacy initiatives, ASEAN may promote a shared responsibility and online safety culture.

Simultaneously, ASEAN must also give top priority to creating cybersecurity regulations that balance privacy and security. Frameworks for cybersecurity should adhere to the conceptsof necessity and proportionality ratherthan being unduly intrusive. Policies must be developed with the goal of protecting vital infrastructures without compromising the rights of individuals. An excellent illustration of how cybersecurity measures may be put into place while maintaining accountability and openness is Singapore's Cybersecurity Act, which covers the protection of critical information infrastructures (CII) (“Data and Privacy Protection in ASEAN,” 2018). Comparably, with explicit rules on consent and security responsibilities, Qatar's data protection law guarantees that personal information is handled securely and with respect (“Data and Privacy Protection in ASEAN,” 2018). Similar frameworks that guarantee human rights, privacy, and digital security are balanced and in line with global best practices can be developed by ASEAN.

Lastly, ASEAN should promoteregional cohesion and cross-border cooperation in the battle against cyberthreats. This entails using channels for information sharing and capacity building as well as cultivating alliances with global organizations like the International Telecommunication Union (ITU). To further strengthen ASEAN's collective digital resilience, such programs should be expanded. ASEAN can establish a digital ecosystem where human rights, privacy, and security live peacefully, resulting in cyberspace that benefits everyone, by bringing together governments, the business sector, and young people.

In addition to protecting the fundamental human rights that are essential to the region's ongoing prosperity and unity, the active participation of youth in these processes will guarantee that ASEAN countries maintain their resilience in the face of changing digital threats.

Conclusion

The delicate balance between privacy, security, and human rights must be carefully considered as ASEAN negotiates the challenging world of cybersecurity. The modern environment involves complex decisions that affect both individuals and civilizations, rather than simple choices. The region cannot afford to allow personal privacy to be compromised or liberties to be restricted due to fear of cyber threats. Reacting is insufficient; ASEAN needs to take the initiative and create policies that empower rather than just defend.

I strongly believe that fairness and inclusivity must be the cornerstones of ASEAN's future. This entails making sure that legislative frameworks are fair by involving marginalized communities in the policymaking process. Fairness necessitates accountability and channelsfor redress, whileinclusivity demands proactive involvement. When combined, these ideas can assist ASEAN in creating a digital future where everyone's rights are respected, security is upheld, and no one is left behind.

The younger generation, which is familiar with the digital world, can bring about significant change at this crucial juncture. Theircapacity to challenge the status quo and close generational gaps in knowledge has the potential to completely transformASEAN's approach to human rights and cybersecurity. This is a shared obligation that calls for innovative thinking, teamwork, and bravery; it is not just a problem for legislators. Although the road ahead is not withoutchallenges, ASEAN can build a digital environment where everyone may prosperin a safe and just manner by enriching minds, empowering the youth, and protecting our rights.

BIBLIOGRAPHY

- Abalos, F. O. (2024, July 19). Pogos: Pros and cons. Philstar.com. https://www.philstar.com/the-freeman/cebu-business/2024/07/20/2371602/pogos- pros-and-cons
- “AI, Privacy, and Data Protection: Legal Considerations in Southeast Asia.” Tilleke & Gibbins. AccessedNovember 22, 2024.https://www.tilleke.com/insights/ai-privacy-and-data-protection-legal-considerations-in-southeast-asia/.
- ASEAN. “The Right to Data Privacy in the Digital Economy.” The ASEAN Magazine, November 10, 2024. https://theaseanmagazine.asean.org/article/the-right-to-data- privacy-in-the-digital-economy/.
- “Data and Privacy Protection in ASEAN.” (2018) Deloitte. Accessed November 22, 2024. https://www2.deloitte.com/content/dam/Deloitte/sg/Documents/risk/sea-risk-data- privacy-in-asean.pdf.
- Dela Cruz, John Michael, and Maricar Navarro. (2024) “Perceived Impact of Mandatory SIM Card Registration to Cybersecurity and Data PrivacyAmong Engineering Students in Technological Institute of the Philippines.” https://doi.org/10.46254/AN14.20240360., February 12, 2024.
- Foucault, Michel.Discipline and Punish the Birth of the Prison. New York: Vintage Books, 1979.
- ILGA Asia. “Joint News Release by the ASEAN Regional Coalition to #stopdigitaldictatorship.” ILGA Asia, March 12, 2024. https://www.ilgaasia.org/news/2024/3/12/joint-news-release-by-the-asean- regional-coalition-to-stopdigitaldictatorship.
- Indonesia’s tax agency probes alleged Personal Data Breach | Reuters, September 2024. https://www.reuters.com/world/asia-pacific/indonesias-tax-agency-probes-alleged-personal-data-breach-2024-09-19/.

- Karnjanatawe, Karnjana. “Call Centre Gangs Exploit Vulnerable Victims.” December 3, 2023.https://www.bangkokpost.com/thailand/general/2697239/call-centre-gangs-exploit-vulnerable-victims.
- Mateo, Janvic. “Sim Registration Law Failed to Curb Scams – Group.”Philstar.com, June 20, 2024. https://www.philstar.com/nation/2024/06/21/2364394/sim-registration-law-failed-curb-scams-group.
- Qatar tops countries in Global Cybersecurity index 2024. Accessed November 22, 2024. https://www.qna.org.qa/en/News-Area/News/2024-09/13/0037-qatar-tops-countries-in-global-cybersecurity-index-2024.
- Tham, Irene. “Personal Info of 1.5m SingHealth Patients, Including PM LEE, Stolen in Singapore’s Worst Cyber Attack.” The Straits Times, October 1, 2021. https://www.straitstimes.com/singapore/personal-info-of-15m-singhealth-patients- including-pm-lee-stolen-in-singapores-most.

YOUTH DIGITAL ACTIVISM IN INDONESIA: BEHAVIORAL DRIVERS MODEL IN REDUCING POLITICAL POLARISATION

ABSTRACT

Social media has evolved into a platform for communication and a site of conflict. Communities' solidarity and trust are at risk due to political polarisation, worsened by echo chambers that magnify attitudes and suppress opposing viewpoints. Despite this challenge, youths in Indonesia are a potent force for transformation. They can bridge gaps through digital action, but what makes them successful? Four main variables are examined in this essay as it focuses on the reasons behind youth digital activism: self-efficacy, risk perception, extrinsic motivation, and intrinsic drive. The results of an analysis of youth behaviour using Structural Equation Modelling show that self-efficacy, or confidence, is the most potent motivator for effective activism. However, risk perception, or fear of retaliation, frequently prevents it. The results also reveal how motivation is increased by digital engagement, transforming values and affirmation into tangible effects. The findings result in practical solutions: equip youth with digital skills to improve their self-efficacy, establish safer online spaces to lessen anxieties, and acknowledge their attempts to motivate others. One post at a time, Indonesia's youth can become the bridge makers in a world where digital walls divide people, transforming differences into harmony.

Keywords: Youth Digital Activism; Self-efficacy; Risk Perception; Political Polarization; Digital Engagement

AUTHOR:

LAZUARDI IMANI HAKAM

(INDONESIA)

Introduction

Political polarization has emerged as one of Indonesia's most significant digital issues. Social media first hailed as a tool for promoting cooperation and communication, has inadvertently widened ideological gaps. Algorithms meant to increase engagement frequently prioritize sensational or emotionally charged content, resulting in echo chambers, digital environments in which users are predominantly exposed to information that supports their opinions. Tensions between groups with different political philosophies are heightened, biases are reinforced, and exposure to other viewpoints is diminished.

There are severe repercussions of political polarization in Indonesia. It damages healthy dialogue, erodes community trust, and obstructs coordinated efforts to address urgent national concerns. Online debates often turn heated, with polarizing rhetoric and false facts escalating the conflict. Ideologically opposed parties' growing mistrust of one another has strained real-life connections and fractured online contacts.

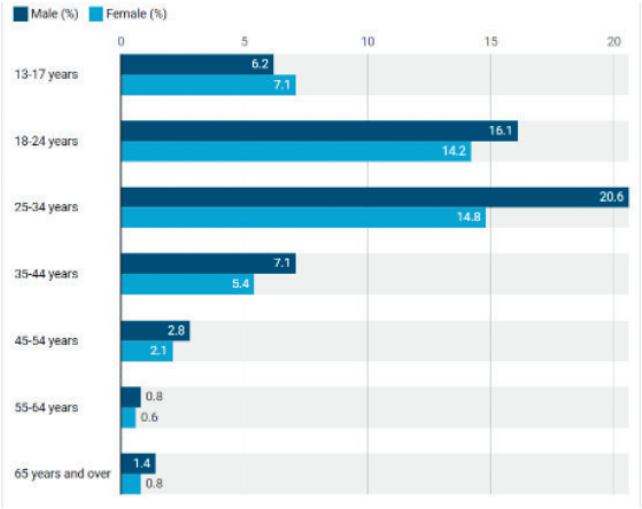


Figure 1. Statistical data of Indonesian social media users by age group (Statista, 2021).

Data from statistics highlights how urgent this problem is (Figure 1). With 20.6% of men and 14.8% of women regularly using social media, the most significant demographic of Indonesian social media users is between the ages of 25 and 34 (Statista, 2021). The 18–24 age group comprises 14.2% of women and 16.1% of men and is the second-largest demographic.

These numbers demonstrate how young people predominate on Indonesian internet platforms. Youth are the main forces behind social media use in ASEAN, where similar demographics predominate. This commonality implies that young people are most affected by and best suited to spearhead initiatives to combat digital polarisation.

Young people in Indonesia are uniquely positioned to address these dynamics because they represent most online users. Through digital activism, people can advocate for unity, encourage communication across divides, and promote inclusive narratives. Their goals, risk perceptions, and belief in their ability to make change are some variables that affect their ability to contribute effectively.

The behavioural drivers of youth participation, such as self-efficacy, risk perception, extrinsic incentive, and intrinsic motivation, are the main emphasis of this essay, which also looks at how these characteristics affect the success of the activism and the engagement of the young. The essay's conclusion, backed by results from Structural Equation Modelling (SEM), offers practical suggestions for empowering Indonesian youth and, consequently, ASEAN youth as instrumental players in promoting unity and combating political polarisation.

Political Polarisation in Indonesia

Political polarisation in Indonesia has grown more vital in the digital age. As the main forum for political conversation, social media frequently worsens rifts between parties with different philosophies. The nature of these platforms emphasises sensational and contentious content rather than encouraging open conversation, which results in fragmented discussions and the emergence of echo chambers, online areas where people only encounter information and ideas that support their own convictions (Soderborg & Muhtadi, 2023).

Platform algorithms like those on Facebook, Instagram, X and TikTok are developed to optimise user interaction. This strategy boosts engagement on these platforms but also gives preference to information that elicits strong emotional responses, frequently at the expense of nuanced or balanced viewpoints. Because of this, users are constantly exposed to content that confirms their prejudices, which leads to a culture in which opposing viewpoints are either ignored or ostracised.

Widespread dissemination of polarising content, such as sensational headlines, memes, and Photoshopped photos, deepens ideological divisions. Because of these dynamics, there is an increasing sense of "us versus them," where opposing factions see one another as enemies rather than fellow citizens.

Political polarization has repercussions that go beyond the internet. At the level of society, polarization has resulted in (Abdi Mohamed Qasaye, 2024; Lee, 2022):

- Social Trust Erosion. People's mistrust of those with different political opinions is growing, threatening the solidarity required to tackle common problems.
- Community Fragmentation. Disagreements stoked by online political discourse have caused rifts in families, localities, and companies.
- Decreased constructive dialogue. Finding common ground or reaching an agreement is challenging when social and political discussions become antagonistic.

In Indonesia, where cultural variety is essential to national identity, such divisions endanger societal cohesion. The fundamental ideals of unity and mutual respect that inspire the country's motto, Bhinneka Tunggal Ika (Unity in Diversity), are threatened. Social media presents chances to combat polarization despite these obstacles. Digital platforms can be used to (Aruguete, 2024; Lu et al., 2024):

a. Spread stories that highlight common ideals and objectives.
b. Promote inter-ideological dialogue by facilitating moderated conversations.
c. Give voice to those who advocate for harmony, understanding, and tolerance.

Digital activism by youth is essential to these initiatives. As the most active social media users in Indonesia, youths have the power to dismantle echo chambers, oppose divisive discourse, and establish forums for inclusive discussion. However, addressing the behavioural factors that affect their participation, such as desire, risk perception, and self-efficacy, is necessary if they are to do this. In the sections that follow, these aspects are examined in more detail.

Behavioral Drivers of Youth Digital Activism in Reducing Political Polarisation

Four significant aspects influence how well digital youth activism addresses political polarisation: self-efficacy, risk perception, extrinsic motivation, and intrinsic motivation. These behavioural drivers have their roots in well-established theories and offer a framework for comprehending the motivations behind and methods by which youth participate in online activism.

Intrinsic Motivation. Intrinsic motivation describes the beliefs and sense of accountability that motivate an individual to participate. Self-determination theory (Deci & Ryan, 1985) states that intrinsic motivation takes place when activities align with firmly held beliefs and give one a feeling of direction. For youths who support fostering harmony in society, inclusivity, or togetherness, this may entail engaging in activism. As shown in the case of the Save KPK movement in Indonesia, intrinsic motivation, such as the desire to share credible and truthful information, significantly drives digital activism and helps combat misinformation, ultimately enhancing civic engagement (Suwana, 2020). For example, a young activist may publish anti-hate or pro-tolerance messages because they feel compelled to act morally, not for attention. Even in difficult or divisive situations, this innate motivation guarantees continued engagement. Since intrinsic motivation fosters sustained dedication and meaningful engagement, research continuously demonstrates that it significantly improves the effectiveness of activism.

Extrinsic Motivation. External factors like rewards, acknowledgement, and social validation are examples of extrinsic motivation. Self-determination theory also explains how extrinsic motivation complements intrinsic motivation by offering external feedback that promotes consistent engagement (Aruguete, 2024; Shen et al., 2022). Young people involved in internet activism are frequently inspired by encouraging comments, likes, and shares on their posts. As demonstrated by (Lilleker & Koc-Michalska, 2017), recognition from peers or social networks plays a pivotal role in motivating individuals to participate in digital activism, thereby expanding their involvement in civic actions. Receiving praise from friends, neighbours, or even influential people encourages them to keep working hard. For instance, a social media post that promotes togetherness and receives much support may inspire the author to make further contributions. Extrinsic drive increases activism by promoting regular and broader participation, albeit less personal.

Risk Perception. According to Risk Perception Theory (Slovic, 1987), risk perception is used to characterise worries or anxieties around possible unfavourable outcomes of the activity. These risks may consist of:

- Cyber harassment: Being the target of personal attacks, threats, or trolling on the internet.
- Reputational harm: Having people stigmatise, label, or misinterpret you.
- Legal repercussions: Fears about breaking rules or laws about internet speech.

A high-risk perception deters young people from participating in politically sensitive conversations or initiatives. Based on a study conducted by (Dal et al., 2023), emotional responses to perceived risks in online activism, particularly in authoritarian contexts, significantly influence decision-making about political expression, often deterring participation. For instance, a young individual may refrain from voicing a contentious viewpoint regarding political unity out of concern for possible adverse reactions. According to the study, activism effectiveness and participation are adversely affected by risk perception. Resolving these anxieties is essential to fostering an atmosphere where young people can freely voice their opinions and participate in discussions.

Self-Efficacy. According to Social Cognitive Theory (Bandura, 1977), self-efficacy is the conviction that one can accomplish goals. Self-efficacy was the most reliable indicator of successful digital activism among the four factors. Research has demonstrated that self-efficacy plays a critical role in empowering individuals to engage in digital activism, as it enhances their ability to organise collective actions and utilise digital platforms effectively for impactful societal contributions (Velasquez & LaRose, 2014). Young people who believe in themselves are more likely to:

a. Produce powerful and captivating digital material like articles, videos, or infographics.
b. Encourage civil and fruitful dialogue across differences of opinion.
c. Fearlessly confront false information and divisive narratives.

For instance, a young activist with high self-efficacy might spearhead a campaign encouraging communication between disparate groups. Their self-assurance in their abilities guarantees the calibre and effect of their activity and encourages engagement. The results emphasise the necessity of equipping young people with digital tools, resources, and training to boost their self-efficacy and enable them to make valuable contributions to lessening polarisation.

Understanding the Pathways to Effective Youth Digital Activism

This study examines how youths in Indonesia use digital activism to address political polarisation based on survey of 300 participant. The study uses a technique known as SEM to examine four important aspects of their activism: self-efficacy, risk perception, extrinsic motivation, and intrinsic motivation (Figure 2). It also examines how digital participation, which serves as a conduit between their goals and the effectiveness of their activism, either strengthens or weakens these aspects.

In Indonesia, young people dominate social media use; comprehending these dynamics is crucial to enacting significant change.

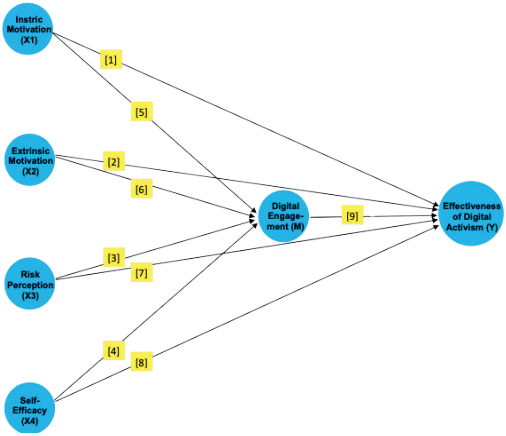


Figure 2. Youth Digital Activism Effectiveness Model

The path analysis enables us to comprehend how many elements impact how youth digital activism works to lessen political polarisation. It demonstrates both direct relationships, how each element influences activism outcomes on its own, and indirect relationships, how these elements cooperate to strengthen activism through digital interaction.

Direct Effects and Indirect Effects

The result of the study in Table 1 shows that self-efficacy, or the belief in one's capacity to impact, is the most significant variable influencing successful activism. It has a considerable positive effect (coefficient = 0.372), meaning that young people are more disposed to lessen polarisation if they believe they can provide engaging content or participate in meaningful conversations. Likewise, intrinsic drive stems from internal values such as a desire to foster togetherness and has a significant beneficial impact (coefficient = 0.325).

Table 1. Direct and Indirect Effect, SEM analysis results

No.	Path	Coefficient	t-value	p-value	Significance
Direct Effects					
[1]	Intrinsic Motivation (X1) → Effectiveness of Digital Activism (Y)	0.325	15.114	0.000	***
[2]	Extrinsic Motivation (X2) → Effectiveness of Digital Activism (Y)	0.299	7.199	0.000	***
[3]	Risk Perception (X3) → Effectiveness of Digital Activism (Y)	-0.231	-8.764	0.000	***
[4]	Self-Efficacy (X4) → Effectiveness of Digital Activism (Y)	0.372	8.208	0.000	***
Indirect Effects					
[5]	Intrinsic Motivation (X1) → Digital Engagement (M) → Effectiveness of Digital Activism (Y)	0.103	2.163	0.031	*
[6]	Extrinsic Motivation (X2) → Digital Engagement (M) → Effectiveness of Digital Activism (Y)	0.078	6.598	0.000	***
[7]	Risk Perception (X3) → Digital Engagement (M) → Effectiveness of Digital Activism (Y)	-0.055	-2.845	0.004	**
[8]	Self-Efficacy (X4) → Digital Engagement (M) → Effectiveness of Digital Activism (Y)	0.082	3.124	0.002	**

*** : Highly significant ($p \leq 0.001$)

** : Significant ($p \leq 0.01$)

* : Marginally significant ($p \leq 0.05$)

Another factor is extrinsic motivation, which has a moderately beneficial impact (coefficient = 0.299) and includes external incentives or praise. Peer or community support and encouragement can maintain youth engagement. However, risk perception negatively impacts activism, which includes worries about harassment, retribution, or damage to one's reputation (coefficient = -0.231). Young people need to be more motivated to fully engage in internet initiatives to lessen polarization by these threats.

The analysis further emphasizes the significance of digital interaction as a mediator. Young people increase the impact of their motives when they actively engage in online activities, such as posting inclusive messages, participating in debates, or producing material. For instance, young people who are intrinsically motivated are more likely to use digital platforms, increasing their activism's impact (indirect effect = 0.103). Likewise, self-efficacy has a beneficial impact on digital participation, increasing activism's impact (indirect effect = 0.082). However, a high-risk perception decreases the total effectiveness of activism by decreasing digital involvement (indirect effect = -0.055).

Recommendations

Adopting policies that support adolescent digital activism should be a top priority for policymakers, who should emphasize that confidence is the primary factor influencing efficacy. Programs that improve self-efficacy by developing digital skills in areas like campaign management, communication, and content creation should be funded by governments, academic institutions, and civil society organizations. Mentorship programs, workshops, and the inclusion of digital literacy in school curricula can give young people the self-assurance they need to take an active part in online activism. Since concerns about cyberbullying and potential legal consequences discourage participation, addressing risk perception is equally crucial. Social media companies and legislators should work together to enhance safety features like more robust content filters and reliable reporting mechanisms. Campaigns to raise public awareness can teach young people about their digital rights and how to safeguard their online identity. Furthermore, regulatory frameworks must balance accountability and freedom of expression to promote open, secure participation. More youth involvement can be encouraged by cultivating intrinsic motivation through value-based initiatives prioritizing peace, tolerance, and respect. Young people are more committed to societal change when they can see the results of their work when digital activism is connected to concrete results.

Extrinsic motivation can also be increased by praising and rewarding activism through projects demonstrating accomplishment. To create a more inclusive digital environment and increase the impact of young activism, governments and tech corporations must work together to develop algorithms that minimise echo chambers and promote inter-ideological discussion.

Conclusion

Social media platforms' tendency to promote political polarization in Indonesia poses an increasing threat to social cohesiveness. Youth internet activism, which encourages inclusive narratives and inter-ideological discussion, provides a hopeful remedy. However, the number of behavioural characteristics determines how effective their activism is. This study shows that self-efficacy, or the belief in one's capacity to bring about significant change, is the most critical factor influencing effective activism. Young people who are intrinsically motivated, driven by their ideals and a sense of duty, are also more likely to participate successfully. Risk perception is a significant obstacle, preventing many young people from altogether participating, even while extrinsic motivation, such as praise and encouragement, reinforces their involvement.

The mediating function of digital engagement underscores the significance of active participation in enhancing the impact of their endeavours. Addressing these elements with targeted activities is necessary to optimise the potential of youth digital engagement in lowering political polarisation. Fostering an atmosphere that encourages action requires boosting young people's self-esteem, lowering perceived risks, and maintaining internal and external motives.

BIBLIOGRAPHY

- Abdi Mohamed Qasaye, O. (2024). Political Polarization and its Impact on Democratic Institutions. International Journal of Science and Research (IJSR), 13(1), 1132–1137. https://doi.org/10.21275/sr24116110024
- Aruguete, N. (2024). Content Sharing Dynamics and Political Polarization in Social Media. In M. Goyanes & A. Cañedo (Eds.), Media Influence on Opinion Change and Democracy: How Private, Public and Social Media Organizations Shape Public Opinion (pp. 215–230). Springer Nature Switzerland. https://doi.org/10.1007/978-3-031-70231-0_13
- Bandura, A. (1977). Self-efficacy: Toward a unifying theory of behavioral change. Psychological Review, 84(2), 191–215. https://doi.org/10.1037/0033-295X.84.2.191
- Dal, A., Nisbet, E. C., & Kamenchuk, O. (2023). Signaling silence: Affective and cognitive responses to risks of online activism about corruption in an authoritarian context. New Media and Society, 25(3), 646–664. https://doi.org/10.1177/14614448221135861
- Deci, E. L., & Ryan, R. M. (1985). Intrinsic Motivation and Self-Determination in Human Behavior. Springer US. https://doi.org/10.1007/978-1-4899-2271-7
- Lee, A. H. Y. (2022). Social Trust in Polarized Times: How Perceptions of Political Polarization Affect Americans' Trust in Each Other. Political Behavior, 44(3), 1533–1554. https://doi.org/10.1007/s11109-022-09787-1
- Lilleker, D. G., & Koc-Michalska, K. (2017). What Drives Political Participation? Motivations and Mobilization in a Digital Age. Political Communication, 34(1), 21–43. https://doi.org/10.1080/10584609.2016.1225235
- Lu, J., Sun, M., & Liu, Z. (2024). Social Media and Political Polarization: A Panel Study of 36 Countries from 2014 to 2020. Social Indicators Research. https://doi.org/10.1007/s11205-024-03367-y
- Shen, Y., Zhang, S., & Xin, T. (2022). Extrinsic academic motivation and social media fatigue: Fear of missing out and problematic social media use as mediators. Current Psychology, 41(10), 7125–7131. https://doi.org/10.1007/s12144-020-01219-9
- Slovic, P. (1987). Perception of Risk. Science, 236(4799), 280–285. https://doi.org/10.1126/science.3563507
- Soderborg, S., & Muhtadi, B. (2023). Resentment and Polarization in Indonesia. Journal of East Asian Studies, 23(3), 439–467. https://doi.org/10.1017/jea.2023.17
- Statista. (2021). Distribution of social media users in Indonesia as of January 2021, by age group and gender. Statista. https://www.statista.com/statistics/997297/indonesia-breakdown-social-media-users-age-gender
- Suwana, F. (2020). What motivates digital activism? The case of the Save KPK movement in Indonesia. Information, Communication & Society, 23(9), 1295–1310. https://doi.org/10.1080/1369118X.2018.1563205
- Velasquez, A., & LaRose, R. (2014). Youth collective activism through social media: The role of collective efficacy. New Media & Society, 17(6), 899–918. https://doi.org/10.1177/1461444813518391

BEYOND "REVENGE PORN": TACKLING NON-CONSENSUAL DISSEMINATION OF INTIMATE IMAGES AND RECOMMENDATIONS FOR VIETNAM

ABSTRACT

In Southeast Asia, particularly in Viet Nam, digital growth has opened doors to countless opportunities but also unleashed new dangers for women and girls. This essay unpacks the rising threat of non-consensual dissemination of intimate images (NCDII), or what some still colloquially call "revenge porn." Through the lens of real-life cases involving Vietnamese celebrities, it reveals the emotional toll, social stigma, and legal blind spots surrounding NCDII. More than just an isolated issue, NCDII reflects the cultural tensions between a rapidly modernizing digital society and deeply ingrained gender norms. The essay suggests for Viet Nam, ASEAN Member States, and Timor-Leste a more victim-centric approach and more innovative pathways which may enable a more comprehensive policy response, tech-driven solutions, and collective regional cooperation that leads to more effective, educative, and preventative strategies.

Keywords: Revenge Porn; Image-based Sexual Abuse; Non-consensual Pornography; ASEAN Digital Transformation

AUTHOR:

HOANG THI NGOC MAI

(VIET NAM)

Setting the scene

We are walking on the thin barriers between the digital and the real world since the line is fading bit by bit due to the increasing digitalization of contemporary society. Consequently, the online dimension can no longer be considered as an intangible and distant reality. On the contrary, it is now considered an essential feature of our life, our second identity, and our medal of social networking. Especially in Southeast Asia, one of the youngest regions in the world as 60% of the population is under 35, even the most ordinary life can not escape the buzzing of digital transformation, connecting millions and reshaping lives.

In Viet Nam, a country where rapid digital growth meets deep-rooted cultural complexities, the impact of these digital phenomena becomes evident. As one of ASEAN's most dynamic digital economies, Viet Nam reflects both the promises and pitfalls of this digital age.

In November 2024, MCK, a popular Vietnamese rapper, faced a wave of backlash after an intimate image of him was leaked online. This incident brought the author back to the case of Hoang Thuy Linh, a well-known actress and singer in the 2010s, whose private video went viral across Viet Nam's top social platforms. Despite the severe emotional toll on both celebrities, Vietnamese netizens largely dismissed their distress. Instead of empathy, Hoang Thuy Linh became the target of relentless misogynistic comments, accused of violating an undefined notion of "moral dignity." This ambiguous concept, deeply rooted in cultural judgment, continues to intrude on the personal spaces of women and girls, both online and offline, making anyone a potential victim.

By numbers alone, women and girls are disproportionately affected by technology-facilitated gender-based violence (TFGBV). As a result, in this essay, I believe "revenge porn" and other manifestations of technology-facilitated gender-based violence (TF-GBV) and non-consensual dissemination of intimate images (NCDII) are rising threats across the region, which need to be addressed and mitigated to protect women and young girls in Viet Nam and ASEAN region.

Overview and definitions

The 2020 global survey on young people's experience of online abuse and harassment, conducted by The World Wide Web Foundation and the World Association of Girl Guides and Girl Scouts, found that 52 percent of young women and girls have experienced online

abuse, including threatening messages, sexual harassment and the sharing of private images without consent; and young people's top concern is the sharing of private photos, videos or messages without their permission – 30 percent said it is what worries them most ("Internet Safety Day - Online harassment," 2020). In Asia scope, image-based abuse is the third most frequently mentioned form of gender-based and sexual harassment (Bansal, et.al., 2023).

Image-based sexual abuse falls into the sixth division of gender-oriented cyberviolence published by the UNESSCO-ITU which is "malicious distribution" ("Cyber Violence Against Women And Girls: A World-Wide Wake-Up Call," 2015) - "both the act of distributing and manipulating private content usually of sexual nature without the consent of the victim and threatening to commit such act". The European Court of Human Rights in Volodina v. Russia also detected 5 features that uniquely characterized cyberviolence against women and girls, consisting of the anonymity of the perpetrator which may cause difficulties in identifying the offender, the distance through which physical harm is not a prerequisite, the accessibility of technology which means the vast number of technologies available to commit crime, automation, propagation, and perpetuity.

Later, the Special Rapporteur added other features typical of the digital dimension such as the "global searchability", replicability, and scalability of data which may result in a re-victimization of the woman abused in their report on violence against women (UNHRC, 2018). Image-based abuse has various manifestations including non-consensual distribution of intimate images (NCDII), sexploitation, sextortion, "Deepfake", "Doxing", "Upskirting" and "Coercing". With the rapid evolution, more shapes of non-consensual intimate image abuse are forming and invading the freedom of being online for women and girls.

Understanding the non-consensual dissemination of Intimate images

In modern days, internet users colloquially use the term - "revenge porn". However, the word "revenge" failed to focus on the harm inflicted on the survivors and shift the spotlight on the perpetrator's motives, misleadingly reducing the criminal applicability to cases where the distribution is linked to vengeance. "Porn" or "Pornography" also describes "pleasure, content, and consent" which has nothing amplified in the cases of hurting victims by image-based abuse. However, in this essay, I still choose to use the term "revenge porn" in some scenarios for its fitting context.

“Revenge porn” is disturbingly big business running wild for a while. However, the number of cases revealed under the sun is only the tip of the iceberg. For example, Hunter Moore’s notorious website “Is Anyone Up?” which regularly featured “revenge porn” was said to receive over 300,000 unique visitors every day in 2012 (Stern, 2012) or the Nth Room scandal of South Korea in 2020 where women and minors were coerced into sharing explicit images, which were then distributed and monetized in online chat rooms.

In 2024 “revenge porn” has evolved from making their ex-partner feel regret, humiliation, or damaging their self-image (Sirianni, 2016) to another level of sex trafficking. In November, Reuter revealed hundreds of girls had been held captive, terrorized, and sexually enslaved to monetize porn from OnlyFans by their partners and ex-partners. The cases recently revealed are getting more technologically complex and sophisticated, enabling enslavement and organized crime to be done in new approaches and prevent charging the offenders and investigating their techniques. Due to the unsanitized database market among tech companies and third-party applications, the database of millions of users is displayed like a buffet line for cybercriminals to track personal information and online activity.

Impacts of Non-consensual Dissemination of Intimate Images

While the literature misses the spotlight on the effect of NCDII on mental health, several stories of victims who have attempted or committed suicide after the incidents are reported on the media. Studies on targets of NCDII have reported symptoms of poor mental health, anxiety, depression, post-traumatic stress disorder, low self-esteem, self-harm, and somatic symptoms being the most common experiences (Bates, 2017). This form of violence can be relentless and widespread, leaving no space to escape.

From the interpersonal perspective, the victims of NCDII would suffer from internalizing problems which later result in trust issues in relationships and social functions. Some deal with mental health impacts, while others are exhausted from managing the aftermath. At the same time, most of them live in constant anxiety as they are not sure about whether their pictures are still circulating on the Internet.

Except for different degrees of emotional damage, victims would universally face ruined reputations and struggles in real life. One Nigerian research among 27 victims of NCDII reported that 19 participants affirmed being compelled to change their ordinary lives as a consequence of the leak, including those who lost their studentship or voluntarily withdrew from schools and work (Aborisade, 2021).

The emotional and psychological stressors caused by NCDII have tangible real-world impacts on women, making it difficult for them to focus on school and work, later affect every aspect of their life including reconnecting with their family and friends, finding and maintaining a job, mental and emotional stress, building a healthy relationship, feeling comfortable with their body, etc. Moreover, the whole experience of NCDII has caused women a forever scar of being online, silencing their voice on social media platforms, causing them to self-censor, and reducing or ending their participation in digital discussion and leadership roles.

Existing Challenges for Combating NCDII

"Why did she send it in the first place?"

This is a predictable comment under the title of another girl's exposed image spreading online. This reflects a sexual double standard theory where women are judged more harshly than men for comparable sexual behaviors. This societal stigma is one of the key obstacles for victims walking past their internal guilt while in the first place, they were not permitting the image to be viewed by anyone else but the intended recipient. The one who should be protected is now feeling physically unsafe while the one who just committed a "crime" runs free and remains unknown. When NCDII was educated and well-recognized globally, legal gaps in defining and prosecuting NCDII as well as ethical problems blocked the way to justify the victims. Sexual "Deepfake" technology alerts a higher threat to the concept of "revenge porn" since it can superimpose on an individual's face in pornography and generate intimate images and videos with neither the acknowledgment nor consent of the victim. As a result, unsupervised technology combined with uncautious cybersecurity created a dilemma where anyone whose images are captured and posted on digital space is fair game to be the victim. This misuse of technology has benefited the attacker more than the victims as the fake videos could be weaponized to coerce the threatened into providing real intimate images to the abusers.

Despite a widespread issue globally, research and data on reported cases of NCDII in specific regions and countries such as ASEAN and Viet Nam have been poorly investigated leading to our understanding of the true prevalence remains murky. However, Viet Nam and ASEAN have the needed foundation to construct a healthy online environment and enact innovative laws addressing gender-based violence (GBV) in digital spaces.

ASEAN countries are observing a growing investment in digital infrastructure and digital literacy, heavily in 5G networks, cloud computing, and smart city initiatives such as Thailand's Eastern Economic Corridor and Malaysia's Cyberjaya. Moreover, strong regional collaboration and supportive national policy frameworks from governments and NGOs such as ASEAN Digital Masterplan 2025 and Viet Nam's National Digital Transformation Program have signaled a collective response to regional digital challenges such as TFGBV and NCDII.

In 2021, Viet Nam's Institute for Social Development Studies (ISDS) is supporting UK Revenge Porn Helpline's launch of StopNCII.org to help stop the non-consensual sharing of intimate images (NCII) on the internet. Established in 2015, UK The Revenge Porn has become the assistant for many young women in removing intimate images from digital platforms with over 330,000 successful images removed. The success of The Revenge Porn Helpline varies in many factors: their victim-centered services, their intensive input of many stakeholders such as survivors, experts, advocates, and tech partners, and most important, their continuum work with government and Parliament to advocate for necessary changes in the law.

Recommendations

By building better consensus around definitions and data and developing tailored programs and policies for this violence. First of all, the Vietnamese government should update and reform legislative frameworks and deliver broad awareness of GBV online. Until the time of this essay, victims of non-consensual dissemination of intimate images in Viet Nam have limited legal recourse, often resorting to suing for defamation rather than specific protection under GBV laws. In the specific socio-economic context of Viet Nam, the government should encourage and distribute more community talks and national-level discussions on digital literacy, cybersecurity, and GBV online. ASEAN Member States and Timor-Leste could adopt similar measures by integrating digital literacy programs and raising public awareness, which would serve as the groundwork for improving victim support services and legal protection across the region.

Secondly, the government needs to work closely with social media companies to pressure them to create effective and accessible reporting mechanisms that target GBV and constantly improve their content moderation.

At the moment, most social media platforms have community standards supervised by both AI and human forces to ban users from posting sexual images and images containing revealed parts of the body. However, the potential of one picture passing the AI censorship appearing in the digital space and maintaining a forever digital footprint is still there. Learning from countries like Germany, which implemented the Network Enforcement Act to strengthen platform accountability, Viet Nam and the ASEAN Member States could push for tighter regulations. These might include requiring social media platforms to verify user identities and track malicious activities, making it easier to collect data, hold perpetrators accountable, and assess the scale of digital GBV across the region.

Thirdly, ASEAN is home to a growing number of tech start-ups and innovation ecosystems particularly in Singapore, Indonesia, and Viet Nam. ASEAN Member States should encourage technology companies to work on their corporate social responsibility (CSR) in combatting NCDII. In recent years, "women in STEM" globally acknowledged has stated that women are taking more pieces of the cake in male-dominant fields such as technology. The penetration of more female voices in gender equality and gender sensitivity in technology indicates a significant change in social platforms policy as well as more technology solutions combating NCDII directly. For example, The UK Revenge Porn Helpline, in consultation with Meta (formerly Facebook), has developed a more secure and trusted report system to take down unwanted private images and flag hostile users in digital space.

Fourth, Viet Nam is sleeping on the importance of gender education and gender-based conversation between parents and children, between educators and learners. This ignorance leaves a wide range of young people unprepared and vulnerable when incidents occur. Applying the success of the "Talk to Someone You Trust" campaign raised by Miss Dominican Republic in 2019 where she used her large online audience and her social impact as a female representative of the nation to highlight the key of communication and mutual support for the victims in the incidents. Viet Nam and other ASEAN states can apply and multiply this model to institutions, workplaces, and community support where women, young girls, and people from vulnerable groups can find sources of strength from other experienced mentors, creating a healthy social network of womanhood. Training educators on the risks of NCDII would also ensure they adopt emotional support strategies and know how to report incidents.

Lastly, one of the most valuable lessons from Viet Nam is the urgency of improving data collection and research on NCDII and TF-GBV. In Viet Nam, research and data in this area are still underdeveloped, and cases are often highlighted only through tabloids and social media posts. Viet Nam's experience reminds the region that achieving a gender-sensitive digital environment requires the joint effort of governments, tech companies, civil society organizations, and communities at large. ASEAN Member States and Timor-Leste should invest in national research initiatives to systematically collect data and create anonymous reporting platforms for victims and bystanders. Before that idealistic vision, a healthy and gender-sensitive online dimension requires help from not only the development researchers but also the joint hands of all stakeholders in the community. Each of us is a vital factor in building a healthy and resilient digital environment without GBV in general.

From policy gaps to grassroots movements, Viet Nam's experience holds the potential to inspire more inclusive and safer online spaces across ASEAN, proving that local efforts can spark broader change.

Conclusion

As digital and online technology is integrated into social and sexual life, it can operate as a new medium for the reproduction and intensification of GBV. The first two cases of two popular Vietnamese celebrities mentioned in the beginning were two insightful marks of a timeline that reflected different social tendencies towards different gender-based incidents. Their cases in two decades embark on how NCDII is worth more attention in Vietnamese discussion. The shortage of reported cases and research in Vietnamese or on the Viet Nam border also alerts the biased ignorance and the poor support systems to which victims are out of touch and under-protected. It is important to provide victims and survivors financial, psychological, and legal assistance as well as deliver digital curricula on how to be safe online and prevent acts of online harassment, specifically NCDII, cyberbullying, threatening communication, and gender rolling.

Exploring how Viet Nam addresses TF-GBV and NCDII is more than just a national case study; it offers valuable lessons for the entire region. Addressing NCDII and GBV in Viet Nam requires collective actions from multiple actors, including government authorities, law officials, NGOs in Viet Nam, technology companies, scholars and communities, and members of communities. Armed with a common but contextually nuanced understanding of GBV, gender norms, and taboos surrounding sex and sexuality, these actors can work accordingly to mitigate and respond to future NCDII in a timely and informative manner.

Lastly, one of the most valuable lessons from Viet Nam is the urgency of improving data collection and research on NCDII and TF-GBV. In Viet Nam, research and data in this area are still underdeveloped, and cases are often highlighted only through tabloids and social media posts. Viet Nam's experience reminds the region that achieving a gender-sensitive digital environment requires the joint effort of governments, tech companies, civil society organizations, and communities at large. ASEAN Member States and Timor-Leste should invest in national research initiatives to systematically collect data and create anonymous reporting platforms for victims and bystanders. Before that idealistic vision, a healthy and gender-sensitive online dimension requires help from not only the development researchers but also the joint hands of all stakeholders in the community. Each of us is a vital factor in building a healthy and resilient digital environment without GBV in general.

From policy gaps to grassroots movements, Viet Nam's experience holds the potential to inspire more inclusive and safer online spaces across ASEAN, proving that local efforts can spark broader change.

Conclusion

As digital and online technology is integrated into social and sexual life, it can operate as a new medium for the reproduction and intensification of GBV. The first two cases of two popular Vietnamese celebrities mentioned in the beginning were two insightful marks of a timeline that reflected different social tendencies towards different gender-based incidents. Their cases in two decades embark on how NCDII is worth more attention in Vietnamese discussion. The shortage of reported cases and research in Vietnamese or on the Viet Nam border also alerts the biased ignorance and the poor support systems to which victims are out of touch and under-protected. It is important to provide victims and survivors financial, psychological, and legal assistance as well as deliver digital curricula on how to be safe online and prevent acts of online harassment, specifically NCDII, cyberbullying, threatening communication, and gender rolling.

Exploring how Viet Nam addresses TF-GBV and NCDII is more than just a national case study; it offers valuable lessons for the entire region. Addressing NCDII and GBV in Viet Nam requires collective actions from multiple actors, including government authorities, law officials, NGOs in Viet Nam, technology companies, scholars and communities, and members of communities. Armed with a common but contextually nuanced understanding of GBV, gender norms, and taboos surrounding sex and sexuality, these actors can work accordingly to mitigate and respond to future NCDII in a timely and informative manner.

BIBLIOGRAPHY

- Aborisade, R. A. (2021). Image-Based sexual abuse in a culturally conservative Nigerian society: Female victims' narratives of psychosocial costs. Sexuality Research and Social Policy, 19(1), 220–232. https://doi.org/10.1007/s13178-021-00536-3
- Bansal, V., Rezwan, M., Iyer, M., Leasure, E., Roth, C., Pal, P., & Hinson, L. (2023). A scoping review of Technology-Facilitated Gender-Based violence in Low- and Middle-Income countries across Asia. Trauma Violence & Abuse, 25(1), 463–475. https://doi.org/10.1177/15248380231154614
- Champion, A. R., Oswald, F., Khera, D., & Pedersen, C. L. (2022). Examining the gendered impacts of technology-facilitated sexual violence: A mixed methods approach. Archives of Sexual Behavior, 51(3), 1607–1624. https://doi.org/10.1007/ s10508-021-02226-y
- CYBER VIOLENCE AGAINST WOMEN AND GIRLS: A WORLDWIDE WAKE-UP CALL. (2015). The Broadband Commission for Digital Development. https://networkedintelligence.com/wp-content/uploads/2019/02/Cyber_violence_Gender-report.pdf
- Dunn, S. (2020). Technology-Facilitated Gender-based Violence: An Overview. In Supporting a Safer Internet Paper. Centre for International Governance Innovation. Retrieved November 27, 2024, from https://www.cigionline.org/publications/technology-facilitated-gender-based-violence-overview/
- Eckert, S., & Metzger-Riftkin, J. (2020). Doxxing. The International Encyclopedia of Gender, Media, and Communication, 1–5. https://doi.org/10.1002/9781119429128.iegmc009
- Hicks, J. (2021). Global Evidence on the Prevalence and Impact of Online Gender-based Violence (OGBV). https://doi.org/10.19088/k4d.2021.140
- Internet Safety Day - Online harassment. (2020). In UReport. UNICEF. Retrieved November 27, 2024, from https://ureport.in/opinion/3983/
- Kreager, D. A., Staff, J., Felmlee, D., Zhang, H., & Veenstra, R. (2024). The Sexual Double Standard and Adolescent Stigma: A Sociometric and Comparative Approach. The Journal of Sex Research, 1–11. https://doi.org/10.1080/00224499.2024.2358144
- M. Sirianni, J. (2016). Bad Romance: Exploring the factors that influence revenge porn sharing amongst romantic partners. Online Journal of Communication and Media Technologies, 6(10/4/2016).
- McGlynn, C., Rackley, E., & Houghton, R. (2017). Beyond 'Revenge Porn': the continuum of Image-Based Sexual abuse. Feminist Legal Studies, 25(1), 25–46. https://doi.org/10.1007/s10691-017-9343-2
- Mckinlay, T., & Lavis, T. (2020). Why did she send it in the first place? Victim blame in the context of 'revenge porn.' Psychiatry Psychology and Law, 27(3), 386–396. https://doi.org/10.1080/13218719.2020.1734977
- Nguyen, H. (2021, December 6). Vietnamese NGO Contributes to Curb the Spread of Non-Consensual Intimate Images. VietnamTimes. Retrieved November 27, 2024, from https://vietnamtimes.org.vn/vietnamese-ngo-contributes-to-curb-the-spread-of-non-consensual-intimate-images-38272.html
- ONLINE HARASSMENT, DIGITAL ABUSE, AND CYBERSTALKING IN AMERICA. (2016). Center for Initiative Public Health Research. Retrieved November 27, 2024, from https://www.datasociety.net/pubs/oh/Online_Harassment_2016.pdf
- So, L., Marshal, A., Ilie, L., & Szep, J. (2024, November 14). Enslaved on OnlyFans: Women describe lives of isolation, torment, and sexual servitude. Reuters. Retrieved November 27, 2024, from https://www.reuters.com/investigates/special-report/onlyfans-sex-trafficking/
- State of the World's Girls 2020: Free to be online? (2020). Plan International. Retrieved November 27, 2024, from https://plan-international.org/uploads/2023/06/SOTWGR2020-CommsReport-edition2023-EN.pdf
- Thornton, B. (2024, October 14). Revenge Porn Helpline Visit Parliament to Address Non-Consensual Intimate Image Abuse. Revenge Porn Helpline. Retrieved November 27, 2024, from https://revengepornhelpline.org.uk/news/revenge-porn-helpline-visit-parliament-to-address-non-consensual-intimate-image-abuse/

TECHNOLOGY AS AN ENABLER: THE IMPORTANCE OF DIGITAL LITERACY

ABSTRACT

Technology can be leveraged to promote trust among households and businesses by improving digital security and innovations that can lead to a more resilient, competitive, and sustainable economy. Yet, I argue that technology is merely an enabler as scams continue to be prevalent and a notable concern. Thus, digital literacy is emphasised as an important factor to ensure that technology can enable trust rather than deteriorate it. Using Brunei and ASEAN as a case study, I show that Brunei has high levels of digital penetration, yet digital literacy and the use of digital technology can be characterised as developing. Online scams and digital fraud continue to grow in Brunei, underscoring the critical need to prioritise and enhance digital literacy across all levels of society. Similarly, other ASEAN Member States find similar scenarios. On a positive note, efforts to promote digital literacy in Brunei and the greater ASEAN region is in place. Policies such as the Digital Brunei Initiatives and the Digital Transformation Plan from the Ministry of Education must be strengthened and expanded to accelerate the development of digital literacy. This includes efforts from various stakeholders that includes the public, private, independent organisations and other relevant stakeholders. More importantly, ASEAN Member States must reaffirm its commitment to regional ASEAN initiatives aimed at advancing digital literacy, particularly those outlined in the ASEAN Digital Economy Masterplan 2025, to leverage technology to build trust in the economy.

Keywords: Digital Literacy; Trust; Scams; Digital Security; Consumer Behaviour

AUTHOR:

DR HAZWAN HAINI

(BRUNEI DARUSSALAM)

Technology as an Enabler: The Importance of Digital Literacy

According to the Merriam-Webster Dictionary, a scam is defined as a fraudulent or deceptive act (Merriam-Webster, n.d.). Scams have existed as long as human history, with the earliest known scam attributed to two Greek Merchants, who devised a scam on an insurance policy by attempting to sink an empty vessel. Fast forward to the twenty-first century, scams continue to plague the digital space, which includes malware, online scams, and various forms of phishing. Yet, some of these more sophisticated scams are nothing more than a progression of older scams, as phishing evolved from sending fraudulent letters or telephone impersonations to email phishing or via text messages. The point is that scams will exist as long as humans do, regardless of whether technology progresses or not.

Scams can erode trust in the economy as it can affect consumer confidence and foster a culture of suspicion, while increasing the cost of insurance that has negative implications on financial stability. In this essay, I argue the importance of digital literacy in promoting the role of technology as an enabler for building peace and trust. More specifically, I provide a 2x2 futures scenario and apply the case of Brunei and the Association of Southeast Asian (ASEAN) nations, where digital penetration rates remain high, yet, online scams remain prevalent, and the use of technology is less sophisticated. There is no doubt that technology is a strong enabler of peace and trust. However, the key word is "enabler" as technology is just a tool and not a means to the end.

On the macro-level, technology can be used to resolve conflict and peace including the protection of beings and assisting in post conflict peace building and construction (Bhardwaj and Kamari, 2018). For example, the use of big data and sentiment analysis can predict and provide early indicators for fostering engagement, as well as empower communities by enhancing citizen access to social media and information to combat fake news (Peace Direct, 2020; Vision of Humanity, 2020).

In my argument, I focus on the role of technology as an enabler of building trust in the economy, which can help reshape economic systems to become more competitive, resilient, and sustainable (World Economic Forum, 2024). Developing trust at the institutional level is important as it can create a virtuous cycle and promote further economic growth as businesses and households can benefit from lower transaction and frictional costs arising from mistrust and malpractice (Kallsh et al., 2021). As such, technology can promote peace and trust at both the macro-, meso- and micro-level.

Yet, as highlighted, scams exist as long as humans do, even as technology evolves. The common denominator here is humans, as agents who consume and use technology. Thus, the importance of digital literacy becomes crucial if we want to leverage the use of technology to build and enable trust. It is no longer enough for a consumer to know how to handle and operate a smartphone or computer, and the need to guarantee their own security is becoming an important factor (Estrada et al., 2022).

Digital literacy can be defined as a person with sufficient skills to understand and utilize information from various digital sources and the ability to use digital technologies while understanding the digital tools, platforms, and ethical responsibilities (Vitak et al., 2018). Digital literacy is becoming more important as the accessibility and consumption of digital sources continues to be incorporated in daily teaching and learning practices, as well as in the e-commerce space. Thus, in this case, the knowledge on how to deal with online dangers is key to ensuring the safe usage and consumption of the digital space and allows technology to promote trust rather than deteriorate it (Ghafir et al., 2018).

In theory, the root causes of cybercrime at the household and individual level appears to be complex. Both hard and soft aspects of cybersecurity appears to be good predictors of cybercrime (Srivastava et al., 2020). This includes hard factors such as the legal legislation, technical hardware and software implementation, and organizational readiness, as well as soft factors that includes digital literacy and capacity of users to minimise the incidence of cybercrime. However, technological capital (hard factors) is only found to partially mediate the frequency of cybercrime (Srivastava et al., 2020).

In fact, there is vast evidence to highlight the importance of education, which includes digital literacy and digital safety skills as a predictor of cyber-safety and reduction in cybercrime (Dodel and Mesch, 2018). Some studies even show that digital safety skills are more important than password safety and even antivirus engagement (Dodel and Mesch, 2019). While there are some caveats as those with higher education attainment tend to report higher levels of cybercrime incidence as they utilise e-commerce platforms more frequently (Padyab et al., 2024), the point remains that education and digital literacy is crucial to the safety of users online.

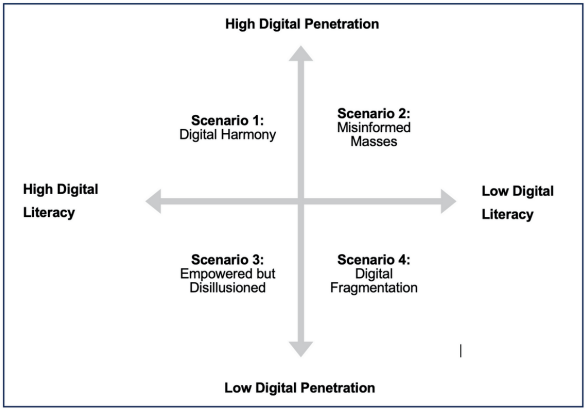


Figure 1. 2x2 Futures Matrix: Digital Penetration and Digital Literacy

(Source: Author's Compilation)

Figure 1 presents a 2x2 futures matrix, which illustrates a simplified trade-off between digital penetration and digital literacy with four outcomes. Scenario 1: Digital Harmony presents the ideal scenario with high levels of internet penetration and digital usage alongside a digitally literate population. In this scenario, technology is utilized as an effective tool to promote trust and avoid misinformation across businesses, societies, and communities. Meanwhile, the extreme case, Scenario 4: Digital Fragmentation, highlights a scenario with limited internet access and low levels of digital literacy. In this case, technology has limited influence to promote trust and at times, is used to deteriorate trust due to misinformation in isolated groups of society.

Scenario 3: Empowered but Disillusioned presents a case where a society has high levels of digital literacy but lacks the depth and use of digital technologies. While this can technically promote peace and trust among societies, it can lead to a gap in development as those that are digitally literate cannot expand their impact. Finally, Scenario 2: Misinformed Masses presents a case, where the population has full access to the internet, but lack of digital literacy leads to the deterioration of trust as scams, fake news, and cyber manipulation continue to target those that are vulnerable. This can potentially worsen due to the misuse and mistrust of technology.

Year	Individuals using the Internet (% of population)	Mobile cellular subscriptions (per 100 people)	Secure Internet servers (per 1 million people)
2019	95.0	131.2	10,603.9
2020	95.1	121.5	15,597.9
2021	95.6	135.5	14,293.6
2022	99.0	117.8	21,394.1

Table 1: Brunei Selected ICT Indicators Over Time

(Source: World Development Indicators, World Bank (2024))

With these four scenarios in mind, which Scenario does Brunei potentially fit into currently? Table 1 presents some selected Information and Communication Technologies (ICT) indicators over time since 2019. The statistics show that in 2022, Brunei's internet penetration rate stands at 99% of the total population, which virtually covers the whole population as only 1% remained offline. Additionally, mobile cellular subscriptions per 100 persons show a high level of mobile usage of more than 100%, which implies that some members of the population use more than a single mobile phone. This indicates that Brunei has high levels of digital penetration.

Meanwhile, the statistics on secure internet servers in Brunei seems to imply that the country is digitally secure, in comparison to other advanced ASEAN nations. This is second after Singapore, which has around 200,000 secure internet services per 1 million people, while Malaysia has around 9,000 secure internet services per 1 million people in 2022 (World Bank, 2024). This implies that Brunei seems to be digitally secure, yet we argue that the use of digital technologies is lagging in comparison to its internet penetration rates.

Figure 2 presents the use of internet activities in households and the use of local web and mobile activities. The main use of household internet is predominantly used for seeking information, followed by messaging and teleconferencing, and the use of social media. Meanwhile, in terms of specific mobile activities, the use of e-commerce is rather low as less than 50% of respondents use local web and mobile applications to pay bills, while around 20% use other applications that includes gaming. While this does not necessarily imply a low level of digital literacy, the use of digital technology at the household level can be characterised as still developing.

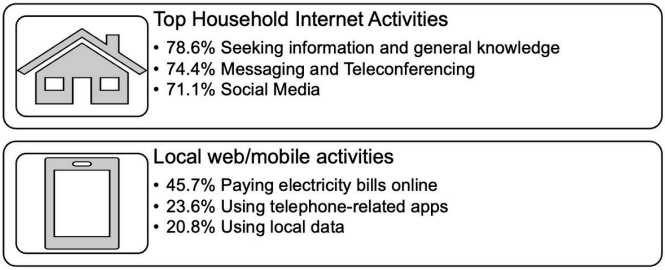


Figure 2: Selected ICT Household Statistics in Brunei 2019

(Source: Authority for Info-communications Technology Industry of Brunei Darussalam (2019))

This point is re-iterated in Figure 3, which presents ICT Business Statistics in Brunei. It can be observed that only 16% of businesses sell their products online despite having access to the internet (90%). In terms of specific payment methods, traditional cash and card payment methods are predominant, while the use of QR codes and other e-wallets are low. The point remains that while this does not necessarily imply that digital literacy is low, yet there are telling signs as the use of technology in e-commerce is still developing. Brunei is most likely in Scenario 2: Misinformed Masses as online scams and cyber-attacks remain a notable concern in Brunei. In recent years, Brunei was recorded to experience a 40% increase in cyber security attacks (ITPSS, 2020). Online scams were rampant during the pandemic, as top scams in Brunei include post office scams, fake COVID-19 relief fund, fake sellers, as well as impersonating health officials to phish for data (The Scoop, 2022).

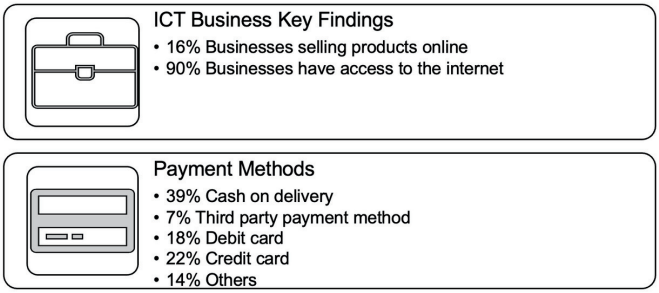


Figure 3: Selected ICT Business Statistics in Brunei 2019

(Source: Authority for Info-communications Technology Industry of Brunei Darussalam (2019))

As of 2023, the Royal Brunei Police Force recorded over 1000 scams of which nearly 75% were online scams (Borneo Bulletin, 2024). More specifically, the economy suffered nearly $2 million in losses from cybercrime in 2023, where 29% of the victims were between 18 and 35 years old, and over 60% of victims were 36 and above (Bakar, 2024).

The Brunei case study emphasise the need for digital literacy as the country has high levels of digital and internet penetration rates, however, the use of technology remains developing and scams continue to be prevalent.

This re-emphasises the importance of digital literacy. Brunei is well positioned in terms of its hard infrastructure, which in theory can minimise the incidence of cybercrime (Srivastava et al., 2020). However, cybercrime remains high in Brunei as a significant number of users fall victim to such cases. An interesting caveat here is that Brunei has high levels of human capital formation, reflected by its high level of education attainment, however, digital safety skills and digital literacy remain low as evident from the case study.

Country	Individuals using the Internet (% of population)	Mobile cellular subscriptions (per 100 people)	Secure Internet servers (per 1 million people)	Real GDP per capita (US$ 2015)
Brunei Darussalam	99.0	117.8	21,094.9	28,549.2
Cambodia	56.7	116.3	183.5	2,010.8
Indonesia	66.5	114.9	2,496.4	4,024.9
Lao PDR	66.2	-	274.0	2,589.1
Malaysia	97.4	141.3	8,416.7	11,174.2
Myanmar	-	106.7	14.8	1,174.8
Philippines	75.2	144.0	100.2	3,577.7
Singapore	96.0	156.5	212,649.3	67,948.9
Thailand	88.0	176.3	2,746.2	6,272.6
Viet Nam	78.6	139.9	4,713.4	3,603.9

Table 2: ASEAN Selected ICT and Economic Indicators (2022)

(Source: World Development Indicators, World Bank)

Extending this argument to the regional level, Table 2 presents selected ICT and economic indicators in the ASEAN region. Singapore is another similar case study to Brunei, where the country has high levels of internet and mobile penetration with even higher levels of hard infrastructure as seen by its level of secure internet servers. However, in 2023, there were 50,376 cybercrime and scam cases as reported by the Singapore Police Force (Shiean and Tan, 2024). This is twice the number of cases from 2022, which implies that despite high levels of hard infrastructure and secure servers, individuals still fall victim to such cases. The Singapore Police Force also re-iterates the need for intervention through collaboration with stakeholders and public education efforts to improve digital security and literacy skills.

On the other hand, Malaysia has high levels of internet penetration rates and usage, however, has significantly lower number of secure internet servers. Nonetheless, there were 34,445 online fraud cases, which stems from consumer's digital security skills, compared to 15,800 cases of organisations targeted by ransomware, which results from lower levels of secure servers (MyCert, 2024).

Similarly, Thailand has high levels of internet penetration with relatively lower number of secure internet servers but also suffers from a high level of cybercrime cases that originate from lack of digital security and literacy skills at the individual level. According to the Royal Thai Police, between 2022 and 2024, a total of 461,044 cybercrime cases were reported with online investment and call centre scams being prominent (Tortermvasana, 2024). Thus, the point remains that while hard infrastructure matters, digital security skills and literacy is crucial to reduce cybersecurity crime. This is reflected in recent studies that highlights the importance of digital literacy as a barrier and allows users to understand their associated rights and responsibilities (Sefrina, 2023).

So, how can we promote digital literacy to ensure that technology can promote trust among businesses and households? Both public and private institutions, as well as the larger community and relevant stakeholders play a major role in promoting digital literacy (BruCert, 2022). The Brunei government has committed to developing the digital landscape in Brunei, moving towards a "Smart Nation", which includes the establishment of the Digital Economy Council that includes programmes to develop the technological skills and capacity of consumers as well as support for micro, small, and medium-sized enterprises (MSMEs) for the use of such technologies (Digital Economy Council, n.d.). This is important as the government institutionalises the need for increased digital literacy.

In addition, the Ministry of Education in Brunei Darussalam has also outlined a Digital Transformation Plan 2023–2027, which aims to integrate digital teaching and learning transformation as well as the public service delivery transformation via digital technologies (Minister of Education, n.d.). This ensures that digital literacy begins at a very young age and grassroots level, as the plan includes the development of a digital curriculum. Such efforts from various ministries can improve digital literacy.

The private sector also continues to play an important role, particularly for e-commerce.

Large corporate banks such as Bank Islam Brunei Darussalam and Baiduri Bank continue to highlight the risks and dangers of online shopping and fraudulent activities through their website and social media (Baiduri Bank, n.d.; Bank Islam Brunei Darussalam, n.d.). Meanwhile, private sector organisations such as the ASEAN Business Advisory Council Brunei and the APEC Business Advisory Council Brunei hosts several events that includes the Digital Economy Forum 2024 that highlights the importance of cyber security (Zin, 2024).

This complements the public sector's efforts as the Authority for Info-communications Technology Industry (AITI) of Brunei Darussalam has recently hosted the Digital Futures Conference 2024 that includes sessions on ethical hacking (Authority for Info-communications Technology Industry of Brunei Darussalam, 2024). The Digital Brunei Initiative from AITI also includes various community outreach programmes specifically aimed at increasing digital awareness and literacy for the elderly population (Authority for Info-communications Technology Industry of Brunei Darussalam, 2024)

In addition to country specific efforts, ASEAN Member States can also benefit from other current and continuing policy efforts. This includes regional initiatives to develop digital literacy levels across the region. One such initiative is the ASEAN Digital Economy Masterplan 2025, which aims for a digitally inclusive society as one of its key strategic areas (ASEAN Secretariat, 2021). This includes the development of a Digital Inclusion Centre that develops educational modules for a wide range of digital services such as Digital Financial Inclusion. Additionally, the ASEAN Digital Economy Masterplan 2025 outlines the need for the delivery of trusted digital services and the prevention of consumer harm, through the ASEAN Framework on Personal Data Protection. This ensures that cybersecurity and digital governance in respective ASEAN Member States can benefit as a country and regionally as a whole.

Finally, ASEAN Member States should continue to re-iterate the development of the ASEAN Digital Economy Framework (DEFA). The ASEAN DEFA Framework outlines nine core elements that includes Online Safety and Cybersecurity, with the aim to improve cooperation across the region alongside an open and secure environment with comprehensive protection for cross-border parties in digital transactions. At the granular level, the ASEAN DEFA Framework includes Cyber Security Cooperation Strategies that emphasise the importance of digital security, particularly through regional capacity building and enhancing trust in the Cyber Space.

Recommendations

1. **Expand and Institutionalise Digital Literacy Programmes**
   - Integrate mandatory digital literacy modules in education and create tailored programmes for specific groups such as MSMEs and marginalised communities.
2. **Enhance Public Awareness Campaigns on Cyber Security**
   - Collaborate with stakeholders to run public campaigns on online risks and ethical digital practices.
3. **Strengthen Public-Private Collaboration**
   - Foster joint initiatives between public agencies and private organisations to align efforts on digital literacy and cybersecurity.
4. **Promote Regional Cooperation on Digital Governance**
   - Actively engage in ASEAN initiatives to build regional cybersecurity capacity and share best practices.
5. **Implement Monitoring and Evaluation Mechanisms**
   - Conduct regular evaluations to improve Digital Literacy programmes and campaigns.

Conclusion

In conclusion, technology is merely an enabler for peace and trust, and in this essay, using Brunei and ASEAN Member States as a case study, it is found that in some cases technological adoption can be high and infrastructure remains secure. Yet, the incentives to commit online and technological fraudulent activities also remain high, especially when digital literacy has room to improve. Governments, the private sector, independent organisations, and other relevant stakeholders should continue to support efforts to promote digital literacy to fully leverage the role of technology in building trust, and the greater economy.

BIBLIOGRAPHY

- ASEAN Secretariat. (2021). ASEAN Digital Masterplan 2025. https://asean.org/wp-content/uploads/2021/08/ASEAN-Digital-Masterplan-2025.pdf
- Authority for Info-communications Technology Industry of Brunei Darussalam. (2019). Brunei Darussalam ICT Household Report 2019. https://www.aiti.gov.bn/events-and-publications/surveys
- Authority for Info-communications Technology Industry of Brunei Darussalam. (2019). Brunei Darussalam ICT Business Report 2019. https://www.aiti.gov.bn/events-and-publications/surveys
- Authority for Info-communications Technology Industry of Brunei Darussalam. (2024, May 8). Bridging the digital gap in Brunei Darussalam. AITI. https://aiti.gov.bn/news/2024/bridging-the-digital-gap-in-brunei-darussalam/

- Authority for Info-communications Technology Industry of Brunei Darussalam, (2024). Digital Future Conference 2024. https://aiti.gov.bn/events/digital-future-conference-2024/
- Baiduri Bank. (n.d.). Can you spot a scam while shopping? Personal, Learn. https://www.baiduri.com.bn/personal/learn/can-you-spot-a-scam-while-shopping-online
- Bakar, R. H. A. (2024). Bruneians rack up $2 million in losses from online scams. August 2024, The Scoop. https://thescoop.co/2024/08/01/bruneians-rack-up-2-million-in-losses-from-online-scams/
- Bank Islam Brunei Darussalam. (n.d.). Protecting Yourself from Fraudulent Activities. Online Security: Fraudulent Activity. https://bibd.com.bn/online-security/fraudulent-activity/
- Bhardwaj, G. & Kamari, K. (2018). Role of Technology in Promoting Peace. Researchers Guild. [Online]. https://doi.org/10.15503/rg2018.12
- Borneo Bulletin. (2024). Over BND2.3M lost to online scams in 2023. August 2024, Borneo Bulletin. https://borneobulletin.com.bn/over-bnd2-3m-lost-to-online-scams-in-2023/
- BruCert. (2022). Online Safety Awareness Survey Report 2022. https://www.secureverifyconnect.info/brucert-online-safety-awareness-survey-2022
- Digital Economy Council. (n.d.). Digital Economy Masterplan 2025. https://www.gov.bn/SitePages/DEC.aspx
- Dodel, M., & Mesch, G. (2018). Inequality in digital skills and the adoption of online safety behaviours. Information, Communication & Society, 21(5), 712–728
- Dodel, M., & Mesch, G. (2019). An integrated model for assessing cyber-safety behaviors: How cognitive, socioeconomic and digital determinants affect diverse safety practices. Computer & Security, 86(2019), 75–91
- Estrada, F. J. R., George-Reyes, E. C., & Glasserman-Morales, L. D. (2022). Security as an emerging dimension of Digital Literacy for education: a systematic literature review. Journal of E-Learning and Knowledge Society, 18(2), 22–33
- Ghafir, I., Saleem, J., Hammoudeh, M., Faour, H., Prenosil, V., Jaf, S., Jabbar, S., & Baker, T. (2018). Security threats to critical infrastructure: the human factor. The Journal of Supercomputing, 74(10), 4986–5002
- ITPSS. (2020). Brunei records nearly 40% increase in cybersecurity attacks. https://itpss.com/brunei-records-nearly-40-cent-increase-cybersecurity-attacks
- Kallsh, I., Wolf, M. & Holdowsky, J. (2021). The link between trust and economic prosperity. Article, Deloitte Insights. https://www2.deloitte.com/us/en/insights/economy/connecting-trust-and-economic-growth.html
- Merriam-Webster. (n.d.) Scam. https://www.merriam-webster.com/dictionary/scam
- Ministry of Education. (n.d.). Digital Transformation Plan 2023-2027. https://www.moe.gov.bn/Shared%20Documents/MOE%20Digital%20Transformation%20Plan%202023-2027.pdf
- MyCert (2024). SR-027.092024: MyCERT Report - Cyber Incident Quarterly Summary Report - Q2 2024. Advisories, Malaysia Computer Emergency Response Team. https://www.mycert.org.my/portal/advisory
- Padyab, M., Padyab, A., Rostami, A., & Ghazinour, M. (2024). Cybercrime in Nordic countries: a scoping review on demographic, socioeconomic, and technological determinants. SN Social Sciences, 4(205), 1–30
- Peace Direct. (2020). Digital pathways for peace: Insights and lessons from a global online consultation. https://www.peacedirect.org
- Sefrina, M. (2023). An Inclusive Digital Economy in the ASEAN Region. ERIA Discussion Paper Series, No. 505 (ERIA-DP-2023-33).
- Shiean, N. Y., & Tan, M. (2024). Three Things you Should Know About the Annual Scams and Cybercrime Brief 2023. Police Life, Singapore Police Force. https://www.police.gov.sg/Media-Room/Police-Life/2024/02/Three-Things-you-Should-Know-About-the-Annual-Scams-and-Cybercrime-Brief-2023

- Srivastava, S. K., Das, S., Udo, G. J., & Bagchi, K. (2020). Determinants of Cybercrime Originating within a Nation: A Cross-country Study. Journal of Global Information Technology Management, doi: 10.1080/1097198X.2020.1752084
- The Scoop. (2022). Scamdemic: How fraudsters exploit fears during the pandemic. May 2024, The Scoop. https://thescoop.co/2022/05/24/scamdemic-how-fraudsters-exploit-fears-during-the-pandemic/
- Tortermvasana, K. (2024). Surveying efforts to halt cybercrime. Bangkok Post, 11 April 2024. https://www.bangkokpost.com/life/tech/2774514/surveying-efforts-to-halt-cybercrime
- Vision of Humanity. (2020). Three ways technology can promote peace. https://www.visionofhumanity.org/three-ways-technology-can-promote-peace/
- Vitak, J., Liao, Y., Subramaniam, M., & Kumar, P. (2018). 'I Knew It Was Too Good to Be True" The Challenges Economically Disadvantaged Internet Users Face in Assessing Trustworthiness, Avoiding Scams, and Developing Self-Efficacy Online. Proceedings of the ACM on Human-Computer Interaction, 2(CSCW), 1–25
- World Bank (2024). World Development Indicators. https://databank.worldbank.org/reports.aspx?source=world-development-indicators
- World Economic Forum. (2024). Three ways technology can transform economies and restore trust. https://www.weforum.org/stories/2024/01/three-ways-technology-can-transform-economies-and-restore-trust
- Zin, A. (2024). Brunei Digital Economy Forum 2024: Paving the Way for a Digital Future. September 2024, Business Insights, The Bruneian. https://thebruneian.news/2024/09/27/brunei-digital-economy-forum-2024-paving-the-way-for-a-digital-future/

CAMBODIA TOWARDS A DIGITAL RESILIENCE : TACKLING CYBERSECURITY CHALLENGES

ABSTRACT

The rapid digital transformation in Cambodia presents both opportunities and challenges, particularly in cybersecurity awareness and digital literacy. While over half of Cambodian citizens are online netizens, many remain vulnerable to cyber threats such as phishing, data breaches, and misinformation due to limited knowledge of digital safety practices. This essay explores the intersection of cybersecurity and human rights, emphasizing how inadequate digital literacy infringes on fundamental rights such as privacy, security, and freedom of expression. By comparing Cambodia's cybersecurity landscape with other ASEAN nations, the study highlights the country's weaknesses and opportunities for improvement. Proposed solutions include educational campaigns tailored to local communities, government-led policy interventions, and the use of technology to scale awareness. By addressing these gaps, Cambodia can build a more resilient and digitally literate society, ensuring individuals can safely and effectively engage in the digital world while safeguarding their human rights.

Keywords: Cybersecurity; Digital Literacy; Human Rights; Cambodia; ASEAN

AUTHOR:

SUN HENG

(CAMBODIA)

Introduction

In an interconnected world that increases every second, the rapid integration of digital technologies offers both unparalleled opportunities and profound challenges. In Cambodia, one of the ASEAN countries where over 56% of its population is online, the digital revolution has reshaped everyday life, from education to commerce and social interactions (Kemp, 2024). Yet, beneath this progress lies a critical issue: the lack of cybersecurity awareness, particularly among vulnerable groups such as students, middle-to-lower-class families, and the elderly.

This challenge is exacerbated by insufficient digital literacy, as many Cambodians remain unaware of the risks posed by online scams, data breaches, and misinformation. Alarmingly, even basic practices like securing passwords or enabling two-factor authentication are uncommon. The consequences of this gap extend beyond individual losses to societal vulnerabilities, including economic risks, weakened national cybersecurity defenses, and infringements on fundamental human rights such as the right to privacy and security (World Economic Forum, 2014).

Drawing on insights from the local research on high school students' information security awareness; which revealed significant gaps in their understanding of online threats, such as phishing and data breaches. This essay proposes targeted solutions tailored to Cambodia's challenges. These include educational campaigns that resonate with the population, relatable media strategies, and governmental policies to institutionalise cybersecurity education. The goal is clear: to empower individuals, protect privacy, uphold human rights, and foster a digitally resilient society.

Case Study Context: Cybersecurity Awareness in Cambodia

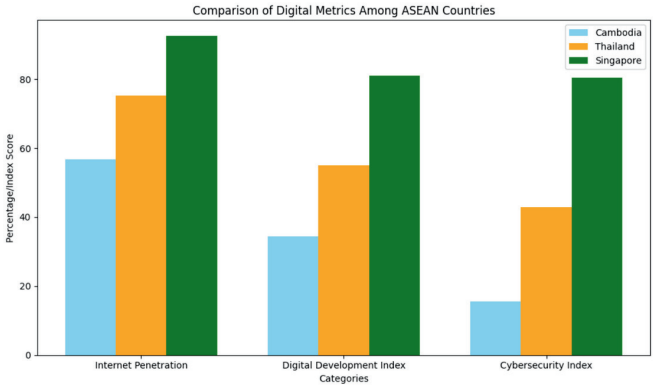
Cambodia's digital landscape has rapidly evolved, with internet penetration exceeding 56% of the population (Kemp, 2024). Yet, the infrastructure supporting cybersecurity awareness and education has not grown at the same pace. A research into the information security habits of Cambodian high school students uncovered a troubling trend: a significant portion of youth remain ill-prepared to navigate the dangers of the digital world. From misinformation to phishing attempts, their lack of awareness leaves them vulnerable to exploitation.

For instance, during interviews, students admitted to sharing personal information online without understanding the implications. According to CDRI (2020), 45% of small

businesses in Cambodia also experienced phishing attacks in the past year, highlighting a broad vulnerability. They often reused simple passwords and overlooked the importance of enabling two-factor authentication. These practices mirror those of many adults in Cambodia, where middle-to-lower-income populations frequently rely on third parties, such as phone vendors, to create email or social media accounts. Such dependency often results in users being unaware of their own login credentials, let alone the risks of unprotected digital behavior.

Beyond students, small business owners and rural communities represent other critical groups affected by cybersecurity gaps. For example, small businesses in Cambodia often suffer financial losses due to phishing scams or malware attacks, as many lack the budget for advanced cybersecurity solutions. Similarly, rural communities face limited access to digital education, with only 12% reporting basic digital literacy skills (World Economic Forum, 2014), leaving them vulnerable to misinformation and online fraud, which can disrupt their livelihoods. Small businesses often lack resources to protect against data breaches, while rural populations face limited access to digital education. Highlighting these cases provides a broader perspective on the challenges and opportunities for intervention.

Moreover, these issues intersect with broader human rights concerns. Limited digital literacy exposes individuals to violations of their privacy and security, which are fundamental rights recognized under international frameworks like the Universal Declaration of Human Rights. For example, unprotected online behaviors can lead to cyber exploitation, including identity theft, financial fraud, and breaches of personal data. These violations not only erode trust in digital platforms but also hinder individuals from exercising their right to securely access and share information. For instance, individuals often fall victim to online scams or data breaches, leading to financial losses and emotional distress. These experiences not only compromise economic stability but also erode the trust individuals place in digital systems. Misinformation worsens issues by spreading fear and discrimination, especially against marginalised groups. This restricts freedom of expression and access to reliable information. These challenges highlight the need for digital literacy to protect human rights. By addressing these gaps, people can better exercise their right to privacy, free expression, and secure access to information. This shows the urgent need to improve digital literacy in Cambodia by addressing both knowledge gaps and cultural and practical barriers to cybersecurity awareness.



A Comparative Chart of Cambodia, Thailand, and Singapore of Digital Metrics

The disparities in digital and cybersecurity awareness across ASEAN countries are starkly illustrated in regional metrics. Cambodia's Internet penetration of 56.7% (Kemp, 2024), Digital Development Index score of 34.41, and Cybersecurity Index score of 15.58 (ITU, 2023) significantly lag behind those of regional neighbors like Thailand and Singapore, which boast higher scores of 88.4% and 97.4% in Internet penetration, respectively, and cybersecurity indices of 92.15 and 98.52. For instance, Singapore boasts an advanced cybersecurity framework, driven by robust policies and widespread digital literacy programs.

In contrast, Thailand has successfully implemented campaigns to raise cybersecurity awareness among its rural populations through community outreach programs. These comparative examples underline Cambodia's vulnerabilities in cyberspace and emphasize the importance of learning from regional best practices. ASEAN's Digital Masterplan 2025 presents a roadmap that Cambodia can align with to bridge its digital gaps and bolster its resilience against cyber threats. For example, Cambodia could adopt the "ASEAN Cybersecurity Capacity Building Program," which focuses on enhancing regional collaboration and training initiatives to improve cybersecurity skills and infrastructure. By implementing tailored workshops and promoting cross-border information sharing, Cambodia can accelerate its digital transformation while addressing its unique vulnerabilities.

Challenges in Cybersecurity Awareness

The barriers to widespread cybersecurity literacy in Cambodia are both structural and cultural. Structurally, the country's digital development is still maturing, with limited cybersecurity education integrated into formal learning systems. High school curriculums, for instance, rarely address the fundamentals of data protection, leaving students unprepared for online risks. Adults, particularly in rural or lower-income urban areas, often lack access to reliable information about online safety, making them easy targets for scams and misinformation.

Culturally, the reliance on convenience over caution exacerbates the problem. Many Cambodians entrust phone vendors or untrained individuals to set up their online accounts. This trend, while practical in the short term, leaves users unaware of their passwords or security settings, a vulnerability that can easily be exploited. Compounding this issue is the prevalence of misinformation, which thrives in environments where users lack the tools to critically evaluate content. Viral fake news stories on social media have led to financial scams and unnecessary public panic in several instances. Additionally, a lack of parental or community involvement in teaching digital habits contributes to the problem. Many parents, unfamiliar with technology themselves, struggle to guide their children in practicing safe online behaviors. This generational gap creates a vacuum where young people, often confident in their digital navigation skills, underestimate the importance of cybersecurity measures. These challenges underline the necessity of holistic solutions that blend education, policy, and technology to bridge Cambodia's cybersecurity literacy gap.

Recommendations

Education Campaigns Through Relatable Media. One of the most effective ways to reach a broad audience is through engaging, relatable content delivered via mass media. Short, impactful video clips can be integrated into television commercials and social media platforms to raise awareness about cybersecurity risks and best practices. These clips should use simple language, local dialects, and culturally relevant scenarios to appeal to diverse audiences. For instance, a skit showing a vendor explaining the importance of strong passwords to a customer could resonate with viewers who rely on informal assistance for tech setup. These media campaigns must emphasize actionable tips, such as enabling two-factor authentication, recognizing phishing emails, and avoiding the oversharing of personal information online. By tailoring the message to the everyday experiences of Cambodians, these campaigns can foster greater engagement and understanding.

Community-Based Training Programs. Community hubs, such as local schools, temples, and youth centers, can serve as venues for cybersecurity workshops. These programs should be designed to accommodate different literacy levels and technological familiarity. For younger audiences, gamified learning experiences, such as cybersecurity-themed quizzes or role-playing activities, can make the content more engaging. For adults, hands-on demonstrations on securing devices and identifying online threats are crucial. Such initiatives could draw inspiration from global programs like the National Initiative for Cybersecurity Education (NICE) in the United States, which collaborates with local communities to promote cybersecurity literacy (NIST, 2024). Specific aspects such as establishing cybersecurity work roles and providing role-specific training frameworks could be adapted to Cambodia's context. For instance, NICE's approach to creating industry-aligned educational resources could help Cambodian schools and training centers develop targeted programs that address both local and regional cybersecurity needs. A similar model in Cambodia could be adapted to train volunteers who act as local digital literacy ambassadors.

Government-Led Policy Interventions. Policy support is critical to institutionalize digital literacy as a national priority. The Cambodian government could integrate cybersecurity education into school curricula, starting with the basics of digital citizenship in primary schools and advancing to more technical concepts in high schools. Additionally, partnerships with tech companies can help subsidise the development and distribution of educational materials. Governments can also enforce regulations that mandate basic cybersecurity training for phone vendors and internet service providers. Ensuring these intermediaries are informed can reduce the risk of unsafe practices trickling down to end-users.

Leveraging Technology to Scale Awareness. Interactive technologies like chatbots, mobile apps, and SMS alerts can provide users with real-time cybersecurity guidance. For example, a government-supported app could send regular tips on safe online behavior, while chatbots could answer basic questions about digital safety. These solutions require initial investment but offer scalable, sustainable ways to improve awareness.

Conclusion

The digital age brings tremendous opportunities for connection and growth, but it also exposes individuals to significant risks if cybersecurity literacy is neglected.

In Cambodia, where rapid technological adoption outpaces public awareness, the consequences of this gap extend from personal data breaches to systemic vulnerabilities. By addressing these challenges now, we have the chance to safeguard privacy, uphold human rights, and build a resilient digital society. This essay has presented a comprehensive case study highlighting Cambodia's pressing need for cybersecurity awareness. From media-driven education campaigns to community-based training and policy-driven initiatives, the proposed solutions aim to bridge the digital literacy divide. These strategies are not merely theoretical but grounded in practical, scalable approaches that can empower Cambodians to navigate the online world safely. However, the responsibility does not lie with governments and educators alone. It requires collective action from all sectors; nonprofits, businesses, and individuals to foster a culture of cybersecurity awareness. As Cambodia stands on the brink of a digital transformation, this is a pivotal moment to ensure that no one is left behind in the journey toward a secure and inclusive digital future. By taking these steps, Cambodia can be an example in ASEAN, demonstrating how even a developing nation can proactively address cybersecurity challenges. Together, we can build a future where the benefits of digital innovation are accessible, equitable, and secure for all.

BIBLIOGRAPHY

- CDRI. (2020). Cybergovernance in Cambodia: A Risk-Based Approach to Cybersecurity. Phnom Penh: Cambodia Development Resource Institute.
- Kemp, S. (2024, February 23). Digital 2024: Cambodia—DataReportal – Global Digital Insights. Retrieved from https://datareportal.com/reports/digital-2024-cambodia.
- National Institute of Standards and Technology (NIST). (2024). Cybersecurity Education and Workforce Development. Retrieved from https://www.nist.gov.
- Pencheva, D., Hallett, J., & Rashid, A. (2020). Bringing cyber to school: Integrating cybersecurity into secondary school education. IEEE Security & Privacy, 18(2), 68–74. https://doi.org/10.1109/MSEC.2020.2969409
- World Economic Forum. (2014). Risk and Responsibility in a Hyperconnected World. Retrieved from https://www3.weforum.org.
- International Telecommunication Union (ITU). (2023). Global Cybersecurity Index 2023. Retrieved from https://www.itu.int.

ASEAN'S ROLE IN ENSURING AMAZON'S COMPLIANCE WITH INTERNATIONAL HUMAN RIGHTS LAW: BALANCING PRIVACY, SECURITY, AND HUMAN RIGHTS IN THE DEPLOYMENT OF FACIAL RECOGNITION TECHNOLOGY WITHIN AMAZON RING

ABSTRACT

The incorporation of facial recognition technology (FRT) into Amazon Ring, initially positioned as a home security device but later expanded to encompass surveillance capabilities, gives rise to apprehensions concerning privacy violations and discriminatory practices. This necessitates the involvement of ASEAN for the adoption of procedural safeguards by Amazon to ensure lawful implementation of FRT, safeguarding against discriminatory use and harm to human interests. This paper aims to explore the significance of the concept of human security in ensuring Amazon's compliance with International Human Rights Law (IHRL) in effectively mitigating discrimination and privacy violations associated with cyberspace tools, specifically FRT in Amazon Ring. The study investigates the relationship between soft technological determinism, human security, and IHRL. While previous research has emphasized ethical principles in regulating the cyberspace and AI industry, the correlation of IHRL as a human security foundation in addressing risks posed by FRT algorithms in this digitalization era remains underexplored. This paper's objective is to bridge this gap by elucidating the responsibilities of corporations regarding human rights implications and highlighting the involvement of ASEAN in proposing appropriate measures to be adopted.

Keywords: Facial Recognition Technology; International Human Rights Law; Privacy Violations; Discriminatory Practices; Human Security

AUTHOR:

ALEXANDRA EVELYNE WIJAYA

(INDONESIA)

Introduction

The predominant view held by young individuals regarding artificial intelligence (AI) leans significantly toward positivity, with an impressive 93.2 percent expressing a favorable perspective (Hogenhout & Takahashi, 2022). As 80 percent of the participants routinely interact with AI, a significant 68 percent exhibit trust in the competencies of AI. Nonetheless, a substantial majority, accounting for 76.3 percent, regards AI technology's risks as significant, with the most commonly mentioned concerns encompassing privacy breaches (57.3 percent), issues of discrimination (53.5 percent), and governmental supervision (51 percent). Youth concerns about human security are reflected in the application of facial recognition technology (FRT) in the Amazon Ring doorbell, a key aspect of cybersecurity.

This analysis will centre on a case study around the Amazon Ring Doorbell. Amazon to purchase a startup called Ring which specializes in selling smart doorbells (Stone, 2018). These doorbells are equipped with built-in cameras, microphones, and speakers with audio-visual recording devices that are triggered by motion detection (Motion Detection in, n.d.). Users have the ability to receive instantaneous alerts to homeowners' devices, store footage in the cloud and anonymously posted videos of suspicious activities to the public through the Neighbors app (Caricola, 2020; Nick, 2018). Moreover, the partnerships brokered by Ring with 1,300 US law enforcement (Ng, 2019) authorizing these agencies to extract footage by utilizing the Neighbors app (Schmelzer, 2019) or attaining a legal authorization under the Stored Communications Act (SCA). Thus these cooperations are not only limited to US and UK as Ring doorbells are available across other European countries and are entering the Southeast Asian market (Ring Alarm Availability, n.d.).

Despite marketing its Ring doorbells as home security devices, Amazon has gone beyond providing video and audio surveillance features (Molla, 2019). Instead, the company has proposed the use of facial recognition technology (FRT) in the future following the 17 patent applications (Haskins, 2021). FRT refers to a type of software or application that is designed to automatically or semi-automatically identify, verify and categorize an individual by analyzing and comparing their unique facial features (Chun, 2020; Romero-Moreno, 2021). This technology employs machine learning, which involves training the algorithm to recognize faces or identify a specific individual. By repetitively exposing itself to a dataset filled with various images, videos, and photos of human faces, the algorithm can form associations and connections within the data.

The primary purpose of FRT in Amazon Ring is to benefit humanity by enhancing security measures, enabling real-time individual tracking, and facilitating data analysis through integration with law enforcement via cloud-based systems in cyberspace. However, the public encounters several instances that jeopardize human rights including concerns about non-users' privacy and implications on discrimination. This implies the urgency for Amazon to adopt procedural safeguards to ensure that FRT is implemented lawfully, protecting human interests from discriminatory use or harm. Therefore, this paper aims to discuss the question: Why is it essential for ASEAN to establish frameworks ensuring Amazon's adherence to IHRL to maintain an effective approach to privacy, security, and human rights when deploying cyberspace tools like FRT within Amazon Ring? Most studies have discussed how ethical principles should be considered when regulating the cyberspace and AI industries, without thoroughly exploring how IHRL could solve the risks posed by FRT's algorithms (McGregor, 2019). This article aims to bridge this discrepancy by clarifying the obligations of corporations for their effects on human rights and the appropriate actions they should take in response.

Legal Analysis

Soft technological determinism focuses on to what extent technology forges society and the consequences that follow (Winner, 1986). This perspective reflects that technologies are inherently political and become intertwined with a particular way of life in the future, as is the case with Amazon Ring (Selinger & Darrin, 2022). To comprehend the conflict between democratic values and Ring doorbell, it is necessary to envision the societal implications that may arise if they become widely adopted.The mass adoption using Ring systems will contribute to the collective harm, and each user will bear responsibility for their involvement.

As ASEAN has the responsibility of regional security, a cyberspace framework for the deployment of FRT by private companies is necessary to protect integrity while fostering human development (Zojer, 2019). An effective cybersecurity framework should emphasize how technologies embody cultural and political values (Bijker & Pinch, 2012) that are integral to human well-being. As soft technological determinism emphasizes the importance of understanding the impact of FRT, it underscores the need to guarantee the proper advancement and utilization of Amazon Ring is guided not only by ethical considerations but also by human rights principles. UN Global Pulse and UN Human Rights consultations have concluded that effective governance of AI must be grounded on human rights principles (Prizzi, 2021).

IHRL serves as a framework for the design, development, and deployment of cyberspace's algorithms, establishing a foundation for human security. The concept of human security can be used as a policy-making tool (Floyd, 2007) as ASEAN countries can identify threats of FRT in Amazon Ring towards individuals and communities. IHRL becomes the benchmark to determine whether States and businesses are infringing upon or violating human rights. By incorporating human security approaches, ASEAN aligns cybersecurity with human rights, empowering its Member States to address the opportunities and challenges of digitalization more effectively. The following IHRL could be used as guidance for future frameworks:

a) The Deployment of Amazon Ring Infringes Upon the Privacy Rights of Nonusers

The installation of FRT in Amazon Ring poses a threat to non-users privacy rights due to the involuntary collection and distribution of facial information (Lai & Rau, 2021). Amazon neglecting the negative liability coming from the usage of Ring equals disregarding the protection of civil liberties (Frascella, 2021). Irrespective of international, regional, and national regulatory measures, Amazon has the liberty to use FRT to access and utilize facial information without being held responsible for the collection process, including granting law enforcement access to facial information related to criminal investigations (Goode & Matsakis, 2020). Regardless of being a helpful preliminary investigation tool, Ring has the potential of false accusations or misuse within the system (Snow, 2018) which enables the possibility of innocent individuals' images being wrongly matched for the purposes of law enforcement (Sarabdeen, 2022). Finally, there is the possibility of Amazon misusing facial information by utilizing recorded videos to produce online TV shows and documentaries (Amazon is Turning, 2022). In conclusion, despite following the necessary procedures to ensure dependability, FRT may still be utilized by entities and for objectives beyond its original purpose (Frascella, 2021).

Amazon, being a multinational corporation, is obligated to adhere to regulations at the global, regional, and local scales that govern the right to privacy. The UN High Commissioner for Human Rights stated the right to privacy is applicable when a government conducts surveillance in public spaces (Talbot, 2021) such as streets (including pavements and bicycle paths), open spaces, and public facilities (UN-Habitat 2021). Correspondingly, Article 17 of the International Covenant on Civil and Political Rights (ICCPR) implied that any interference with privacy must adhere to the principles of legality, legitimacy, necessity, and proportionality (United Nations Human Rights Council, 1988). Similar to Article 21 of the ASEAN Human Rights Declaration (AHRD) which protects people from arbitrary interference with their privacy.

Article 9(2) of the General Data Protection Regulation (GDPR) of the European Union (EU) also recognizes biometric data as sensitive information that cannot be gathered through FRT unless an individual has given explicit consent or there exists a significant public interest for enforcing the law as determined by EU or Member State law (Pin, 2021). For instance, the UK Data Protection Act 2018 incorporates the GDPR and has identified 23 substantial public interest conditions with 3 situations relevant for corporate actors to use FRT: prevention and detection of unlawful acts, fraud, and suspicion of terrorist financing or money laundering (European Commission, 2021). To prevent excessive discretion in managing technology, the use of FRT must be administered by a detailed legal framework that aligns with Article 8 of the European Convention on Human Rights (ECHR) as mentioned in R (Bridges) v. Chief Constable of South Wales Police (2020). The Supreme Court's decision in Carpenter v. United States (2018) further highlights the need to protect privacy when FRT is used over a prolonged period (Hamann & Smith, 2019). Therefore, it is necessary to obtain approval in advance from a court or an impartial administrative body for the utilization of FRT (Romero-Mareno, 2021), and to comprehensively examine the permissibility of FRT (Kouroupiis, 2021).

b) The Deployment of Amazon Ring Infringes Upon the Non-Discrimination Rights of Non-Users

Amazon has asserted that FRT's racial bias and potential for error decrease over time as the algorithm interacts with consumer data (Crawford, 2015). Due to the encouragement given by Amazon Ring's FRT features towards users' apprehension of home burglary, property theft, and other minor offenses, people are more likely to make negative judgments about suspicious activities on the basis of existing biases related to race, gender, and social class (Selinger & Darrin, 2022). The unequal application of FRT within a neighbourhood could have a discriminatory impact on minority groups (Trujilo, 2021), particularly in light of the heightened anxiety about exaggerated crime rates (Molla, 2019). Consequently, this results in users employing such technologies for profiling and reporting others as suspicious, even in instances where these individuals have a legitimate right to be part of these communities (Cole, 2019).

For instance, FRT misidentification poses a greater risk for low-income Black people due to the technology's higher rates of identifying darker-skinned individuals (Haber, 2021). Based on findings from the ACLU, a study reveals that the Rekognition software developed by Amazon falsely matched the identities of 28 individuals serving in Congress as having prior criminal records (Talbot, 2021).

The study also emphasized that a disproportionate number of misidentifications (40%) occurred among dark-skinned individuals, even though they represented only 20% of the congressional members. Correspondingly, the use of FRT to identify a person's criminality based on their facial features and pre-existing criminal records (Buolamwini, 2018) has resulted in the targeting of vulnerable dark-skinned populations (Van Noorden, 2020). Furthermore, the overrepresentation of dark-skinned people in the law enforcement database used by FRT exacerbates the technology's negative impact on dark-skinned communities (Garvie, 2016). This caused Black people to be incarcerated and wrongfully convicted of high-level crimes than their White counterparts despite no statistical evidence that dark-skinned people are engaging in criminal activities (Coles & Powell, 2020). Aside from the dark-skinned population, the National Institute of Standards and Technology (NIST) has also shown higher error rates for Asians and Native Americans, women, and older adults (Singer & Metz, 2019). A biased system combined with institutional or individual racism within law enforcement has the potential to increase the mistreatment of marginalized communities, and legitimize legal action against them, resulting in an increase in racial disparities and greater social control over these communities (Coles & Powell, 2020). Consequently, Amazon Ring shall prevent the presence of systematic bias in FRT that arises from both the developer's and the technology's tendency to replicate patterns and biases that are inherent in human behavior (Buolamwini, 2018).

It is crucial for Amazon to respect international and national provisions regulating the right to non-discrimination, as the Ring involves classifying individuals based on their traits (Chun, 2020). The international prevention of discriminatory practices outlined in the International Bill of Human Rights is elaborated in three treaties: Article 1 of the Universal Declaration of Human Rights (UDHR) emphasizes the importance of freedom and equality in dignity and rights, while Article 24(1) of the International Covenant on Civil and Political Rights (ICCPR) and Article 2(1) of the International Covenant on Economic, Social and Cultural Rights (ICESCR) prohibit discrimination based on race, color, and national origin. Article 2 of AHRD also emphasizes the right to non-discrimination in race, national or social origin, economic status, or other standings. The UN Declaration on the Elimination of All Forms of Racial Discrimination highlights the global significance of eradicating racial discrimination, while the International Convention on the Elimination of All Forms of Racial Discrimination (ICERD) specifies the requirement for taking active steps to eliminate policies that foster racial divisions or prolong discrimination.

These conventions can be a valuable tool in countering the vague terms of "bias" or "discrimination" by offering a way to discern when bias and discrimination are illegal. IHRL offers a clear definition of harm that is universally applicable and capable of identifying forms of bias and discrimination that are prohibited and unlawful (United Nations Human Rights Council, 1989).

Proceeding to the EU region, companies utilizing FRT must implement appropriate safeguards in compliance with GDPR (Chun, 2020). The regulation in Article 22(1) aims to avoid algorithmic decisions causing discriminatory outcomes on individuals belonging to protected categories (Baldini, 2019), as automated decision-making processes frequently incorporate profiling. as defined in Article 4(4). Moreover, the Artificial Intelligence Act recognizes the implications of technical accuracies towards biased outcomes and discrimination based on sex, ethnic origin, age, or disabilities (European Commission, 2021). Thus, FRT should incorporate operational constraints that are inherent and cannot be overridden by AI, be responsive to human operators, and train human administrators to be unbiased as discussed in Orange România SA v Autoritatea Națională de Supraveghere a Prelucrării Datelor cu Caracter Personal (2020).

Role of ASEAN

ASEAN has yet to fully commit to a comprehensive cybersecurity agenda, whereas the EU has established a robust legislative framework aimed at enhancing cyber resilience and developing a regional cybersecurity strategy that upholds human rights (European Commission, 2023), even in the face of advancements in Internet of Things devices like the Amazon Ring. ASEAN has demonstrated its commitment to addressing cyber threats by adopting the consensus reports from two key UN cybersecurity initiatives: the inaugural UN Open-Ended Working Group (OEWG) and the sixth iteration of the UN Group of Governmental Experts (UNGGE). However, with the rise of new cross-border technologies and the growing cyber threats to human rights, ASEAN leaders have recognized the critical need for cooperation and coordination among Member States on cybersecurity policies. The absence of a unified cybersecurity framework in ASEAN has resulted in varying approaches to addressing cybersecurity challenges. Indonesia, Lao PDR, Malaysia, the Philippines, and Singapore have prioritized data protection through dedicated policies, while Brunei Darussalam has implemented a national data protection policy. In contrast, Myanmar and Vietnam have yet to consolidate their data protection efforts, as measures remain dispersed across various laws and regulations (Kasih, 2023).

Member States need a robust governance or legal framework to effectively combat cybercrime, grounded in comprehensive risk identification, analysis, and evaluation. These risk assessments should be specifically designed to address potential cyber threats posed by companies at the national level. These regional regulations will advocate business to adopt a risk centric approach to minimize carber threats and ensure the protection of human rights.

To tackle this issue, it is crucial to reference UN's and EU's framework of protection, provision, and participation as a basis for developing an cyberspace and AI strategies focused on international collaboration. Active involvement of ASEAN Member States should be highlighted to prevent any harmful consequences, to secure interactions between AI and human, and to maximize the use of AI as cybersecurity tools. Although universal guidelines such as the UN Guiding Principles on Business and Human Rights (UNGPs) (McCorquodale, 2021) and the OECD's guidance on "Human Rights Due Diligence (HRDD) through responsible AI (OECD, 2021), encourage regional corporations to prioritize human rights, it has failed to fully integrate the perspective and voices of developing countries. To maximize the role of ASEAN means providing Member States with the capacity and opportunities to exert influence over the development of FRT in Amazon Ring, enabling them to make well-informed decisions regarding their use of AI in the present and future. Empowerment of Member States will lead to the establishment of a responsible digital future for corporations, governments, and the international community. Accordingly, ASEAN will establish a platform for stakeholders to participate in comprehensive discussions on inclusive cyberspace and AI policy approaches and applications (Dignum & Pigmans, 2020). These dialogues should aim to highlight the development of Amazon Ring in accordance with local context by considering the backgrounds of different Member States and the operations of corporations. Thus, regulations should evolve to accommodate the requirements and entitlements of youth as they are entitled to the rights outlined in ICCPR, ICESCR and AHRD.

Conclusion

In conclusion, the current global initiative surrounding FRT in Amazon Ring emphasizes the immediate need to prioritize human rights by involving Member States in shaping the development of cybersecurity and AI. The regional-centered approach stresses the importance of protection, provision and participation for responsible AI usage.

Despite existing global directives, the viewpoints of regional cooperations are frequently overlooked, underscoring the need for inclusive discussions and regulatory modifications to safeguard the rights enshrined in the ICCPR, ICESCR, and AHRD. As technologies like Amazon Ring with facial recognition raise concerns about privacy, bias, discrimination, and human rights, it's crucial to embed human rights principles in development and deployment. Hence, the involvement of ASEAN is crucial for companies like Amazon to conform to these guidelines and diligently ensure the ethical and rights-based use of facial recognition technology, promoting a responsible and transparent AI in cyberspace environment.

BIBLIOGRAPHY

Conference Papers

- Buolamwini, J. (2018). Gender Shades: Intersectional Accuracy Disparities in
- Commercial Gender Classification. Proceedings of the 1st Conference on Fairness, Accountability and Transparency in Proceedings of Machine Learning Research. https://proceedings.mlr.press/v81/buolamwini18a.html
- Consumer Rights and Corporate Interests. International Carnahan Conference on Security Technology (ICCST), IEEE. https://doi.org/10.1109/ICCST49569.2021.9717403
- Romero-Moreno, F. (2021). AI Facial Recognition and Biometric Detection: Balancing

Online Source

- Amazon is Turning Ring Security Videos into TV Shows. (2022, 12 August). CBCS News. https://www.cbsnews.com/news/amazons-ring-videos-tv-show-mgm/
- Cole, S. (2019). Amazon's Home Surveillance Company is Putting Suspected Petty Thieves in its Advertisements. Vice. https://www.vice.com/en/article/amazon-home-surveillance-company-ring-law-enforcement-advertisements/
- European Commission. (2023). Cybersecurity Policies: Shaping Europe's Digital Future. https://digital-strategy.ec.europa.eu/en/policies/cybersecurity-policies
- Goode, L. & Matsakis, L. (2020, January 7). Amazon Doubles Down on Ring Partnerships With Law Enforcement. Wired. https://www.wired.com/story/ces-2020- amazon-defends-ring-police-partnerships/
- Haskins, C. (2021, December 28). See the Facial Recognition Patents Recently Awarded to Amazon's Ring. Business Insider. https://www.businessinsider.com/see-the-facial-recognition-patents-recently-awarded-to-amazons-ring-2021-12
- Haskins, C. (2021, December 28). See the Facial Recognition Patents Recently Awarded to Amazon's Ring. Business Insider. https://www.businessinsider.com/see-the-facial-recognition-patents-recently-awarded-to-amazons-ring-2021-12
- Molla, R. (2019, May 7). The Rise of Fear-Based Social Media Like Nextdoor, Citizen, and Now Amazon's Neighbors. Recode. https://www.vox.com/recode/2019/5/ 7/18528014/fear-social-media-nextdoor-citizen-amazon-ring-neighbors

- Motion Detection in Powered Ring Devices. (n.d). Ring Support Center. https://support.ring.com/hc/en-us/articles/360022461232-Motion-Detection-in-Powered-Ring-Devices
- Ng, A. (2019, December 3). Ring Let Police View Map of Video Doorbell Installations for Over a Year. CNET. https://www.cnet.com/news/ring-gave-police-a-street-levelview-of-where-video-doorbells-were-for-over-a-year/
- Nick. (2018, May 8). Introducing the Neighbors App: The New Neighborhood Watch. RING. https://blog.ring.com/2018/05/08/introducing-the-neighbors-app-the-new-neighborhood-watch
- Ring Alarm Availability In Europe. Ring. (n.d). Ring. https://support.ring.com/hc/en-gb/articles/360048999972-Ring-Alarm-availability-in-Europe-
- Schmelzer, E. (2019, September 24). Two Colorado Police Departments Already Partner with a Popular Doorbell Camera Company — and More Are Considering. Denver Post. https://www.denverpost.com/2019/09/22/ring-colorado-police-camera-surveillance/
- Snow, J. (2018, July 26). Amazon's Face Recognition Falsely Matched 28 Members of Congress with Mugshots. ACLU. https://www.aclu.org/news/privacy-technology/amazons-face-recognition-falsely-matched-28
- Stone, B. (2018, March 5) "Here's Why Amazon Bought a Doorbell Company. https://www.bloomberg.com/news/articles/2018-03-05/here-s-why-amazon-bought-a-doorbell-company

Journals

- Chun, S. (2020). Facial Recognition Technology: A Call for the Creation of a Framework Combining Government Regulation and a Commitment to Corporate Responsibility' (2020) North Carolina Journal Law & Technology 21(99). https://scholarship.law.unc.edu/ncjolt/vol21/iss4/5
- Coles, J. A. & Powell, A. (2020). A BlackCrit Analysis on Black Urban Youth and Suspension Disproportionality as Anti-Black Symbolic Violence. Race Ethnicity and Education, 23(1), 113. 10.1080/13613324.2019.1631778
- Floyd, R. (2007). Human Security and the Copenhagen School's Securitization Approach. Human Security Journal, 5, 38-49.
- Frascella, C. (2021). Amazon Ring Master of the Surveillance Circus. Federal Communications Law Journal, 73(3), 393.
- Kasih, M., C. (2023). Fostering ASEAN's Digital Future through Cybersecurity Policies and Human Empowerment Economic Research Institute for ASEAN and East Asia. ERIA,023(2). https://www.eria.org/uploads/Fostering-ASEANs-Digital-Future-through-Cybersecurity-Policies-and-Human.pdf
- Lai Pei-Luen, X., & Rau, P. (2021) Has Facial Recognition Technology Been Misused? A Public Perception Model of Facial Recognition Scenarios. Computers in Human Behavior, 124. https://doi.org/10.1016/j.chb.2021.106894
- McCorquodale, R. (2021). Artificial Intelligence Impacts: A Business and Human Rights Approach. Communications Law Journal, (11), 11.
- McGregor, L. (2019). International Human Rights Law as a Framework for Algorithmic Accountability. The International and Comparative Law Quarterly, 68(2), 309. https://doi.org/10.1017/S0020589319000046
- Selinger, E., & Darrin, D. (2022). Amazon's Ring: Surveillance as a Slippery Slope Service. Science as Culture, 31(1), 92. https://doi.org/10.1080/09505431.2021.1983797
- Talbot, R. (2021). Automating Occupation: International Humanitarian and Human Rights Law Implications of the Deployment of Facial Recognition Technologies in the Occupied Palestinian Territory. International Review of the Red Cross, 102(914), 823. https://doi.org/10.1017/S1816383121000746

- Trujilo, L. (2021). In the Absence of A Uniform Biometric Law: A Proposal Comparing Current Biometric Laws, Issues, and Future Solutions. Southern Illinois University Law Journal, 46(1),161.
- Zojer, G. (2019). Human Security and a Cyber Multi-Disciplinary Framework in the European High North'. Juridica Lapponica, 14,17. http://urn.fi/URN:NBN:fi-fe202001314068

Laws

- 18 U.S.C. §§ 2701 et seq. (2019).
- ASEAN Human Rights Declaration (AHRD). (2012).
- Convention for the Protection of Human Rights and Fundamental Freedoms (European Convention on Human Rights, as amended) (ECHR).
- General Data Protection Regulation (GDPR).
- International Convention on Civil and Political Rights (ICCPR). (1976). UNTS 171.
- International Convention on the Elimination of All Forms of Racial Discrimination (ICERD). (1965). 660 195 UNTS.
- International Covenant on Economic, Social and Cultural Rights (ICESCR). (1976). 993 3 UNTS.
- UN Declaration on the Elimination of All Forms of Racial Discrimination. (1904).
- United Kingdom Data Protection. (2018).
- Universal Declaration of Human Rights (UDHR). (1948). UNGA Res 217 A(III).

Official Documents

- United Nations Human Rights Council. (1988). General Comment 16: Article 17 (Right to Privacy. UN Doc. HRI/GEN/1/Rev9
- United Nations Human Rights Council. (1989). General Comment No. 18: Non-Discrimination. UN HRI/GEN/1/Rev.9 (Vol. I)

Report

- Dignum, V. & Pigmans, K. (2020). Tools to Operationalize the UNICEF policy guidance on AI for Children. UNICEF Office of Global Insight and Policy. https://www.unicef.org/globalinsight/media/1166/file/UNICEF-Global-Insight-tools-to-operationalize-AI-policy-guidance-2020.pdf> Roadmap
- Hogenhout L., & Takahashi, T. (2022). A Future with AI-Voices of Global Youth. United Nations Office of Information and Communications Technology. https://unite.un.org/sites/unite.un.org/files/a_future_with_ai-final_report.pdf
- OECD. (2021). AI in Business and Finance: Global Finance Outlook 2021. https://www.oecd.org/finance/oecd-business-and-finance-outlook-26172577.htm

Thesis

- Crawford, C. (2015). Technology Producers Use of Language and Discourse to Shape and Reinstate Anti-black Global Realities: An Analysis of Amazon's Facial Recognition Technology Communications and Responses to Racial Bias in Rekognition. MRP, Ryerson University. https://doi.org/10.32920/ryerson.14647572.v1

BYTES OF PEACE: LEVERAGING TECHNOLOGY TO PROMOTE TRUST AND SECURITY

ABSTRACT

Technology continues to permeate every aspect of modern life, showcasing its undeniable dual capacity to drive progress while amplifying vulnerabilities. This paper examines the role of technology in fostering peace and trust, alongside the potential risks posed by its misuse. The real-world examples and case studies demonstrated how technological innovations such as artificial intelligence (AI), blockchain, and social media can improve global communication, increase transparency, and enable early conflict prevention. AI-powered systems have been found to improve cybersecurity, reduce misinformation, and provide predictive insights for humanitarian efforts, whereas platforms such as social media and translation tools foster international understanding and collaboration. Simultaneously, ethical issues also raised by technology innovations—privacy problems, algorithmic bias, and the potential of exploitation—are thoroughly studied. Collaborative regional efforts, such as ASEAN's Cybersecurity Cooperation Strategy, highlight the necessity of international coordination in ensuring a safe digital future. Finally, this paper proposes the responsible use of technology as a catalyst for trust, unity, and long-term peace, emphasizing the importance of ethical behaviors and collaborative action to realize its full potential.

Keywords: AI Ethics; Digital Diplomacy; Peacebuilding; Predictive Analytics; Conflict Prevention

AUTHOR:

TAN JING JIE

(MALAYSIA)

Imagine opening the news to yet another headline about a big data breach or an AI-powered scam, raising new questions about how technology influences our lives. It's understandable that many of us are concerned about artificial intelligence and digital innovation. After all, the proliferation of frauds and cyber dangers has painted a bleak picture of a society in which the instruments designed to ease and protect our lives appear to be sources of anxiety and vulnerability. In 2023, cybercriminal activities in Southeast Asia resulted in losses amounting to USD 37 billion, driven by various illicit operations, including AI-involved fraud schemes. This worrisome figure emphasizes the essential importance of using technology responsibly to foster trust and security. (Herzlich, 2024).

I have discovered that my PhD studies' **application provides benefits but is also associated with potential risks of misuse and misplaced trust.** For instance, one of my developed applications, “Social Enhancement Application for Visually Impaired People”, incorporates a custom-trained low-resolution image-to-text model: Siamese-Driven Optimization for Low-Resolution Image Latent Embedding in Image Captioning (Tan, 2022; Tan et al., 2024). This app serves as an "eye" for visually impaired individuals, enabling them to identify people, recognize emotions, estimate the age and gender of those nearby, and receive descriptions of their surroundings through machine learning. However, despite its potential, the app poses major risk – **privacy could be jeopardized** by the machine learning attacker or even from the developer, or errors could arise simply due to algorithmic bias or faults in the machine learning system. Such errors could even endanger lives — for example, if **the app prompts the user to trust a malevolent individual, sensitive information is mistakenly provided to the incorrect person**. At the same time, for text output aimed at visually impaired individuals, personality recognition models play a role in customizing the output. These models not only perform recognition but also enhance the classification of sentiments, emotions, and more (Tan et al., 2023). Their purpose is to better understand users and suggest activities tailored to their personalities, ultimately improving interaction. This raises questions about possible abuse, though, as it may unintentionally result in **negative outcomes like sadness or even suicide if someone regularly and silently alters their mood by manipulating the system.**

Instead of merely exacerbating our fears, technology should help us alleviate them. It should be a force for good, a means to bring people together and create a foundation for mutual understanding. As we navigate an increasingly interconnected world, the real challenge comes in changing our attitude to innovation—utilizing technical developments to build harmony, rather than breaking trust.

In the highly interconnected world of today, **social media technology serves as a potent conduit for communication.** Effective communication facilitates information exchange, reduces misunderstandings, and helps prevent scams arising from information asymmetry (Bouraffa & Hui, 2025). Social media platforms are able to break down boundaries of language and geography, allowing billions of people to communicate quickly. Users can communicate in real time, share information, and raise awareness of global concerns on platforms like Twitter, Instagram, and TikTok. According to Kemp (2024), there are about 5 billion social media users are active globally, comprising 62.3% of the world's population. This highlights the enormous potential of social media platforms to bring people together from all over the world while digital influencers and key opinion leaders (KOLs) are important for promoting intercultural understanding. These people frequently post content that raises awareness and educates others, igniting discussions on significant issues like social justice and environmental preservation. They play a crucial role in encouraging positive change and aid in bridging cultural divides by utilizing their sizable fan bases. For instance, campaigns led by influencers can reach millions within hours, amplifying messages of peace and promoting global initiatives. In addition to advancements in translation technology, including apps that use large language models, make communication even easier by interpreting messages' context in addition to their literal meaning. For instance, about 3 million American users switched to China's RedNote app during the temporary TikTok ban in the United States in January 2025, encouraging cross-cultural contacts between Chinese and American users (Fu & Cohan, 2025). This illustrates how technology, especially artificial intelligence (AI) translation skills, facilitates meaningful engagement between individuals with diverse linguistic origins, opening doors to increased empathy and teamwork.

Technologies can also promote trust by **increasing transparency and accountability across various sectors.** For instance, innovations like blockchain technology guarantee that data cannot be altered due to its decentralized nature. This has revolutionized secure and transparent record-keeping, particularly in voting systems, public service record management, and financial transactions. According to Fortune Business Insights (2024), the global blockchain technology industry is projected to grow at a compound annual rate of 52.8%, increasing from USD 27.84 billion in 2024 to an estimated USD 825.93 billion by 2032. Similarly, the World Bank (2020) underscores the transformative potential of open government initiatives, which prioritize responsiveness, accountability, transparency, and public participation, in reducing corruption.

In the private sector, businesses are likewise using technology to meet more strict compliance requirements and acquire client trust. Adopting the Internet of Things (IoT) and blockchain technology can add value to supply chain monitoring solutions, allowing their stakeholders to verify the provenance of everything from luxury goods to food items, ensuring that ethical standards are met (Raja Santhi & Muthuswamy, 2022). In a similar vein, AI-powered monitoring systems and whistleblower platforms give staff members secure channels to report unethical activity, reaffirming a company's dedication to honesty. As Mike Paul aptly stated, "Trust, honesty, humility, transparency, and accountability are the building blocks of a positive reputation" (Blind, 2007; Kemp, 2024).

On the other hand, **technologies like data analytics and machine learning have completely changed how we anticipate and avoid conflicts.** Artificial intelligence (AI), in particular large language models (LLMs), can identify tendencies that might indicate rising tensions by examining enormous volumes of data from many sources, including news articles, social media trends, and economic indicators. For example, social media analysis can reveal spikes in negative sentiment or the spread of inflammatory content, serving as an early indicator of potential conflict. These findings can be used by governments and international organizations to assign resources or send out mediation teams to defuse tensions before they turn violent. According to The Centre for Humanitarian Data (2019), predictive analytics have significantly enhanced crisis response efficiency. For example, in Somalia, predictive models anticipated food insecurity, enabling earlier interventions and reducing response times by up to 50%. Such proactive, data-driven strategies foster trust in humanitarian efforts, demonstrating reliability and commitment to timely action, thereby avoiding further loss of confidence. Beyond conflict prevention, AI algorithms are critical in disaster preparedness and mitigating the spread of fake news during crises. Predictive models that analyze weather data and geological activity help anticipate natural disasters, allowing authorities to issue timely warnings and minimize loss of life. For instance, in 2023, predictive alerts enabled the evacuation of approximately 232,000 individuals in Canada due to wildfires (Jones et al., 2024). At the same time, AI-powered systems can monitor and counter the spread of misinformation or fake news during such emergencies, which can exacerbate panic or hinder relief efforts. In essence, AI goes beyond prediction and classification; it actively fosters confidence by enabling timely, reliable, and data-driven interventions that build trust in crisis response and humanitarian efforts.

Furthermore, **technology has opened new avenues for peacebuilding,** allowing organizations and individuals to engage in conflict resolution and education even across great distances. Digital platforms facilitate virtual peace talks by connecting stakeholders who might otherwise be inaccessible due to geographic or political barriers. These platforms are essential in regions where conventional diplomacy is challenging, offering a forum for discussion. Furthermore, AI-powered tools play a significant role in peacebuilding by analysing massive amounts of conflict-related data to identify key actors, track changing dynamics, and recommend successful mediation tactics. For example, AI-powered platforms can map conflict zones and recommend the best courses of action based on historical patterns. Artificial intelligence (AI) has considerably boosted peacebuilding efforts by increasing negotiating success rates. For example, AI technologies have been utilised to promote peace talks in the Yemen war, demonstrating its potential to organise complicated data and assist mediators in understanding conflict processes. (Arana-Catania et al., 2022). Additionally, digital storytelling and virtual reality (VR) experiences are being used to foster empathy and understanding between conflicting groups. These technologies allow users to experience the realities faced by others, breaking down prejudices and encouraging mutual understanding. Initiatives like the "Digital Storytelling as Community-Based Intercultural Learning in Higher Education" project have gained traction, enabling individuals from conflict zones to share their narratives (Marshall, 2021). These emerging technologies collectively open new avenues for peacebuilding by bridging divides, enhancing mediation efforts, fostering greater understanding among conflicting parties, and promoting education that empowers communities to address conflicts constructively.

While technology raises security problems, it also delivers solutions to these negative risks. As technology improves, so do cybercriminals' threats, which use system vulnerabilities to destabilize stable economies, violate privacy, and even influence democratic processes. Prioritizing investment in AI-driven threat detection and automated response systems is essential, as they can analyze patterns and detect anomalies much faster than humans, facilitating swift and effective reactions to emerging threats. IBM's Cost of a Data Breach Report (2024) highlights the significant impact of AI-powered automation on cybersecurity efficiency. Organizations that extensively implemented security AI and automation reduced the average time to identify and contain a data breach by nearly 100 days compared to those without these technologies. Additionally, organizations employing extensive AI security automation not only saved an average of $2.22 million per data breach but also reduced their cybersecurity insurance costs (Funk & SevenAtoms, 2024).

These findings underscore the critical role of AI in not only strengthening cybersecurity defenses but also in providing substantial economic advantages. Moving on, international collaboration is critical for improving global cybersecurity. Global cybersecurity alliances and information-sharing mechanisms allow states to collaborate to defend against cyberattacks (AlDaajeh et al., 2022). The Association of Southeast Asian Nations (ASEAN) also exemplifies such collaborative efforts. ASEAN has developed a Cybersecurity Cooperation Strategy (2021–2025) focusing on advancing cyber readiness, strengthening regional policy coordination, and enhancing trust in cyberspace, aiming to create a safe and secure ASEAN cyberspace (Association of Southeast Asian Nations, 2021). The creation of global rules for ethical cyber behavior is critical to preventing digital conflicts from turning into real-world disasters. Prioritizing cybersecurity allows us to create a safer and more secure digital environment, ensuring that technology remains a source of growth and peace.

In a nutshell, as we navigate the digital age, the potential of technology to promote peace and trust has become increasingly apparent. From facilitating global communication and fostering understanding to enhancing transparency and enabling early conflict prevention, the benefits of innovation are transformative. Cybersecurity stands as a critical pillar, with AI and automation significantly reducing breach detection times and fortifying our defenses against malicious threats. Yet, alongside these advancements come responsibilities—ensuring ethical practices, safeguarding against misuse, and fostering international collaboration to establish norms for digital safety. In this setting, ASEAN's efforts to advance regional cooperation on cybersecurity and digital governance highlight the need of taking collective action to solve these concerns. Our common challenge is to use these technologies for good, to bridge gaps, protect our futures, and create a society where digital developments promote peace and trust. Our vision of a united, harmonious world is achievable if we commit to using technology as a force for connection and progress. Let us work together to ensure that technology remains a tool of unity and a lasting beacon of hope for generations to come.

BIBLIOGRAPHY

- AlDaajeh, S., Saleous, H., Alrabaee, S., Barka, E., Breitinger, F., & Raymond Choo, K.-K. (2022). The role of national cybersecurity strategies on the improvement of cybersecurity education. Computers & Security, 119, 102754. https://doi.org/10.1016/j.cose.2022.102754
- Arana-Catania, M., van Lier, F.-A., & Procter, R. (2022). Supporting peace negotiations in the Yemen war through machine learning. Data & Policy, 4, e28. https://doi.org/10.1017/dap.2022.19
- Association of Southeast Asian Nations. (2021). ASEAN Cybersecurity Cooperation Strategy (2021–2025). https://asean.org/wp-content/uploads/2022/02/01-ASEAN-Cybersecurity-Cooperation-Paper-2021-2025_final-23-0122.pdf
- Bouraffa, T., & Hui, K.-L. (2025). Regulating Information and Network Security: Review and Challenges. ACM Comput. Surv. https://doi.org/10.1145/3711124
- Fortune. (2024). Blockchain Technology Market Size, Share & Industry Analysis. Fortune Business Insights.
- Fu, T., & Cohan, D. (2025). TikTok refugees are pouring to Xiaohongshu. Here's what you need to know about the RedNote app. The Associated Press. https://apnews.com/article/tiktok-refugee-xiaohongshu-rednote-855692624aa52825b30afc5474af881d
- Funk, J. & SevenAtoms. (2024). The AI edge in cybersecurity: Predictive tools aim to slash response times. In Venture Beat.
- Herzlich, T. (2024). Southeast Asia cyber scammers stole $37B in 2023 as AI-driven crimes soar: UN report. New York Post.
- IBM. (2024). Cost of a Data Breach Report 2024. IBM.
- Jones, M. W., Kelley, D. I., Burton, C. A., Di Giuseppe, F., Barbosa, M. L. F., Brambleby, E., Hartley, A. J., Lombardi, A., Mataveli, G., McNorton, J. R., Spuler, F. R., Wessel, J. B., Abatzoglou, J. T., Anderson, L. O., Andela, N., Archibald, S., Armenteras, D., Burke, E., Carmenta, R., … Xanthopoulos, G. (2024). State of Wildfires 2023–2024. Earth System Science Data, 16(8), 3601–3685. https://doi.org/10.5194/essd-16-3601-2024
- Kemp, S. (2024). Digital 2024: Global Overview Report. Data Reportal.
- Marshall, D. J. (2021). Digital Storytelling as Community-Based Intercultural Learning in Cultural/Historical Geography. In Experiential Learning in Geography (pp. 211–225). Springer International Publishing. https://doi.org/10.1007/978-3-030-82087-9_13
- Raja Santhi, A., & Muthuswamy, P. (2022). Influence of Blockchain Technology in Manufacturing Supply Chain and Logistics. Logistics, 6(1), 15. https://doi.org/10.3390/logistics6010015
- Tan, J. J. (2022). Real-time face recognition social enhancement for visually impaired people [PhD Thesis]. UTAR.
- Tan, J. J., Kwan, B. H., Ng, D. W. K., & Hum, Y. C. (2023). Enhancing Performance in Sentiment Classification of Textual Messages through Personality Recognition Integration. Proceedings of the 11th International Symposium on Applied Engineering and Sciences (SAES2023), 258–259.
- Tan, J. J., Mokraoui, A., Kwan, B.-H., Ng, D. W.-K., & Hum, Y.-C. (2024). Siamese-Driven Optimization for Low-Resolution Image Latent Embedding in Image Captioning. 2024 Signal Processing: Algorithms, Architectures, Arrangements, and Applications (SPA), 79–84. https://doi.org/10.23919/SPA61993.2024.10715604
- The Centre for Humanitarian Data. (2019). Predictive Analytics in Humanitarian Response. In The Centre for Humanitarian Data.
- World Bank. (2020). Enhancing government effectiveness and transparency: The fight against corruption. In World Bank.

ADDRESSING TECHNOLOGY-FACILITATED GENDER-BASED VIOLENCE: WORKING TOWARDS A SAFER CYBERSPACE FOR ALL

ABSTRACT

Violence in any form should not be tolerated, given that human rights are globally acknowledged and declared. Among different forms of violence, online violence is unique due to its nature and the impacts it creates. Moreover, technology-facilitated gendered violence is often overlooked since the perpetrators escape their crimes with ease; meanwhile, the victims may also lose chances to proclaim their miseries, ensure justice and return to safer cyberspace. Even though there are ongoing initiatives and active policies to secure cybersecurity for everyone, regardless of gender, people's virtual profiles are still susceptible to fraud and threats, simply because of their gender. Moreover, the impacts that are created by virtual violence can be serious, ranging from depression and mental issues to physical inflicts. Therefore, it is of colossal importance to combat online gender-based violence and help build a safer virtual space for everyone.

Keywords: Technology-Facilitated Gender-Based Violence; Cybersecurity; Cyberbullying; Human Rights

AUTHOR:

MAY THET MAUNG

(MYANMAR)

Introduction

Gender-based violence has existed long before the emergence of information technology. It has been a prevalent issue across the globe: rising from various root causes from patriarchy to basic gender stereotypes and appearing in a variety of forms such as harassment, physical abuse, and psychological manipulation. With the rise of technology, such violent acts have also switched to virtual network-based. Being the victim of cyberbullying is not restricted to females (Sey, 2022). Without well-framed cybersecurity laws, anyone on the virtual platform, using any of the established social media sites, has the potential to be victimised by gender-based violence. However, globally, women and girls are disproportionately subjected to gender-based violence (SIDA, 2019). Therefore, battling against online gender-based violence and creating safe digital spaces for all are vital to ensuring secure and efficient online communication. This essay aims to explore the divergent styles, the impacts and the causes of online gender-based violence, concentrating on the discussion of feasible solutions to combat it and proposing several multilevel and all-inclusive approaches.

Different Forms of Online Gender-based Violence

Online gender-based violence is mainly confined to several issues, ranging from some as basic as contributing negative comments on social media postings and publicly defaming individuals on virtual sites to some as damaging as illegally accessing private information, identity thefts and blackmailing to harass or frighten someone, based on their gender. Referring to these activities, online gender-based violence is deemed to embody any activities that induce physical or psychological impairments or hinder the exercising of human rights by individuals due to their gender in cyberspace. Particularly, cyberbullying young girls by threatening to expose explicit photos could even lead the victims to end their own lives (BBC, 2012). According to the UN Women (2023), (16) to (58) per cent of women are experiencing online violence.

Fundamentals of Online Gender-based Violence

Social norms play an important role in causing violence against people based on their genders, either in-person or online. Not only women and girls but also gender non-conformists often suffer from brutality, directly aimed at them owing to patriarchy and sexism. False pride and gender superiority, occasionally, disturb people from safely expressing themselves online. In many cases, abusers of free speech in cyberspace overexploit their rights to express their opinions by sending constant direct messages or leaving hateful comments on people's social media profiles, which may affect the well-

being of both the victims and other observers negatively (Walther, 2022). Moreover, executing gender-discriminative violence is much more accurate and independent online than in person. Technological functions are also deemed to be influenced by traditional gender norms (Wilkinson et al., 2024). Thanks to anonymity, offenders can escape criminal charges effortlessly since advanced technology can equip them to erase their digital footprints once they are exposed. The motive behind the perpetrators' mind can often be the deciding factor, such as financial gain and sexual exploitation. Regardless of the extent of online gendered violence, it generates immense impact on the lives and communities of the victims.

Impacts of Online Gender-based Violence

Online harassment, often imposes risks to people who seek public popularity in professional or academic contexts with defamation being the major issue. Meanwhile, human trafficking and young people accidentally participating in criminal activities are encouraged by cyberbullying as well. Numerous psychological problems faced by people can also be linked to receiving cautionary messages and being shamed in public owing to their gender. As women, girls and gender non-conformists are highly susceptible to gender-based violence, it is undoubtedly challenging for them to take on the roles of leaders and activists. Women and girls are considered vulnerable under traditional norms so they often lose chances to lead even if well-suited to do so, especially in public sectors such as politics and the digital economy (Sey, 2022). Therefore, online gender-based violence may discourage women, girls and gender non-conformists from expressing themselves freely and consequently, deny fundamental human rights to them.

At the same time, virtual gendered violence could also weaken the efficient implementation of the Sustainable Development Goal (5): Gender Equality as women and girls lose their chances to participate equally in global race. Not only to eliminate cyber-based gendered violence but also to prevent all cybercrimes, both public and private sectors have commenced extensive initiatives depending on regional specifications.

Government Initiatives to Respond to Online Gender-based Violence

According to Papapietro and Macabies (2024), the European Union has recently adopted "the first-ever directive to combat violence against women and domestic violence [...], recognizing several forms of online gender-based violence such as non-consensual sharing of images and cyberstalking as violence against women".

Through this initiative, cyberspace has transformed from an unruly virtual society into a more regulation-driven social space with safe publicity, protecting women's rights not only from a social but also from an economic perspective, as women entrepreneurs tend to publicize their visual information on cyberspace. As an ongoing process, the effectiveness of this initiative is progressive and variable depending on the implementation by each member state.

In countries such as the Philippines, the Safe Spaces Act (2019) was passed, publicly adopting the idea of gender-based violence sexual harassment, including "threats (physical, psychological, and emotional), unwanted sexual misogynistic, transphobic, homophobic and sexist remarks and comments online whether publicly or through direct and private messages" (Philippine Commission on Women, 2021). This detail-oriented act serves as an inclusive mechanism for all forms of cyber-based gender-related crimes, ensuring that no crime is left unpunished, no matter how minuscule it is. In Korea, the Digital Sex Crimes Monitoring taskforce was founded in 2019 to detect and enforce deterrence on the spreading of non-consensual images and videos both on Korean and foreign websites (Wilkinson et al., 2024). This particular step has assisted the enforcers in efficiently preventing cyber-based crimes beforehand. These government-led initiatives are applicable to appeal to fellow administrations around the world in acknowledging online gender-based violence and generating counteractive measures against them.

Moreover, women and girls are still protected by UN-led bodies such as the United Nations General Assembly (UNGA) and the Human Rights Council (HRC) (Flemming & Castro, 2023). Overall, deterring online gender-based crimes via government initiatives is a more reliable strategy, compared to taking action only after the crimes have transpired, as it endows women with safety and security in cyberspace without having to be concerned about dignity and privacy breaches.

Private Sector Initiatives Against Online Gender-based Violence

The role of non-profit organizations and technological giants is enormous in eradicating online gender-based violence. On the one hand, networks such as the Sexual Violence Research Initiative focus on funding research projects, providing spaces and knowledge access to develop awareness on studies of technology-facilitated gender-based violence and strengthening the prevention of gendered violence worldwide (Sexual Violence Research Institute (SVRI), 2024).

On the other hand, the aspect of technological giants such as Google or Meta can be controversial in discussions regarding online gender-based violence. Such companies rarely respond to call-outs on virtual crimes against marginalized groups unless they are charged or heavily pressured by the public, considering different priorities and business orientation (Wilkinson et al., 2024). Technological support and expertise from private sectors are to be appreciated as they can cooperate with the online monitoring task forces in identifying virtual crimes timely and adequately.

Moreover, those tech giants still maintain the capability to check and balance online interactions on their platforms, so their initiatives on enhanced cybersecurity would be more directly effective than those laid out by other sectors such as content moderation mechanisms and transparency in reporting. By cooperating with the public sector, they would be of great assistance in combating against online gendered violence and mitigate the number of cybercrimes. Beyond observing the multiple strategies from different regions, the following section will discuss the author's perspectives on improving cybersecurity regardless of their personal and gender backgrounds.

Recommendations

A top-down approach is a promising answer; as it underscores the vitality of policy making and law enforcement to permeate social awareness on online gender-based violence to the masses. Actions against technology-facilitated gendered violence could be expended towards the grassroots level; advertisement campaigns and public talks, online commercials, and integration of celebrities and influencers' support in raising awareness among the people. Raising awareness among the people is significant, given that most occupied adults and underaged children might fall victim to cyber-based crimes. Furthermore, victim-survivors of online gender-based violence should be welcomed and encouraged to report their experiences to the authorities and seek justice. Their stories, shared with their consent, can be some good examples to potential victims and even everyone in cyberspace. Furthermore, this proactive drive facilitates mental rehabilitation and creates a haven for the victims to rebuild a sense of security in society. Moreover, government-led initiatives are often criticized due to information undisclosed to the public and a lack of checks and balances. Multi-faceted investigations should be taken to process with more transparency in the government sector, and the imposition of cyber security law should be explicit.

In the private sector, cybersecurity measures should be comprehensive; tech giants have to listen to and support safety concerns raised by non-profit organizations and governments and take immediate action. Their collaboration with the governments in enabling advanced monitoring technology to deter cyber-based crimes should be encouraged.

For parents, young children using technology and cyberspace are supposed to be closely supervised as they may not fully understand how some functions work and may eventually publicise some sensitive information. In middle schools and high schools, STEM-based education should incorporate the risks of cybersecurity complications. In society, victims of online gender-based violence should have enough assistance from their surroundings. In case they are required to rehabilitate mentally or physically, aid should be available to them, regardless of time and place. Nevertheless, the proposed solutions would have to face several challenges prior to implementation as discussed below.

Challenges in Ending Online Gender-based Violence

The most prominent factor is built-in gender norms that most people still hold on to; technology-facilitated gendered violence exists because of fundamental attitudes towards gender roles and supremacies. It is rooted in biased outlooks which may obstruct public awareness campaigns. In stereotypical households, patriarchy mainly prevails with some members being silenced by their own families in expressing their opinions freely. Even in case of sexual violence, either offline or online, they may be told not to report it, out of shame and guilt suffered by the head of the household.

Cybersecurity loopholes in social media sites and websites may be exploited by the governments and tech giants, themselves, to earn profit. In such cases, victims may necessitate the community's support in seeking justice, where again the community might be deterred from helping the victims. Furthermore, social communication platforms provide easier access to cross into random people's direct messages and make prevention efforts more vulnerable compared to offline initiatives. Sometimes, it seems formidable for governments to allocate a significant amount of budget to preventing online gender-based violence. For instance, Myanmar, as one of the least-developing countries with network connection issues, would find it hard to adopt robust cybersecurity measures that genuinely protect its people from cyber-based violence, in comparison to other regional countries such as the Philippines and Malaysia.

The values of human rights entail inclusivity in all sectors of interaction; from in-person dealings to virtual networking. The female members of society are no exceptions to this: they engage in networking on cyberspace, promote their businesses and pursue academic development. Therefore, the challenges that impede them from entering safe cyberspace should be tackled with diligence and comprehensive public-private cooperation.

Conclusion

Briefly, technology-facilitated gendered violence is obtrusive and prevalent across the globe; however, in some remote regions of the world, the violence is not well-recognized and the victims are still shadowed by other economic and political struggles. As it may arise from various causes including social norms and technological loopholes, the violence is, sometimes, hard to track down. However, network designers are also aware of the widespread cybersecurity breaches, so further alterations and regulations on social communication platforms are expected in the future (Wilkinson et al., 2024). Combating online gendered violence and creating a safer cyberspace for all cannot be executed by a single person, a single community or even by a single government. The actions must be implemented at every level of the community with public-private partnerships, ensuring the participation of everyone who is well aware of the issue and once victimised by the violence. Calls in unity are guaranteed to bring improvements in actions.

BIBLIOGRAPHY

- BBC. (2012, October 17). Amanda-Todd: Memorial for teenage cyberbullying victim. https://www.bbc.com/news/newsbeat-19960162
- Flemming, S., & Castro, F. (2023, April). Online gender-based violence: Implications, developments and the legal framework. Global Human Rights Defence. https://www.ghrd.org/wp-content/uploads/2023/11/Online-Gender-Based-Violence-implications-developments-and-the-legal-framework.pdf
- Papapietro, G., & Macabies, A. D. (2024, November 25). Online gender-based violence in the EU: What now? Center for Democracy and Technology. https://cdt.org/insights/online-gender-based-violence-in-the-eu-what-now/
- Philippine Commission on Women. (2021, September 17). FAQs Republic Act No. 11313: Safe spaces act (Bawal Bastos law). https://pcw.gov.ph/faq-republic-act-no-11313/
- Sexual Violence Research Institute (SVRI). (2024, September 26). English full report. Technology-Facilitated Gender-Based Violence: Developing a shared research agenda. https://www.svri.org/english-full-report-technology-facilitated-gender-based-violence-developing-a-shared-research-agenda/

- Sey, A. (2022, December 13). Gender security and safety in the ASEAN digital economy. Economic Research Institute for ASEAN and East Asia. https://www.eria.org/publications/gender-security-and-safety-in-the-asean-digital-economy
- SIDA. (2019, September). Gender-based violence online. https://www.sida.se/en/about-sida/publications/gender-based-violence-online
- UN Women. (2023, November 13). Creating safe digital spaces free of trolls, doxing and hate speech. https://www.unwomen.org/en/news-stories/explainer/2023/11/creating-safe-digital-spaces-free-of-trolls-doxing-and-hate-speech
- Walther, J. B. (2022). Social media and online hate. Current Opinion in Psychology, 45, 101298. https://doi.org/10.1016/j.copsyc.2021.12.010
- Wilkinson, I., Hofstetter, J.S., Shires, J., & Yahaya, M. S. (2024, June 28). The role of the private sector in combatting gendered cyber harms. Chatham House – International Affairs Think Tank. https://www.chathamhouse.org/2024/06/role-private-sector-combatting-gendered-cyber-harms/05-private-sector-state-interaction

BEYOND THE HASHTAGS AND SUPERFICIALITIES: A CALL TO ACTION FOR GENDER- INCLUSIVE SAFE SPACES IN THE CYBERSPACE

ABSTRACT

In the rise of digitalization across the globe, so is the increase in the different types of violence and cruelty because of some who would take advantage of these innovations in the area of Information, Communication and Technology. One of the emerging types of these violence is the online gender-based violence which centers on violences done in the cyberspace which is attributed to the gender of the victims. Research shows that women and girls in the minorities, who have disabilities, as well those who identify themselves as members of the LGBTQIA+ community are disproportionately attacked by these violences online. This paper tackles these issues of digital gender-based violence in the world, in the Asian region, as well as in the author's home country. The paper will also propose some strategies and interventions to effectively combat this problem. Finally, the author proposes this paper as a call to action to those in power, who has the authority and everyone including the public, to be vigilant in fighting against online gender based violence, to call out the offenders of this type of violence and to serve as an agency for the victims to stand up and fight for their rights and create the digital space as a safe space for everyone.

Keywords: Intersectionality; Online Gender-Based Violence; Safe Space; Women; Gendered Disinformation

AUTHOR:

APHIA KATHERINE D. FAJARDO

(PHILIPPINES)

Bustling nations, remarkable people and synergies of cultures, the Southeast Asian Region truly defines harmonious diversity within its nations. The Association of the Southeast Asian Region is continuously aiming for peacebuilding in every facet of life. In pursuit of this peacebuilding, it is important to determine the current issues surrounding the region. It is important to realize that with the rise of the digital age, there is also a rising issue of violence and human rights violations that could take place in cyberspace. Online gender-based violence, as much as one of the most common types of violence committed on cyberspace, is more often overlooked and undermined. This is due to the nature of it being done online or virtually, which is perceived by some as less intense because it doesn't cause any bodily harm to the victims. As stated by the International Media Support (2021), online gender-based violence is often neglected and overlooked due to the same roots of every gender-based violence out there–gender inequality and power struggle of women.

Try scrolling in social media platforms now, and most likely you would come across posts, videos, or reels that use the hashtag #womeninmalefields. It is mostly used on posts which are related to the experiences of women in some aspects of their lives. These posts are meant to be sarcastic, in a sense that it targets the usual toxic stereotype of men on women with their roles dating, relationships, family roles, gender roles, and even on career. As discussed by The Economic Times (2024), this trend is an eye opener for everyone, especially for men, on every statement, remarks or stereotypical gender expectations towards their partners hurt them. It's like giving men a "taste of their medicine" through these satirical and sarcastic Internet posts.

At a hindsight, this trend is effective in illustrating the realities faced by women in the different aspects of their lives which is often overlooked as society expects women and girls to just conform with the patriarchal culture of the society. The trend is more than just a counter argument to the toxic behavior of men towards women, but is also an eye opener for everyone to realize the stereotypes and bullying experienced by women.

Before moving into the main parts of this paper, it is important to have a clear definition of online gender-based violence. According to Tanusi (2021), it is a type of violence that takes place in cyberspace which involves gender discrimination and injustices. Some online gender-based violences are in the form of stalking, trolling, doxxing, cyberbullying, and unsolicited pornography, misinformation and deep fakes (AI generated photos and videos).

In this type of systemic violence, it is the women and the girls who are disproportionately and adversely affected due to their unique traits. Another term to define in this paper is “intersectionality”. As defined by the Oxford dictionary, it is used to describe the overlapping discrimination experienced by certain members of a society which is most often attributed to their demographics and social statuses. The term was coined by Kimberle Crenshaw (1989) to properly label the discrimination and oppression experienced by African-American women, all because they are women and their race.

On a world view, statistics and stories emphasize the unfortunate experiences of women and girls about online gender-based violence they have gone through in cyberspace, particularly in the different social media platforms today. According to the United Nations Population Fund Philippines (2023), nearly 60% of women and girls who participate in cyberspace, most commonly through social media platforms, experienced some form of digital violence. Furthermore, the intersectionalities of women, girls, members of the LGBTQIA+ community, African women and Black American women, are often the target of this digital violence. Research shows that black women have an 84% higher chance of experiencing online gender-based violence compared to white women. Another report from UN Women in 2023 emphasized that across the world, around 16-58% of women and girls experience this online gender-based violence. Similarly as discussed in the same report, European studies show that women are 27% more at risk of being targeted by online or digital violence compared to men. Sixty percent of women in the Arab region who are internet users also experience this type of violence. Several research shows that 92% of women, across the world, who experienced this type of online violence reported that its has negatively affected their overall wellbeing. Finally, in another study conducted by Amnesty International in 2018, it has been established that women of color (Black, Asian, Latin, etc), are 34% more likely to experience this type of violence in the digital space.

Delving deeper, online gender-based violence is also prevalent in Asia, as well as in the ASEAN region. In a 2021 study cited in the research of Bansal et al (2023), statistics show that the prevalence rate of online violence to women is at 88% in the Asia-Pacific region. In the South and Southeast Asian region, the prevalence of this online gender-based violence was the highest during the lockdown of the COVID-19 pandemic.

Another study conducted by UN Women (2020) in 2019 in the five countries of Republic of South Korea, India, Malaysia, Pakistan, the Philippines which is aimed at analyzing the ICT VAWG in these countries reinstated the argument that violence against women, even in the cyberspace, is still prevalent. Some of the widespread digital violence acted on women in the Internet are sexist and misogynistic comments and gender-hate comments, voyeurism, morphing of women and girl's faces, as well as threatening or posting sensitive videos and photos of women such as during sexual intercourse or worst, rape footages of women and girls. This rise in the number of misogynistic posts during the COVID-19 lockdown is further emphasized in a report of UN Women Asia and the Pacific (2024) where Sri Lanka, Malaysia and India have recorded a 168% of misogynistic posts online. Women and girls who also have active participation in the public and political landscape are also a target of this digital violence in an attempt to silence them and their voices, and to "put them in their places". This phenomenon is witnessed and experienced by female journalists, not just in Asia but across the globe. Studies show that three out of four women (73%) have experienced online violence due to their line of work (International Media, Support, 2021).

Filipino women and girls aren't safe from O-GBV. As cited by the UNFPA Philippines in its report in 2023, the most prevalent types of digital violence against women are non-consensual distribution of intimate images (48.00%), threats of violence or blackmail (41.33%), and deleting, changing or faking personal data (22.67%). Another article by Berizo (2023) cited that the Foundation for Media Alternatives recorded a staggering 686 cases of online gender-based violence in their midyear report. Consequently, as discussed in the same article of Berizo, the Commission on Human Rights' Gender Ombud Report revealed that there is an increase in this type of violence during the COVID-19 pandemic lockdown. The 2022 was also a presidential election year for the Philippines, and studies show that misogynistic remarks on female candidates were more rampant compared to their male competitors.

Another topic closely related to these cases of online gender-based violence is the phenomenon of gendered disinformation. This pertains to the intentional and misleading attacks which further propagate the existing gender biases and stereotypes, affecting mostly the women. It further exacerbates the problem on gender equality and safe spaces since the different fallacious and misleading narratives on women affect their credibility and image (Veritasia, Muthmainnah, de-lima-Santos, 2024).

Similar to the cases of female journalists experiencing O-GBV, gendered disinformation is widely observed in politics, wherein female politicians are often the target of these malicious and fallacious narratives.

Everything presented in this paper is just focused on the data and statistics provided by the different organizations who are focused on shedding light to this neglected issue of digital gender violence. It does not account the untold stories and unreported cases because of fear, threats and the perennial problem of stigmatization of the society to the victims. These numbers do not account for the fear, trauma and distraught brought by the perpetrators of this violence to their victims. It does not account for the stress, the adverse emotional, physical and mental effects of seemingly unharmful remarks from people. These numbers do not reflect the everyday struggle and challenge of victims which are subjected to public shame, harassment and bullying which results to sleepless nights, panic attacks, anxiety attacks, depression and more, just because of their sexual orientation, gender identities, age, race, work, disabilities, cultures, social statues, etc. It is important to realize that online gender-based violence, just like any other types of violence, is a threat to human rights, and thus perpetrators should be penalized accordingly for victims to get the justice they rightfully deserve.

Gender-based violence is truly one the most long-standing issues affecting women and girls. Every country has their laws to protect people from these types of violences, especially the women and girls who are more vulnerable and susceptible to experiencing violence. However, some, or maybe most of these laws and legal instruments may not cover the digital landscape, hence the difficulty to report these types of violences to the authorities and properly sanction the perpetrators. Most of the time, what we only consider as acts of violence are those that cause bodily harm which could be physically seen. But in the era of digitalization, we also have to adapt to the dangers brought by these innovations, as such update our legal policies so as to broaden the coverage of the provisions for these laws. Social media platforms in each country should have a specific set of regulations regarding posts and contents that involves or portrays online gender-based violence. Whenever there is a report about online gender-based violence, these social media platforms should have direct communication with the local law enforcement units of the specific country. In this way, taking legal actions towards O-GBV is faster and generally more efficient. Having specific and tailor-fit guidelines based on the local laws and policies of a country will ensure a more accessible way of reporting these types of violence.

Cumbersome procedures of reporting and gathering evidence sometimes also discourage the victims to report these types of violences they experience, hence they would just choose to silence themselves and go on with their life. Reporting such incidences should be easy, accessible and affordable to everyone regardless of their demographics and status in life. Help Desks in law enforcement units which specifically cater to O-GBV should be reinforced, with volunteers and employees who are knowledgeable enough to handle these cases.

In addition, we also have to acknowledge that online gender-based violence is a widespread phenomenon that doesn't just affect those in the urban areas. Even the communities living in rural and remote areas, which have little to no access to the Internet and cyberspace in general due to lack of infrastructures can be affected by this type of gender-based violence. For most, a large number of the rural population living in poverty also experience different types of discrimination and O-GBVs. As women and girls from the rural and marginalized communities turn online, they are disproportionately affected by these online gender-based violence. Since they are not sufficiently equipped with the knowledge to protect themselves from the online perpetrators of this type of gender-based violence, they are more at risk of O-GBVs. In line with this, infrastructure development, building and rehabilitation should be one of the focuses in rural development projects. Aside from building appropriate infrastructures to easily adapt to the digital age, cheaper digital devices, as well as mobile plans should be introduced and provided to rural and marginalized communities so that participating in digital activities with ease.

Teaching children proper etiquette in the digital space, as well as good manners and right conduct to everyone, regardless of their gender, demographics or work should be reinstated at a young age. Including these topics in the curriculum of children will help in combating this online gender-based violence. Aside from teaching them these manners and right conduct in the cyberspace, teaching them when to spot a content involving online-gender based violence, as well as knowing what to do in case that they become victims of these violences is extremely important so as to ensure that they are knowledgeable as they participate in the digital space, as well as prevent them from being enablers of O-GBV. Parents should also be encouraged by the school to teach their children on these topics in their homes.

The ASEAN region as a whole is also a crucial player in eradicating the online gender based violence experienced by women in association with their intersectionalities. Considering that the social media platforms aren't just focused on certain countries, but are used widely within the region and around the globe, strengthening international laws and policies and penalizations on these types of digital gender-based violences will impact greatly in reducing the incidences of these cases. Countries in the Southeast Asian region could also help one another through partnerships towards improving the infrastructure development in neighboring countries, as well as reducing the digital divide between rural and urban areas through development of the digital space, availability and accessibility in the more rural and marginalized communities. Providing sufficient support and funding to progressive organizations who aim to give light to the issue of intersectionality in cyberspace through advocacy campaigns, activities and research is also a step to reduce the prevalence of O-GBV.

As a region aiming for solidarity and reconciliation, we should realize that the purpose of modern technology and digitalization is to improve and make our lives easier. It aims to reach broader communities for everyone's active participation and empowerment. But what we are experiencing right now with online gender-based violence is the opposite of the primary objectives of these innovations. Instead of empowering everyone to talk and engage with communication and information dissemination through technology, some people attack them for their thoughts and opinions just because of their gender, race, age, social status, etc. Instead of being a safe space for everyone to tell about their stories, it became an avenue, and even a free pass for everyone to shame and criticize other people. Instead of encouraging everyone to participate in every online forum, what happens is that people, most especially the women and girls who are disproportionately attacked in these platforms, are invalidated and disempowered from voicing out their thoughts because people will just shame them for having opinions and all.

The trend #womeninmalefields is a reactionary approach from women who experience these misogynistic remarks from their counterparts. It is an effective tool for the women to efficiently call out other people from their disrespectful; behaviors on the Internet; finally, it is a lens that should be used to see the underlying issues of gender disparity in cyberspace which stem from the never ending dilemma on gender inclusivity and violence.

BIBLIOGRAPHY

- Amnesty International. “What Is Online Violence?” Amnesty International, 6 Aug. 2024, www.amnesty.org/en/what-we-do/technology/online-violence/.
- Bansal, V., Rezwan, M., Iyer, M., Leasure, E., Roth, C., Pal, P., & Hinson, L. (2024). A Scoping Review of Technology-Facilitated Gender-Based Violence in Low and Middle-Income Countries Across Asia. Trauma, Violence, & Abuse, 25(1), 463-475. https://doi.org/10.1177/15248380231154614
- Crenshaw, Kimberlé . “Kimberlé Crenshaw on Intersectionality, More than Two Decades Later.” Www.law.columbia.edu, Columbia Law School, 8 June 2017, www.law.columbia.edu/news/archive/kimberle-crenshaw-intersectionality-more-two-dec ades-later.
- ET Online. (2024, November 25). “Are we all dating the same men?”: Women in male fields TikTok trend is all over the Instagram. All you ne. The Economic Times; Economic Times. https://economictimes.indiatimes.com/news/international/global-trends/are-we-all-dating -the-same-men-women-in-male-fields-tiktok-trend-is-all-over-the-instagram-all-you-need -o-know/articleshow/115658213.cms?from=mdr
- International Media Support. “Virtual but Real: Online Violence against Women Journalists.” International Media Support, 8 Mar. 2021, www.mediasupport.org/news/virtual-but-real-online-violence-against-women-journalists/
- Sanusi, T. (2021, November 17). Online Gender-Based Violence: What You Need to Know. Global Citizen. https://www.globalcitizen.org/en/content/what-is-online-gender-based-violence-2/
- UNFPA Philippines. “Violence against Women and Girls Has Invaded All Spaces, Including Virtual Ones, and This Must End.” UNFPA Philippines, 2023, philippines.unfpa.org/en/news/violence-against-women-and-girls-has-invaded-all-space s-including-virtual-ones-and-must-end-6. Accessed 29 Nov. 2024.
- UNFPA Philippines. “UNFPA Launches Bodyright Campaign in PH to Counter Online Abuse vs Women.” UNFPA Philippines, 31 Mar. 2023, philippines.unfpa.org/en/news/unfpa-launches-bodyright-campaign-ph-counter-online-a buse-vs-women.
- UN Women. “Creating Safe Digital Spaces Free of Trolls, Doxing, and Hate Speech.” UN Women – Headquarters, 13 Nov. 2023, www.unwomen.org/en/news-stories/explainer/2023/11/creating-safe-digital-spaces-free of-trolls-doxing-and-hate-speech.
- UN Women Asia and the Pacific. “Online Violence against Women in Asia.” UN Women – Asia-Pacific, 2020, asiapacific.unwomen.org/en/digital-library/publications/2020/12/online-violence-against women-in-asia.
- UN Women Asia and the Pacific. “FAQs: Trolling, Stalking, Doxing and Other Forms of Violence against Women in the Digital Age.” UN Women – Asia-Pacific, 19 Nov. 2024, asiapacific.unwomen.org/en/stories/news/2024/11/faqs-trolling-stalking-doxing-and-othe r-forms-of-violence-against-women-in-the-digital-age. Accessed 29 Nov. 2024.
- Veritasia, M. E., Muthmainnah, A. N., & de-Lima-Santos, M. F. (2024). Gendered disinformation: a pernicious threat to equality in the Asia Pacific. Media Asia, 1–9. https://doi.org/10.1080/01296612.2024.2367859

THE HUMAN COST OF CYBER THREATS: THE IMPACT OF CYBER THREATS ON HUMAN SECURITY

ABSTRACT

While the use of cyberspace has become an integral part of our everyday lives, governments face significant challenges in ensuring cybersecurity and failure to do so may have effects on human security. This essay aims to explore a broad view of how cyberspace and human security are related, and how "cyber threat" – defined as a threat toward confidentiality, integrity, and accessibility of cyberspace – may undermine "human security," particularly in the Southeast Asian context. This essay argues that, due to increasing human dependency on cyberspace, cyber threats may cause major impacts on human security in at least two ways. First, cyber threats may create a "systemic restriction" of human security when access to and use of cyberspace, which usually contributes to human well-being, is degraded or disrupted. Second, cyber threats may also directly undermine human security itself when the confidentiality or integrity of crucial information is compromised. To effectively address these challenges, states must adopt a comprehensive approach that acknowledges the interconnected and multidimensional nature of cyberspace while still prioritising human security.

Keywords: Cybersecurity; Human Security; Cyber Threats

AUTHOR:

PANUTAD WATCHARAPORN

(THAILAND)

Introduction

As cyberspace becomes increasingly integrated into our daily lives, it is crucial to thoroughly explore potential threats and their impact on human security. However, conventional debates on international cyber affairs often prioritise state-level threats and outcomes, mostly through a military security lens (Zojer, 2019). Although this view of traditional security concerns is understandable, its narrow focus risks generalising cyber issues solely as high-politics and techno-deterministic issues, where human security is marginalised. As of 2022, Southeast Asia had approximately 460 million internet users, representing around 80% of the region (Kearney, 2023). The usage ranges from communication, economic activities, access to crucial information and government services, and political activities. Any disruption of cyberspace would inevitably affect these cyber-related activities. Therefore, studying cyber threats from a human security lens is necessary for states to better address this new security challenge.

Within this scope, "Cyber threats" refers to any threat toward confidentiality, integrity, or accessibility of information or systems related to the cyber domain. These threats are "multi-dimensional" (Clark, 2010), meaning they could refer to threats on the physical layer, the logical layer, the information layer, or the human layer of cyberspace.

This essay argues that, due to increasing human dependency on cyberspace, cyber threats may cause major impacts on human security in at least two ways. Firstly, cyber threats may create a "systemic restriction" of human security when access to the use of cyberspace which usually contributes to human well-being is degraded. In the second way, cyber threats may also directly undermine human security itself when the confidentiality or integrity of crucial information is compromised. The outline of this essay consists of four parts. The first part illustrates how cyberspace enabled better human security in Southeast Asia in relation to the seven key areas of human security according to the Human Development Report (HDR) 1994 (United Nations Development Programme, 1994). The second part discusses the impacts of cyber threats on human security. The third part suggests how Southeast Asian states may enhance their cybersecurity policies and posture to better protect human security. The last part will be the conclusion.

How Cyberspace Enabled a Better Human Security in Southeast Asia

The increasing integration of cyberspace into everyday life has significant implications for "human freedom and fulfilment."

This paper argues that the availability of cyberspace in Southeast Asia does preserve and enhance human well-being, aligning with the seven key areas of human security as defined by the Commission on Human Security (United Nations Development Programme, 1994). Firstly, on economic security, cyberspace such as digital platforms allows people to buy, sell, and advertise products and services. They also allow local businesses to access a worldwide customer base, therefore significantly enhancing economic opportunities. In Southeast Asia, the use of cyberspace is crucial to the regional economy, as among 460 million internet users (in 2022), 370 million users are classified as digital consumers who purchase goods and services online (Singh, 2023). This is also related to the area of food security and health security, where today access to food delivery and telehealth services are becoming more viable. Within this regard, information such as healthy diet and poisonous food are also available to enhance and preserve human security.

When it comes to environmental security, contributions from cyberspace are more complicated. The most prominent one would be that the availability of e-government services could help save paper waste and have the potential to reduce transportation costs for humans to access crucial services. The growing number of e-government services, including online applications for permits, tax filing, and access to public records within the region contribute to this aspect (United Nations Asian and Pacific Training Centre for Information and Communication Technology for Development, 2019). However, the substantial energy demands of data centres and telecommunication infrastructure also present significant environmental challenges (Valkhof, 2024). Therefore, cyberspace's contributions toward the environment are still to be determined.

For personal security and community security, the availability of online information has contributed to the safety of individuals and communities as people gain more access to information related to their safety such as severe weather predictions, pandemic warnings, or crime incidents nearby. People also tend to rely on cyberspace to keep in contact with their communities. Within Southeast Asia, as of 2024, 64.3% of the region's population has engaged in social media platforms – significantly higher than the global average ("Study: SEA Most Active Social Media Users," 2018). The same data also shows that a large portion of users have social media as their primary source for news, indicating that cyberspace is a crucial channel for both information dissemination and community connection.

Last but not least is political security. The availability of cyberspace has enhanced political engagement for people. This includes the ability for citizens to gather information regarding politics and policies, and the ability to drive political interests of diverse groups. Within Southeast Asia, social media are also a key component for several political movements, allowing people to gather and push for their political interests (Sinpeng, 2020). It is also worth mentioning that cyberspace has many contributions to human security ways beyond the examples mentioned.

The Impact of Cyber Threats on Human Security

The matching of cyber dependency and HDR's seven key areas reveals two ways in which cyberspace contributes to "human security." Firstly, it is a 'means' for a human to accomplish their human security goals. From examples in the previous part, this includes access to the market, food delivery, health services, government services, crucial information related to human safety, and political engagement. Secondly, cyberspace itself has become an element of human security, particularly within the realm of confidentiality and integrity of data and information.

Cyber Threats Create Systemic Impacts on Human Security. This essay argues that cyber threats may create a 'systemic restriction' of human security. This refers to when the availability of cyberspace, where it usually contributes to human well-being, is degraded or disrupted. This phenomenon may not obstruct human reach for their well-being, since goods, services, or information are still accessible in the physical world. Cyber threats related to this 'systemic restriction' may occur within three layers of cyberspace: **physical, logical, and human layer.**

The threats toward the **physical layer** are likely to have the widest impacts on human security. This includes any threats toward infrastructures crucial for the availability of cyberspace. Submarine cables, for example, are the most important component for the Internet – as more than 95 per cent of Internet traffic relies on these cables (Tcheyan, 2023). It also appears that these cables are vulnerable to many sources of threats from geopolitical tensions, natural hazards, or accidents by humans (Tcheyan, 2023). Any disruption on undersea cables could severely limit the internet speeds of the whole nation. This incident is also prominent within the Southeast Asia region, as in the recent case of Vietnam where three out of five submarine cables were down, causing mass internet outage ("Three Subsea Cables Go Down in Vietnam, Leading to Widespread Internet Outages," 2024).

It appears that the physical layer of cyberspace is vulnerable to many forms of threats from geopolitical tensions, natural hazards, or accidents by humans. Any damage to undersea cables could severely limit internet speeds, affecting the availability of cyberspace usage. Vietnam, for example, has had to manage multiple cable failures, causing mass internet outages, in the past two years. Systemic challenges for Southeast Asian states are that the governance of cyber infrastructure, particularly submarine cables, lies largely beyond their control. Ownership rests predominantly with private sector "hyperscalers," powerful tech giants with global reach. This dependence extends to the repair process, which depends on the availability of several repair vessels. Malaysia's recent policy shift, revoking exemptions that allowed foreign vessels to repair cables in its waters, underscores the influence of private actors in maintaining cyber infrastructure to support the expansion of the regional digital economy (Qiu, 2024).

The threats toward the **logical layer** refer to the disruption of internet protocol or computer systems. In Southeast Asia, these threats primarily stem from financially motivated criminal groups engaging in “cyber-dependent crime” (European Parliamentary Research Service, 2024), where cyberattacks facilitate criminal activities. Attacks on the government sector, such as a ransomware attack Indonesia faced in July 2024 could disrupt a wide range of government services (“Indonesia Says it Has Begun Recovering Data After Major Ransoware Attack,” 2024). Additionally, attacks on critical private sectors, such as the Vietnamese brokerage VNDirect in March 2024, can have severe consequences for individuals, potentially compromising their access to assets.

For the **human layer,** threats are the negative perceptions that hinder people from utilising cyberspace for their human security benefits. The issue of “cyber-enabled crime,” which is the human conduct of traditional crime through cyberspace such as online scams (European Parliamentary Research Service, 2024), is the focus here. The surge of online scams can erode community trust in the integrity of cyberspace usage, which may lead to a decline in trust in the digital economy in the long run. As a study shows, the rising cases of cyber fraud influence Indonesian customers to avoid e-commerce transactions (Apau and Korentang, 2019).

In dealing with these cybercrime activities, states are facing technical, legal, and political challenges. From the technical side, cybercriminals primarily hold the advantage of anonymity where they can easily hide their identity and origin of attack while the process of tracing back and “attribution” is more costly and time-consuming.

The decentralised nature of cryptocurrency also allows criminals to further avoid state detection. The lack of harmonized national cybercrime laws and timely sharing of digital evidence between countries are also legal obstacles to cybercrime investigations ("Obstacles to Cybercrime Investigations," n.d.). The case may even be more complicated when it is state-sponsored, where the host country lacks the will to cooperate.

Cyber Threats Directly Undermines Human Security. Cyberspace also serves as an "end" in itself for human security through the confidentiality and integrity of data and information. Any breach of either factor may have an undermining effect on human security. A study by WHO, for example, shows that online misinformation on health information has negatively influenced people's health behaviours – clearly undermining personal and health security (World Health Organisation, 2022). Disinformation campaigns related to politics also risk polarising societies, undermine social cohesion and trust – and negatively affect community security. The leak of personal information is also directly related to personal security as criminals may use leaked personal information for social engineering to enhance their criminal activities.

Cyber threats that undermine human security may also happen through other layers of cyberspace. For example, an attack on an operating device such as a medical device for an ICU patient, or a DDoS attack resulting in the inaccessibility of patient health data are both threats that directly undermine human health security.

Recommendations

Strengthen Human Security Elements within the National Cybersecurity Framework. As this essay illustrated, cyber threats are not purely technical and their effects on human security are inseparable. As cyber threats will always happen and incident responses for human security will be needed, nations should have their cybersecurity framework beyond securing computer systems and critical. Having human elements within the national framework can shape state apparatus to have human security within their consideration of cyber incidents. An example would be the case of Thailand, where its Cybersecurity Act 2019 includes "fatality of people," "public safety," and "protection of rights and liberties" as critical cyber threats - the highest level of threat (Cybersecurity Act, B.E. 2562, 2019). By doing so, government officials related to cybersecurity will need to evaluate the effects of cyber threats further toward human security and prepare their incident response plans outside of the cyber domain, to also reconcile any effects on human security.

Bridging Gaps Between Nations. The disparity in cyber capabilities among Southeast Asian nations presents a challenge to regional crisis response, especially when regional infrastructure such as telecommunications and finance facilities are becoming more interconnected (Hitziger and Ruf, 2021). Through capacity-building cooperation, such as the sharing of best practices, regular regional training, and developing a regional plan of action, countries can enhance their understanding of each other's capabilities and develop a common understanding of cyber incidents. This is especially crucial given the diverse cyber lexicon, including definitions, goals, and perceptions of the crisis, that still exists in the region (Ho and Ho, 2023). Harmonising cybersecurity regulations seems to be a challenging task. However, countries can start by having a clear stance on key international cybersecurity issues. Currently, Singapore is the only Southeast Asian country to have published its official position on international law in cyberspace (United Nations General Assembly, 2021). With a further release of national positions, countries in the region can identify areas of agreement and shared objectives, which serve as a valuable foundation for future harmonisation efforts, promoting greater cybersecurity cooperation across the region. The region may also follow the African Union (AU) of publishing a shared position across the region (African Union, 2023).

Building Regional Resilient. Since, October 2024, ASEAN has launched the ASEAN-CERT ("Singapore and ASEAN Member States Deepen Commitment to Enhance Collective Cybersecurity in the Region," 2024). which in the future may serve as a central point of contact for cybersecurity incidents in the region. This was already an establishment for regional resilience that allowed countries to act beyond differences in their domestic measure, especially when dealing with cyberattack threats against the logical layer. When it comes to the physical layer, regional resilience is still limited. While the 2019 ASEAN Guidelines for Strengthening Resilience and Repair of Submarine Cables represent a step towards addressing vulnerabilities in the physical layer, such as those related to submarine cables, they fall short of providing proactive security and resilience measures ("ASEAN Guidelines for Strengthening Resilience and Repair of Submarine Cables," 2019). The guidelines primarily focus on streamlining the repair process for damaged cables. To effectively enhance regional resilience, Southeast Asian nations may adopt a more proactive approach to submarine cable security such as having strong regulations for cable construction and incentivise the development of redundancy.

Support International Laws and Norms that Enhance and Protect Human Security. Despite Southeast Asia being a region without armed conflicts, the proliferation of international norms and laws will better secure the region from any spill-over effects of cyber conflicts among the rising geopolitical tensions. International norms such as the UNGGE 11 norms on responsible state behaviour in cyberspace do have the concept of human security within their design (Hanson, 2021). For example, cooperating and stopping crimes and terrorism, respecting human rights and privacy, and securing critical infrastructure, all contribute positive effects toward human security. Right now, these norms are already subscribed by ASEAN nations. Further implementation of these norms will contribute to the protection of human security within the region.

Another crucial norm is the applicability of International Humanitarian Law (IHL) within cyberspace (Gisel, et.al., 2021). This refers to the use of cyberattacks within armed conflicts, where most of the cyber infrastructures are "dual-use" between civilians and combatants, making any cyber operation may cause civilian suffering. The point of this norm is to protect civilians from unnecessary suffering, which is a crucial aspect of human security.

Conclusion

Cyberspace has become an integral part of our everyday lives, while governments face significant challenges in ensuring cybersecurity and failure to do so may have effects on human security, as this essay demonstrated. However, with proper framing, states can still preserve their significant role in this challenge. The starting point is to recognise the human cost of a cyber incident and prepare to act further than just securing computer systems. As both human security and cybersecurity are beyond the concept of territories, cooperation is always the core measure. Ultimately, a comprehensive approach that acknowledges the interconnected and multidimensional nature of cyberspace while still prioritising human security will enable states to navigate the complexities of the digital age and safeguard the well-being of their citizens.

BIBLIOGRAPHY

- African Union. “The African Union Takes Significant Steps Towards Establishing a Common African Position on the Application of International Law in Cyberspace.” 1 June 30, 2023, https://au.int/en/pressreleases/20230630/african-union-takes-significant-steps-towards-establishing-common-african.
- Apau, Richard, and Felix Nti Koranteng. "Impact of Cybercrime and Trust on the Use of E-Commerce Technologies: An Application of the Theory of Planned Behavior." International Journal of Cyber Criminology 13, no. 2 (2019): 228-54. Accessed November 22, 2024. https://www.cybercrimejournal.com/pdf/ApauKorentangVol13Issue2IJCC2019.pdf.
- Clark, David D. "Characterizing Cyberspace: Past, Present and Future." ECIR Working Paper no. 2010-3. Cambridge, MA: MIT Political Science Department, 2010. Accessed November 22, 2024. https://dspace.mit.edu/handle/1721.1/141692.
- "Cybersecurity Act, B.E. 2562 (2019)." Thailand Netizen Network. Accessed November 29, 2024. https://thainetizen.org/wp-content/uploads/2019/11/thailand-cybersecrutiy-act-2019-en.pdf.
- European Parliamentary Research Service. Cybercrime: EU Policy and Challenges. Luxembourg: European Union, 2024. Accessed November 22, 2024. https://www.europarl.europa.eu/RegData/etudes/BRIE/2024/760356/EPRS_BRI(2024)760356_EN.pdf.
- Gisel, Laurent, Tilman Rodenhäuser, and Knut Dörmann. "Twenty Years On International Humanitarian Law and the Protection of Civilians against the Effects of Cyber Operations during Armed Conflict." International Review of the Red Cross 102, no. 913 (March 2021): 287–34. https://international-review.icrc.org/sites/default/files/reviews-pdf/2021-03/ihl-and-cyber-operations-during-armed-conflicts-913.pdf.
- Hanson, Fergus. UN Norms for Responsible State Behaviour in Cyberspace: Guidance for Implementation. Canberra: Australian Strategic Policy Institute, 2021. Accessed November 22, 2024. https://www.aspi.org.au/report/un-norms-responsible-state-behaviour-cyberspace.
- Hitziger, Franziska Faul, and Matthias Ruf. "Cybersecurity Governance in Southeast Asia." DCAF, 2021. https://www.dcaf.ch/sites/default/files/publications/documents/Cybersecurity_Governance_in_Southeast_Asia_Thematic_Brief.pdf.
- Ho, Joshua, and Jia Hui Elaine Ho. "ASEAN Cyber-Security Cooperation: Towards a Regional Emergency-Response Framework." International Institute for Strategic Studies, June 2023. https://www.iiss.org/research-paper/2023/06/asean-cyber-security-cooperation-towards-a-regional-emergency-response-framework/.
- "Indonesia Says it Has Begun Recovering Data After Major Ransomware Attack." Reuters. Accessed November 22, 2024. https://www.reuters.com/technology/cybersecurity/indonesia-says-it-has-begun-recovering-data-after-major-ransomware-attack-2024-07-12/
- Kearney. The Future of the Internet in Southeast Asia. Singapore: Infocomm Media Development Authority, 2023. Accessed November 22, 2024. https://www.imda.gov.sg/-/media/imda/files/programme/special-reports-by-atxsummit-knowledge-partners/kearney.pdf.
- “Obstacles to Cybercrime Investigations.” United Nations Office of Drugs and Crime, Accessed January 24, 2025. https://sherloc.unodc.org/cld/en/education/tertiary/cybercrime/module-5/key-issues/obstacles-to-cybercrime-investigations.html.
- Sinpeng, Aim. "Aim Sinpeng on the Dynamics of Social Media in Southeast Asia." The Diplomat, December 11, 2020. Accessed November 22, 2024. https://thediplomat.com/2020/12/aim-sinpeng-on-the-dynamics-of-social-media-in-southeast-asia/.

- "Singapore and ASEAN Member States Deepen Commitment to Enhance Collective Cybersecurity in the Region." Cyber Security Agency of Singapore, October 15, 2024, https://www.csa.gov.sg/news-events/press-releases/singapore-and-asean-member-states-deepen-commitment-to-enhance-collective-cybersecurity-in-the-region.
- Singh, S. "ASEAN goes full throttle on digital transition." The ASEAN Magazine, August 14, 2023. https://theaseanmagazine.asean.org/article/asean-goes-full-throttle-on-digital-transition/.
- "Study: SEA Most Active Social Media Users." Marketing Interactive, July 11, 2018. Accessed November 22, 2024. https://www.marketing-interactive.com/study-sea-most-active-social-media-users.
- Tcheyan, Lucas. "The Weakest Link: Securing Critical Undersea Infrastructure in ASEAN." The Diplomat, June 20, 2023. Accessed November 22, 2024. https://thediplomat.com/2023/06/the-weakest-link-securing-critical-undersea-infrastructure-in-asean/.
- "Three Subsea Cables Go Down in Vietnam, Leading to Widespread Internet Outages." Data Center Dynamics, June 18, 2024. Accessed November 22, 2024. https://www.datacenterdynamics.com/en/news/three-subsea-cables-go-down-in-vietnam-leading-to-widespread-internet-outages/.
- United Nations Asian and Pacific Training Centre for Information and Communication Technology for Development. E-government strategies in Asia and the Pacific. 2019. https://www.unapcict.org/sites/default/files/2019-01/E-Government-Strategies-Asia-Pacific.PDF
- United Nations Development Programme. Human Development Report 1994. New York: Oxford University Press, 1994. Accessed November 22, 2024. https://hdr.undp.org/content/human-development-report-1994.
- United Nations General Assembly. “Official Compendium of Voluntary National Contributions on the Subject of How International Law Applies to the Use of Information and Communications Technologies by States Submitted by Participating Governmental Experts in the Group of Governmental Experts on Advancing Responsible State Behaviour in Cyberspace in the Context of International Security Established Pursuant to General Assembly Resolution 73/266.” July 13, 2021, https://front.un-arm.org/wp-content/uploads/2021/08/A-76-136-EN.pdf.
- Valkhof, Bart, Emmanuelle Kemene, & Jesse Stark. "Growing data volumes drive need for ICT energy innovation." World Economic Forum, May 22, 2024. https://www.weforum.org/agenda/2024/05/growing-data-volumes-drive-need-for-ict-energy-innovation/.
- Winston Qiu. “Malaysia Reinstates Cabotage Exemption for Subsea Cable Ships.” Submarine Cable Networks, Accessed January 24, 2024. https://www.submarinenetworks.com/en/nv/news/malaysia-reinstates-cabotage-exemption-for-subsea-cable-ships.
- World Health Organization. “Infodemics and Misinformation Negatively Affect People’s Health Behavious, New WHO Review Finds.” Accessed November 22, 2024. https://www.who.int/europe/news/item/01-09-2022-infodemics-and-misinformation-negatively-affect-people-s-health-behaviours--new-who-review-finds.
- Zojer, Gerald. "The Interconnectedness of Digitalisation and Human Security in the European High North: Cybersecurity Conceptualised through the Human Security Lens." The Yearbook of Polar Law Online (2019): 297-320. https://brill.com/view/journals/yplo/10/1/article-p297_14.xml.
- ———. "Theorising Security: A Human Security Perspective on Cybersecurity." 2019. Accessed November 22, 2024. https://lauda.ulapland.fi/bitstream/handle/10024/64113/Zojer.Gerald%20part%202.pdf?sequence=1.

TACKLING ONLINE GENDER-BASED VIOLENCE: ENSURING SAFETY AND EQUALITY IN THE DIGITAL AGE

ABSTRACT

Online Gender-Based Violence (OGBV) is an escalating concern in the digital age, particularly in the ASEAN region, where it threatens human security and perpetuates gender inequality by disproportionately targeting women and LGBTQ+ individuals. Despite the growing reliance on digital platforms, regional cybersecurity policies often fail to address the gendered dimensions of online violence. This paper explores the prevalence and impact of OGBV, identifies gaps in ASEAN's digital safety policies, and proposes actionable solutions to strengthen regional responses. Through a review of case studies, reports, and policy frameworks, this study highlights ASEAN's shortcomings in addressing digital violence. It analyzes how legal frameworks, cultural norms, and technological factors contribute to the persistence of OGBV. Additionally, the paper evaluates ASEAN's cybersecurity policies and their effectiveness in combating digital gender-based violence. Findings reveal that OGBV manifests in various forms, including cyber harassment, doxing, misinformation, and non-consensual image sharing. Many victims, particularly young women and LGBTQ+ individuals, hesitate to report incidents due to fear of social backlash or inadequate legal support. The case of Ain Husniza Saiful Nizam demonstrates the severe consequences of OGBV, including psychological distress, social isolation, and economic hardship. ASEAN's cybersecurity policies primarily focus on economic and cybercrime issues, lacking gender-specific protections. To address these issues, the essay proposes a multi-stakeholder approach, recommending regional policy enhancements, improved law enforcement, stronger collaboration with the tech industry, public awareness campaigns, and expanded victim support services. By adopting these measures, ASEAN can foster a safer digital environment and advance gender equality in the digital age.

Keywords: Online Gender-Based Violence; Cybersecurity; ASEAN, Digital Safety; Human Security

AUTHOR:

JUDELIO DA SILVA BARROS BARRETO

(TIMOR-LESTE)

In today's technological era, women and LGBT+ people have access to many opportunities, but at the same time they are also often become victims in the online world. Online Gender-Based Violence (OGBV) is a pressing global issue, and its impact is particularly significant in ASEAN countries, where it present a serious threat to human security. The high number of victims and the lack of public awareness about OGBV makes it even more urgent to deal with this issue. By involving all societal stakeholders from government to community based, this problem can be effectively tackled, especially in the ASEAN region. This essay opens with a definition of online gender-based violence (OGBV), explores its various forms and prevalence, and examines its effects on human security. It will also connect these points to cybersecurity in the ASEAN region and provide some practical ideas for improvement. OGBV refers to harmful actions executed via digital platforms primarily on social media, targeting individuals based on gender identity, sexual orientation, or gender norms (Amnesty International, n.d.). Most often, women and the LGBTQ+ community are targeted, but men can be victims too, although less frequently reported. According to UN Women, 85% of women online have witnessed OGBV, and 38% have been direct targets (UN Women, n.d.). Vulnerable groups, such as young women in the LGBTQ+ community, are particularly affected, with 15% of lesbian girls and 12% of bisexual girls aged 15-17 experiencing cyber-harassment in the past year (International Committee of the Red Cross, 2024).

OGBV thrives on power imbalances and societal norms that reinforce gender discrimination. The internet's anonymity and vast reach give perpetrators the means to harm others without facing immediate consequences. This makes OGBV particularly challenging, as its impact goes beyond individual victims, disrupting the broader societal framework. OGBV manifests in various forms, including misinformation and defamation (67%), cyber harassment (66%), hate speech (65%), impersonation (63%), hacking and stalking (63%), coordinated efforts to spread harmful content (58%), abuse involving videos or images (57%), doxing (55%), violent threats (52%), and unsolicited sexually explicit content (43%) (UN Women, n.d.). These statistics show how widespread OGBV is and its severe consequences for victims' security and peace of mind. Each form of online gender based violence (OGBV) has different characteristics but shares common effects of instilling fear, eroding self-esteem, and limiting victims' online and offline activities. Misinformation and defamation can damage personal and professional reputations, while hacking and stalking invade privacy and create a sense of vulnerability. The dissemination of explicit content without consent, often referred to as "revenge porn," is particularly devastating, as it combines humiliation with long-term social stigma.

In the ASEAN region, the increasing use of the internet has been accompanied by a rise in cases of OGBV. Children and adolescent girls, especially those between the ages of 10 and 18, are among the most vulnerable. Many of these incidents occur on social media and instant messaging platforms, where victims frequently encounter anonymous sexual comments, pressure to share explicit material, and harassment that often relates to local culture (OGBV Report, n.d.). Most teenagers lack an understanding of media literacy, which often makes them targets of online harassment. Even if they want to report such incidents, they are reluctance because they don't know where and how to report or seek for help. So they choose to stay silent due to embarrassment. In some cases, they are not even aware that they are experiencing OGVB due to the lack of information. As a result, cases like these persist, with victims remaining quiet and perpetrators continuing to roam freely, looking for new targets.

Cultural and social factors in ASEAN further compound the problem. Traditional gender roles and societal expectations often discourage victims from speaking out, fearing victim-blaming or social ostracization. For example, in more conservative communities, women and LGBTQ+ individuals who experience OGBV may face additional scrutiny for their experiences, with their character or lifestyle called into question. This creates a culture where silence is common and attackers feel safe.

OGBV deeply affects various aspects of human security:

- Physical Security: Threats of violence or doxing can escalate into real-life harm, such as stalking or physical attacks.
- Mental Health: Victims often suffer from anxiety, depression, or post-traumatic stress disorder (PTSD). More than half of women have reported mental health issues stemming from OGBV, with transgender individuals facing even greater risks (Council of Europe, n.d.).
- Economic Security: Victims can push victim to withdraw from online platforms which essential for career or business growth. Public figures and journalists may self-censor or leave their professions to avoid abuse.
- Social Participation: OGBV erodes freedom of expression and community engagement. Nearly 60% of young women and girls report reducing their online activity due to harassment (UN Women, n.d.).

The effects of online gender-based violence are wide-ranging and can be extremely severe. It is not uncommon for such incidents to lead to cases of suicide, physical assaults, or even murder. The rapid spread of information online, particularly explicit content, has made it easier for individuals to face attacks and judgment both virtually and in their everyday lives.

Moreover, OGBV slow down progress in society, making victims feel lonely and powerless. Many of them withdraw from public discussions, career opportunities, or community activities, reducing their ability to contribute and reinforces cycles of inequality and marginalization. Despite the rising problem of OGBV, ASEAN's cybersecurity frameworks remain inadequate in addressing this issue. While initiatives such as the ASEAN Framework on Digital Data Governance aim to enhance regional cybersecurity, they often lack gender-specific considerations. Existing laws and frameworks fail to explicitly tackle online harassment, leaving gaps in the protection of women and LGBTQ+ individuals. For instance, the absence of comprehensive digital safety legislation in many ASEAN countries hinders the prosecution of perpetrators and the enforcement of penalties.

Furthermore, ASEAN's regional cybersecurity policies, such as the ASEAN Cybersecurity Cooperation Strategy, primarily focus on cybercrime and digital economy issues, but overlook the gendered dimensions of digital security. This gap makes it difficult to protect vulnerable people and groups from OGBV. The case of Ain Husniza Saiful Nizam from Malaysia illustrates these gaps. Ain faced significant cyber harassment after exposing inappropriate comments made by her teacher. This led to widespread online bullying, including threats of violence and rape, which caused her significant emotional stress and negatively affected her mental health. The backlash extended beyond Ain, affecting her family, who faced social rejection. Her father also experienced professional difficulties, adding economic strain to the situation. Her case highlights the intersection of physical, psychological, and economic consequences of OGBV and underscores the need for robust legal and institutional responses (Al Jazeera, n.d.).

Recommendations

The absence of a unified strategy to tackle OGBV across ASEAN creates significant gaps in protecting victims and responding to incidents. While some countries have made progress by introducing digital safety regulations, others lag behind, leading to an uneven framework that weakens regional cooperation and enforcement efforts.

To effectively combat OGBV, ASEAN must adopt a comprehensive, collaborative approach involving governments, tech companies, and civil society:

1. **Strengthen Regional Policies:**
   - Integrate gender-specific measures into the ASEAN Framework on Digital Data Governance.
   - Develop regional legislation addressing OGBV, ensuring harmonized laws across ember states.
   - Align national cybersecurity strategies with the principles of the Convention on the Elimination of All Forms of Discrimination Against Women (CEDAW).
2. **Enhance Law Enforcement:**
   - Train law enforcement to handle OGBV cases with sensitivity.
   - Establish specialized cybercrime units to investigate and prosecute OGBV.
   - Promote cross-border collaboration to address transnational cyber harassment.
3. **Collaborate with Tech Companies:**
   - Require social media platforms to implement stricter content moderation policies.
   - Develop user-friendly reporting tools and faster mechanisms for removing harmful content.
   - Ensure transparency in how abuse complaints are handled.
4. **Promote Public Awareness and Digital Literacy:**
   - Launch campaigns to educate citizens about OGBV and reporting mechanisms.
   - Incorporate digital literacy programs into school curriculums, focusing on online safety and respectful behavior.
   - Create online resources to help users identify and combat OGBV.
5. **Support Victims:**
   - Provide anonymous reporting channels and offer psychological, legal, and social support.
   - Encourage youth-led initiatives to promote a culture of online respect.
   - Partner with NGOs to create safe spaces for survivors to share experiences and access help.

These recommendations emphasize the importance of a comprehensive and collaborative approach. Governments must create and enforce laws, tech companies must ensure safe digital environments, and civil society must advocate for change and support victims.

OGBV is a pervasive issue that threatens the well-being and security of women and LGBTQ+ individuals in ASEAN. While digital platforms have amplified these risks, they also offer opportunities for intervention. By adopting gender-sensitive policies, fostering collaboration between governments, tech platforms, and civil society, and raising public awareness, ASEAN can create a safer digital environment. Addressing OGBV is essential not only for protecting human security but also for building a more inclusive and resilient society. With coordinated efforts, ASEAN can set a global example for combating online abuse and ensuring secure digital spaces for all.

BIBLIOGRAPHY

- Amnesty International. (n.d.). What we do: Online violence. Retrieved from https://www.amnesty.org/en/what-we-do/technology/online-violence/
- UN Women. (n.d.). FAQs: Trolling, stalking, doxing, and other forms of violence against women in the digital age. Retrieved from https://www.unwomen.org/en/articles/faqs/faqs-trolling-stalking-doxing-and-other-forms-of-violence-against-women-in-the-digital-age
- International Committee of the Red Cross (ICRC). (2024, January 4). Online violence and its real-life impacts on women and girls in humanitarian settings. Retrieved from https://blogs.icrc.org/law-and-policy/2024/01/04/online-violence-real-life-impacts-women-girls-humanitarian-settings/
- UN Women. (n.d.). FAQs: Trolling, stalking, doxing, and other forms of violence against women in the digital age. Retrieved from https://www.unwomen.org/en/articles/faqs/faqs-trolling-stalking-doxing-and-other-forms-of-violence-against-women-in-the-digital-age
- OGBV Report. (n.d.). Understanding Online Gender-Based Violence. (p. 8).
- UN Women. (n.d.). FAQs: Trolling, stalking, doxing, and other forms of violence against women in the digital age. Retrieved from https://www.unwomen.org/en/articles/faqs/faqs-trolling-stalking-doxing-and-other-forms-of-violence-against-women-in-the-digital-age
- Council of Europe. (n.d.). Cyberviolence against women. Retrieved from https://www.coe.int/en/web/cyberviolence/cyberviolence-against-women
- UN Women. (n.d.). FAQs: Trolling, stalking, doxing, and other forms of violence against women in the digital age. Retrieved from https://www.unwomen.org/en/articles/faqs/faqs-trolling-stalking-doxing-and-other-forms-of-violence-against-women-in-the-digital-age
- Al Jazeera. (n.d.). The 17-year-old exposing rape culture in Malaysian schools. Retrieved from https://www.aljazeera.com/news/2024/1/4/the-17-year-old-exposing-rape-culture-in-malaysian-schools
- Statista. (n.d.). Perceived digital literacy of youth in ASEAN by gender. Retrieved from https://www.statista.com/statistics/1247962/asean-perceived-digital-literacy-of-youth-by-gender/
- Amnesty International Philippines. (n.d.). Digital disruptors. Retrieved from https://www.amnesty.org.ph/digital-disruptors/

#CyberPeacebuilding

ASEAN Institute for Peace and Reconciliation (ASEAN-IPR)

https://asean-aipr.org/
asean_ipr
@ASEAN_IPR
ASEAN Institute for Peace and Reconciliation
ASEAN Institute for Peace and Reconciliation
ASEAN IPR

ASEAN-Republic of Korea Cooperation Fund (AKCF)

https://www.aseanrokfund.com/
@akcf_pmt