ERIA Discussion Paper Series

No. 465

Gender Security and Safety in the ASEAN Digital Economy[12]

Araba SEY
Principal Research Scientist, University of Washington Information School

December 2022

Abstract: *Gender-based cyber violence inhibits progress towards gender digital equality by discouraging women from participating in the digital economy. From the magnitude of the problem to its economic and social impacts, much remains to be understood about how women experience safety and security in the Association of Southeast Asian Nations (ASEAN) digital economy. Drawing on academic and grey literature, this paper reflects on the implications of gender-based cyber violence for digital equality and economic development. Overall, data are lacking on the prevalence, economic costs, and social impacts of gender-based cyber violence within ASEAN. Policy tends to focus more on measuring domestic and intimate partner violence, likely due to its designation as the main indicator for Sustainable Development Goal 5. Although a variety of national, regional, and global frameworks exist to address different dimensions of violence against women, cybersecurity, and workplace harassment, more work is needed to identify the scale and scope of gender-based cyber violence in the region, in order to target policy appropriately.*

Keywords: Cyber violence; Cybersecurity; Digital economy; Economic costs; Gender, women; ASEAN

JEL Classification: O53, J16; J18; J7; L86

[1] Preparation of the paper was supervised by Giulia Ajmone Marsan, director, Strategy and Partnership, Economic Research Institute for ASEAN and East Asia (ERIA). Gratitude is also extended to Dilini Wijeweera for assisting with background research.

[2] This paper is supported by the Economic Research Institute for ASEAN and East Asia (ERIA) and the Government of Australia through the Department of Foreign Affairs and Trade. The views expressed in this publication are the author's alone and are not necessarily the views of ERIA or the Government of Australia.

1. Introduction

> … the ASEAN region is not the same as it was when the ASEAN RPA-EVAW[3] was adopted. The socio-economic and political realities faced by women and girls are changing. While various forms of violence persist, emerging forms of abuses are coming into fore. This includes … abuses in the cyber space, and violence that specifically targets women and girls (ASEAN Committee on Women, 2021: 6).

The Istanbul Convention[4] defined violence against women as 'all acts of gender-based violence that result in, or are likely to result in, physical, sexual, psychological or economic harm or suffering to women, including threats of such acts, coercion or arbitrary deprivation of liberty, whether occurring in public or in private life' (Council of Europe, 2011: 3). This definition could be revised to add 'whether online or offline', as violence against women increasingly occurs in cyberspace or has a digital technology component, reproducing other forms of gender-based violence. This type of violence is commonly termed online violence against women or gender-based cyberviolence, amongst other names, and is defined as 'any act of gender-based violence against women that is committed, assisted or aggravated in part or fully by the use of ICT, such as mobile phones and smartphones, the Internet, social media platforms or email, against a woman because she is a woman, or affects women disproportionately' (Simonovic et al., 2018: 7). Cyber violence goes by different names (e.g. online violence, technology-facilitated violence) and takes a variety of forms (e.g. bullying, stalking, defamation, doxing, image-based abuse, sexual harassment, trolling, hacking).[5]

Gender-based cyber violence, as well as offline violence against women in the digital economy, inhibits progress towards gender digital equality. It discourages women from participating in the digital economy or slows down their progress significantly. However, it tends to be a largely unexamined topic in discussions of digital inclusion and diversity in the Association of Southeast Asian Nations (ASEAN) region,

[3] ASEAN Regional Plan of Action on the Elimination of Violence against Women (ASEAN, 2015).
[4] Council of Europe Convention on Preventing and Combating Violence Against Women and Domestic Violence (Council of Europe, 2011).
[5] This paper uses the term to refer to this phenomenon in all its forms.

and relatively little attention has been paid to cyber safety issues that affect women's participation in the digital economy. Drawing on academic and grey literature, this paper reflects on the implications for ASEAN of gender-related insecurities associated with the digital economy. From the magnitude of gender-based cyber violence, to the economic and social impacts, much remains to be understood about how cybersecurity, safety, and violence affect women's ability to function as digital professionals and entrepreneurs. Several initiatives are under way to promote gender digital equality in the ASEAN region – but for these initiatives to be successful, concerted efforts are needed to address unintended outcomes such as increased exposure to gender-based cyber violence as well as intentional actions by actors seeking to limit women's visibility in the digital economy.

2. Prevalence of Gender-Based Cyber Violence in the ASEAN Region

Being the target of cyber violence is not unique to females – more than 50% of both males and females in a global study by the World Wide Web Foundation and World Association of Girl Guides and Girl Scouts (2020) said they had experienced abuse or violence online. However, gender-based cyber violence disproportionately targets women, while the type of cyber violence that males encounter is less likely to be based on gender (Hicks, 2021), although it may occur in the context of their sexual identity.

Although there is a general lack of disaggregated data on the prevalence of gender-based cyber and technology-facilitated violence (Fraser and Martineau-Searle, 2018; Posetti et al., 2021), a study of 50 countries estimated that globally, 38% of adult women aged 18–74 had experienced online violence personally and 65% knew other women who had experienced online violence (Economist Intelligence Unit, 2021). The overall prevalence rate for Asia-Pacific was 88%, the fourth highest of six regions – the Middle East had the highest prevalence at 98% and Europe the lowest at 74%. The study also found that only a quarter of women had reported incidences to the platform on which it occurred and 14% to an offline agency. Other studies have found similarly high

prevalence levels (see Hicks (2021) for more examples). According to Lomba, Navarra, and Fernandes (2021), 4%–7% of women in the 27 member countries of the European Union (EU 27) have experienced cyber harassment in the last 12 months. Pew Research estimated that in the United States (US), the percentage of women who have experienced online harassment doubled from 8% in 2017 to 16% in 2021 (Hicks, 2021).

High levels of gender-based cyberviolence have also been documented in several ASEAN Member States (AMS) including Malaysia, Thailand, and Viet Nam (NORC at the University of Chicago and the International Center for Research on Women, 2022a), although prevalence rates are mostly available for cyberbullying amongst the youth. Research by UN Women rated Malaysia and the Philippines as having some of the worst scores for several types of gender-based cyberviolence (Timur, 2022). In Malaysia, a survey by the Malaysian Centre for Constitutionalism and Human Rights in 2018 found that women were sexually harassed online at least twice as often as men (Aziz and Hassanein, 2020).

Furthermore, during the coronavirus disease (COVID-19) pandemic, there were dramatic increases in gender-based cyber violence as well as online misogyny and hate speech targeted at women, almost certainly a direct result of more people – male and female – being online. For instance, in Indonesia, the National Commission on Violence Against Women recorded more than triple the number of reports of cyber violence in 2020 compared with 2019 (NORC at the University of Chicago and the International Center for Research on Women, 2022b). The Southeast Asia Freedom of Expression Network (SAFEnet) saw a jump of almost 400% in complaints about the sharing of non-consensual intimate content (SAFEnet, 2021).

Emerging trends in cybersecurity also present gender-related risks that are not fully accounted for in cybersecurity mechanisms. The development and spread of new high-speed communication devices – coupled with the Internet of Things, the expansion of cloud storage services, and the shift towards remote work during the COVID-19 pandemic – have created opportunities for more intrusive cyberattacks and data breaches that could have severe consequences for women. Cybersecurity is a serious concern in ASEAN, but discussions rarely consider gender dimensions such as the fact that data

breaches and doxing enable specific genders to be identified and targeted (Timur, 2022). This is exacerbated by the low representation of women in cybersecurity jobs, potentially contributing to inadequate provision for gender-sensitive cybersecurity tools and practices (Timur, 2022). Gender analysis is therefore important to incorporate the possibility for women and other genders to be disproportionately affected by cybersecurity events, and to design security products with alternative values to the typical technical and militaristic approaches (see Millar, Shires, and Tropina (2021) for an example of a gender lens cybersecurity framework).

At the policy level, there is greater focus on measuring and addressing domestic and intimate partner violence, likely due to its designation as the main indicator for Sustainable Development Goal (SDG) 5 Target 5.1 (End all forms of violence against all women and girls in the public and private spheres, including trafficking and sexual and other types of exploitation).[6] When cyber aspects are considered, they relate largely to human trafficking and cyberbullying (mostly amongst students). While workplace gender-based violence is recognised and being addressed (see Cruz and Klinger (2011), for example), relatively little targeted attention goes to work-related cyber violence, such as that faced by professional women in employment and entrepreneurship in the digital economy. However, countries such as the Philippines are beginning to adopt more expansive definitions of gender-based violence that include online spaces (Box 1).

[6] The two indicators for this SDG target measure the proportion of women and girls subjected to violence by an intimate partner or a person other than an intimate partner.

Box 1: Safe Spaces Act, 2019 – the Philippines

The Safe Spaces Act, passed in 2019, updates the policy definition of the sites in which people are to be protected from gender-based sexual harassment. Section 2 of the act acknowledges the right to safety and security 'not only in private, but also on the streets, public spaces, online, workplaces and educational and training institutions' (Section 2). Article II of the act is devoted to the online dimension – it defines gender-based online sexual harassment, identifies implementing bodies for the issue, and outlines penalties for violations of the policy. Article IV on workplace harassment categorises acts as sexual harassment 'whether done verbally, physically or through the use of technology such as text messaging or electronic mail or through any other forms of information and communication systems' (Section 16a)

Source: Republic of the Philippines (2018).

Online harassment in professional contexts or for career-related reasons is a particularly serious risk for women who aspire to leadership roles within the digital economy and in public life in general. This is evident in the numerous incidents of cyber violence against women journalists and politicians in particular (e.g. Aziz and Hassanein, 2020; Hicks, 2021; Plan International, 2020; Tech Policy Design Lab, 2021). Less publicly visible women (in the gig economy, for instance) also often have to endure both the risk of and actual cyber violence in the daily course of their duties without appropriate measures in place to protect them or avenues for recourse (e.g. Athreya, 2021; Kasliwal, 2020).

3. Implications for Women's Participation in the Digital Economy

> 'This absence of security online hinders women's participation in the public sphere, governance and leadership roles' (UN Women, n.d.: 5).

The increase in cyber violence against women during the COVID-19 pandemic demonstrates that increased digital access results in increased exposure to cyber violence. This means that as ASEAN progresses with its regional agenda to accelerate women's participation in the digital economy through increased digital access, the risk of cyberviolence against women will increase in parallel, unless appropriate mechanisms are put in place for social and institutional change. Within the realm of cybersecurity, data breaches may not specifically target women but do have gendered safety implications. Because some of the most egregious forms of gender-based cyber violence thrive on exposing people's personal information, cybersecurity events can have serious consequences for women whose information is stolen. Participating in the digital economy makes women's data vulnerable and this can be exacerbated if they are coming online with outdated devices and operating systems, limited knowledge of data risks, and cybersecurity systems that do not account for gendered risks.

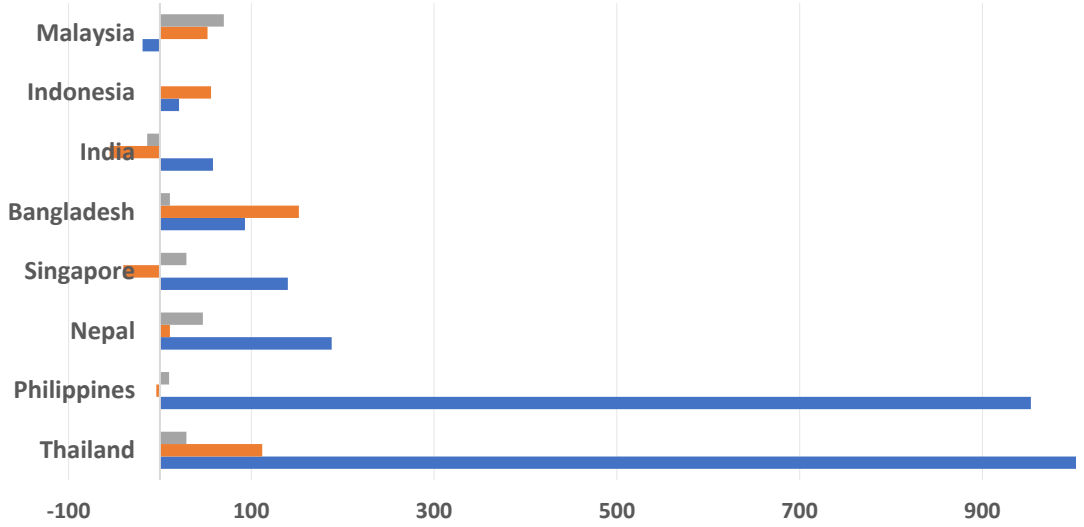
According to Hicks (2021: 2), the underlying drivers of online gender-based violence highlight 'an overarching theme of power and control, and heteronormative expectations around gender roles and sexual practice.' This observation is especially pertinent for women's participation in the digital economy as leaders and activists, since women in the public eye are particularly susceptible to online attacks. Irrespective of public policy against gender discrimination, in most cultures, visible demonstrations of achievement or power by women are looked upon less favourably than the same for men, and often lead to attempts to subdue, silence, or punish them for transgressing gender norms. This constitutes a serious barrier to women's participation in the digital economy, as such attacks tend to have a chilling effect in which women may reduce their use of online platforms, withdraw from public debate, become reluctant to take on leadership positions, and self-censor in order to prevent or escape cyber violence directed at them (Economist Intelligence Unit, 2021). Women might also hide their

identities, where possible, to avoid being singled out for attack, thereby depriving society of awareness of potential role models to promote a more diverse digital economy.

Where they have limited choices, women may choose to tolerate cyber violence for fear of repercussions such as losing their job. This is often the case with women working in the gig economy. Not only does this compromise their quality of life, but it also affects productivity (Lomba, Navarra, and Fernandes, 2021), not to mention signalling to perpetrators that their actions are acceptable. An atmosphere of gender-based cyber violence causes job insecurity for women and can limit their access to employment opportunities, for example if their reputation is damaged by attackers.

Digital technologies present a double-edged challenge because alongside being the source of cyber violence, they can enable women to participate online anonymously – thereby reducing the chances of facing gender-based cyberviolence. Digital technologies are also perceived and in fact used as a resource for support and information when targeted (Economist Intelligence Unit, 2021; UN Women, UNFPA, and Quilt.ai, 2021). As demonstrated in Figure 1, in some AMS, this attribute of digital technologies was significant during the early years of the COVID-19 pandemic. In the AMS covered in the study, all except Indonesia saw an increase in internet searches using help-seeking keywords. However, in most cases this was not in proportion to the much higher rate of increase in misogynistic language.

Figure 1: Change in Indicators of Online Misogyny, Support for Victims of Violence, and Search for Help Online



	Thailand	Philippines	Nepal	Singapore	Bangladesh	India	Indonesia	Malaysia
% change in average search volume for help-seeking keywords	29	10	47	29	11	-14	-1	70
% increase in tweets with references to support for victims of violence	112	-4	11	-40	152	-55	56	52
% increase in number of tweets with misogynistic language	22384	953	188	140	93	58	21	-19

Source: UN Women, UNFPA, and Quilt.ai (2021: 7–10).

4. The Business/Economic Case for Eliminating Gender-Based Cyber Violence

Gender-based violence is not only a problem for women and their families or for social goals; it has harmful economic implications for industry and national economies. There is growing interest in estimating the costs of gender-based violence in general and gender-based cyber violence specifically. It is believed that the costs are enormous in monetary terms and in impacts on sustainable development agendas (e.g. ESCWA, 2019; Hicks, 2021; Khumalo, Msimang, and Bollbach, 2014).

The World Bank (2019) estimated that in some countries, violence against women costs up to 3.7% of gross domestic product (GDP). Measuring the cost of gender-based cyber violence will provide advocacy tools to raise awareness and stimulate action within government and industry about the financial costs of inaction as well as the potential gains from policy action and resource allocation to address the problem. There are already instances of such cost estimates driving policy and industry action on domestic violence in Viet Nam, Peru, and Egypt (ESCWA, 2019).

It is difficult to measure the costs of gender-based violence, and some of its aspects cannot be quantified. Nevertheless, various types of costs have been identified. They include costs to the individual, family, community, industry, service providers, and nations. Costs may be direct, such as medical fees incurred by a survivor, or indirect, such as a reduction in productivity due to injury. Other types of costs that have been quantified are lost income, job loss, loss of employment opportunities, legal fees, incarceration, mediation costs, and shelter costs.

Few countries have undertaken exercises to estimate the cost of gender-based cyber violence, but two examples cover Australia and the European Union.

Australia – A 2018 survey (The Australian Institute, 2019) estimated the cost of online harassment and cyberhate, and concluded that in aggregate over the years:

- Total medical and lost income had cost Australians A$330million conservatively and could be as high as A$3.7billion
- Lost income at the lower end was estimated to be A$267million
- Medical costs at the lower end were estimated to be A$62million

European Union – A study drawing on data from 2012 and 2019 as well as other information sources (Lomba, Navarra, and Fernandes, 2021) calculated the cost of online gender-based violence (harassment and stalking) and concluded the following:

- Online gender-based violence cost the EU €49 billion–€89 billion per year
- About half of this amount (€28 billion–€53 billion) was quality of life related, followed by labour market costs (€4 billion–€6 billion) and medical and legal costs (€4 billion–€8 billion)
- These costs could fall by 6%–12% if nations accede to the Istanbul Convention or similar agreements
- These costs could decrease by 5%–15% if an EU directive on gender-based cyberviolence is established
- These costs could reduce by 15%–24% if the EU collaborates with tech companies on illegal hate speech
- A combination of legislative and non-legislative measures would yield the greatest cost reductions

5. National Actions on Gender-Based Cyber Violence

Within AMS, few countries are explicitly implementing measures targeting gender-based cyber violence. Apart from the Philippines and Singapore, whose policies spell out that online spaces are subject to anti-discrimination or violence legislation, the policy and legislative provisions of countries in the region mostly conceptualise violence in domestic settings and occasionally in public and workplace settings as well (Table 1).

Table 1: Existence of Legislation and Actions Related to Gender-Based Violence

Country	Domestic violence laws	Sexual harassment laws	Includes cyber violence	Implementing actions targeting social norms
Brunei Darussalam	-	Yes	-	Yes
Cambodia	Yes, 2005	Yes, workplace	-	Yes
Indonesia	Yes, 2004	-	-	Yes
Lao PDR	Yes, 2015	-	-	Yes
Malaysia	Yes, 1994	Yes, under amendment, 2021	-	Yes, via building capacity of stakeholder institutions
Myanmar	-	-	-	Yes
Philippines	Yes, two in 2004/2010	Yes, including public spaces, 2019	National Safe Spaces Act, 2019 includes online spaces	Yes
Singapore	Yes, several, latest in 2018	Yes	Protection from Harassment Act, 2014 criminalises sexual offences committed online	Yes, including via building capacity of stakeholder institutions
Thailand	Yes, 2007	Yes, including academic and public settings, 2018	-	Yes
Viet Nam	Yes, 2007	Yes, including workplace, 2020	-	Yes

Source: Belen (2021).

At the regional level, the ASEAN Regional Guidelines on Violence against Women and Girls Data Collection and Use (Haarr, 2018) included a recommendation

to regularly update record-keeping systems to reflect new trends such as gender-based cyber violence.

Various authors have proposed solutions and strategies, including enacting national and regional policy, establishing legal and regulatory measures, developing or improving services to support survivors, public education, industry/organisational change, collaboration amongst public and private sector stakeholders, and deepening knowledge through research and data. Evidence to date suggests that some of these actions have or are being enforced, but with limited observable results so far. This could be due to policy, implementation, or management problems.[7]

Policy problems: Within and beyond AMS, the slow progress towards eliminating gender-based cyber violence can be partly attributed to policy problems – i.e. either no relevant policies are in place or the existing policies are inadequate. As already noted, most AMS do not have gender-based cyber violence specific policies. Existing laws are outdated, disjointed, or lack clear definitions (NORC at the University of Chicago and the International Center for Research on Women, 2022a). Some also criminalise cyber violence in ways that either result in prosecution rather than protection of victims, or are perceived as detrimental to free speech (Aziz and Hassanein, 2020; NORC at the University of Chicago and the International Center for Research on Women, 2022a). The prioritisation of specific types of online violence, such as human trafficking and cyberbullying, while important, also creates blind spots regarding other prevalent types.

Implementation problems: Implementation problems relate to how existing policies are being implemented. There is a general sense that current policies that could apply to gender-based cyber violence are not being fully or effectively implemented. For example, potentially effective arenas such as schools and workplaces are underutilised in implementation plans or lack the appropriate mechanisms to enforce strategies (NORC at the University of Chicago and the International Center for Research on Women, 2022a); platform reporting mechanisms are cumbersome, opaque, not

[7] As elaborated by Blume (n.d.), distinguishing between policy, implementation and management problems can enable more efficient policymaking.

trusted by users, and often unable to monitor content in Asian languages (NORC at the University of Chicago and the International Center for Research on Women, 2022a; Tech Policy Design Lab, 2021; Timur, 2022); and agencies lack the capacity for effective enforcement of policies (Belen, 2021; Vitis, 2021).

Management problems: Management problems occur when the desired policy outcomes are prevented by external factors such as social or religious beliefs. Indeed, social norms hamper the ability and/or desire of victims to report their experience of gender-based cyber violence to family members or other potential support systems within their community (Belen, 2021; NORC at the University of Chicago and the International Center for Research on Women, 2022a). Notably, all AMS appear to recognise the key role of social norms in sustaining gender-based violence and are implementing actions to address this (Table 1), but it may be too early to see results.

6. Regional and Global Frameworks and Partnerships Against Gender-Based Violence, Cyber Violence, and Cybercrimes

At the global and regional levels, a variety of initiatives address gender-based violence, cyber violence, and cybercrimes (e.g. Box 2). Few of them adequately consider the combined category of gender-based cyber violence. However, having already established some important characteristics of the problems in their focal areas, they could be updated to build in measures that more directly address either the gendered or cyber dimensions as applicable.

Box 2: ASEAN HeForShe Campaign

Even if formed for economic purposes, regional bodies can play an important role in garnering cross-national support on social issues.

ASEAN has made significant progress in raising the profile of EVAW in the region. In partnership with UN Women, it launched the ASEAN HeForShe Campaign on 30 November 2017 in conjunction with the 16 Days of Activism

against Gender-Based Violence (16 Days). The launch aimed to raise awareness on gender equality in the region by encouraging men and boys to be agents of change, to promote a culture of respect for women and girls and to recognize how men and boys can benefit from gender equality and a region free from violence against women.

ASEAN = Association of Southeast Asian Nations, EVAW = elimination of violence against women.
Source: Belen (2021: 19).

(i) **Budapest Convention, 2004:** Also known as the Convention on Cybercrime, this was the first international treaty to target cybercrime. It aims to do so by 'providing for the criminalisation of such conduct, as described in this Convention, and the adoption of powers sufficient for effectively combating such criminal offences, by facilitating their detection, investigation and prosecution at both the domestic and international levels and by providing arrangements for fast and reliable international co-operation.' It does not cover gender-based cybercrimes. It has been ratified by 67 countries including the Philippines (Council of Europe, 2001).

(ii) **Istanbul Convention, 2011:** This is a human rights treaty intended to combat all forms of violence against women. Signatories are expected to promote gender equality and enforce legislative and non-legislative measures to protect women from violence. It does not cover cyber violence. The treaty has been ratified by 33 countries, none of them AMS. It is currently facing political challenges with the recent withdrawal of Turkey from the treaty (Council of Europe, 2011).

(iii) **Global Partnership for Action on Gender-Based Online Harassment and Abuse, 2022:** This partnership aims to gather national, international, civil society, and private sector stakeholders to 'better prioritize, understand, prevent, and address the growing scourge of technology-facilitated gender-based violence'. Its three strategic objectives are to develop and advance shared principles, increase targeted programming and resources, and expand the collection of and access to

reliable data. Partners (listed as the Australia, Canada, Chile, Denmark, New Zealand, Republic of Korea, Sweden, United Kingdom, and US) are expected to commit to supporting these objectives within their spheres of influence. Concrete results are expected by the end of 2022 (US Department of State, 2022).

(iv) **Generation Equality Action Coalition on Technology and Innovation, 2021:** An arm of UN Women's Generation Equality initiative, this coalition has made the issue of cyber violence against women one of its priorities, with the aim of seeing results by 2026. It proposes that governments and tech companies design better tools for preventing, monitoring, and responding to gender-based cyber violence, improve legislation and enforcement systems, and promote cultural change to address the problem. Generation Equality also has a separate action coalition on gender-based violence that does not specifically identify cyber violence as an area of focus (Generation Equality, 2021).

(v) **ILO Convention on Violence and Harassment, 2019:** More directly focused on the workplace, this convention highlights gender-based violence in its definition of violence and harassment 'in the world of work'. It seeks to protect people in the world of work from violence and harassment occurring in a variety of work-related contexts, including technology-facilitated work-related communications. Significantly, it also recognises domestic violence as having work implications, and the guide to the convention notes several countries that are already building provisions against gender-based cyber violence into their workplace policies (ILO, 2019, 2021).

(vi) **Declaration on the Elimination of Violence Against Women in the ASEAN Region, 2004:** This declaration commits to eliminating all forms of violence and discrimination against women through legislation, support for survivors, social change, and collaboration with public and private sector institutions. The associated ASEAN Regional Plan of Action on the Elimination of Violence Against Women specifies violence that uses information and communication technology as falling within its remit (ASEAN, 2004, 2015).

(vii) **ASEAN Declaration to Combat Cybercrime, 2017:** This declaration proposes regional cooperation to combat cybercrime through awareness raising, harmonisation of laws, and technical assistance, amongst other things (ASEAN, 2017a).

(viii) **Joint Statement on Promoting Women, Peace and Security in ASEAN, 2017:** In furtherance of peacebuilding efforts in the Region, AMS committed to gender equality, integration of gender perspectives in peacebuilding strategies, and programmes to protect women from gender-based violence in armed conflict environments (ASEAN, 2017b). Regional agendas for women, peace, and security are also opportunities to integrate measures against gender-based cyberviolence (Sharland et al., 2021).

7. Conclusion and Recommendations

Gender-based cyber violence inhibits women's full and free participation in the digital economy, especially in digital leadership. It has tangible and intangible impacts on women, families and society, and the national economy. In addition, gender-based cyber violence has tangible economic costs to business entities and the national economy. Existing research suggests that there are high levels of different types of gender-based cyber violence in some AMS. However, there are insufficient data to determine the extent to which such violence is a deterrent to women's participation in the digital economy in AMS.

There is a variety of global, regional, and national initiatives on gender, gender-based violence, cybersecurity, and labour practices that individually address separate components relevant to gender-based cyber violence. They provide a starting point to develop comprehensive strategies that capture the evolving phenomenon of gender-based cyber violence, while aiming to eliminate gender-based violence in all its forms.

Unchecked, gender-based cyber violence will curtail ASEAN goals regarding women's participation in the digital economy. Conversely, if effectively addressed, nations can reap the economic benefits of women's participation in the digital economy

in addition to avoiding the economic costs of gender-based cyber violence. As an initial step, the following actions are recommended for policymakers:

- **Integrate different dimensions of gender-based violence**: Expand the definition of gender-based violence in regional treaties to include cyber and technology-facilitated violence, and assess the gender dimensions of cybersecurity issues within such treaties. Recognise the relevance of gender-based violence that occurs outside traditional workplaces, as might be the case with home-based gig economy workers, for example. Such recognition opens the door to integrating policies against cyber violence into frameworks on gender-based violence in general and in the digital economy specifically.
- **Measure gender-based cyber violence**: Develop standardised measurement frameworks and use them to conduct population-level prevalence studies of gender-based cyber violence in digital economy settings. Conduct studies to understand the nature of and reasons for gender-based cyber violence in individual AMS. Without such understanding, policy and other strategies may not be accurately targeted. Comparative studies and longitudinal analyses will facilitate understanding of common and unique situations in each AMS and provide opportunities to learn from countries that have widespread digital access but low levels of gender-based cyber violence.
- **Capture the social and economic costs**: Develop and/or identify tools to measure the costs of gender-based cyber violence. This includes examining impacts related specifically to participation in the digital economy, such as women's experience of cyber violence in the workplace or in their professional life as entrepreneurs and leaders. In particular, estimates of the economic costs of gender-based cyber violence can be effective tools for government and industry advocacy.

References

ASEAN (2004), 'Declaration on the Elimination of Violence Against Women in the ASEAN Region', Jakarta: 13 June. http://hrlibrary.umn.edu/research/Philippines/Declaration%20on%20the%20Elimination%20of%20Violence%20Against%20Women%20in%20the%20ASEAN%20Region.pdf

ASEAN (2015), ASEAN Regional Plan of Action on the Elimination of Violence against Women. Jakarta: ASEAN Secretariat. https://asean.org/wp-content/uploads/2021/01/ASEAN-Regional-Plan-of-Action-on-Elimintation-of-Violence-Against-WomenAdopted.pdf

ASEAN (2017a), 'ASEAN Declaration to Prevent and Combat Cybercrime', Manila, 3 November. https://asean.org/wp-content/uploads/2017/11/ASEAN-Declaration-to-Combat-Cybercrime.pdf

ASEAN (2017b), 'Joint Statement on Promoting Women, Peace and Security in ASEAN', 31st ASEAN Summit, Manila, 13 November. https://asean.org/wp-content/uploads/2017/11/8.-ADOPTION_Joint-Statement-on-Promoting-Women-Peace-and-Security-in-ASEANACWC-Endorsed_rev2.pdf

ASEAN Committee on Women (2021), Foreword, In K. M. Belen, (2021), Ending Violence against Women in ASEAN Member States: Mid-Term Review of the ASEAN Regional Plan of Action on the Elimination of Violence against Women (ASEAN RPA on EVAW 2016–2025). Jakarta: ASEAN Secretariat and UN Women Regional Office for Asia and the Pacific. https://asiapacific.unwomen.org/sites/default/files/Field%20Office%20ESEAsia/Docs/Publications/2021/11/ap-evaw-MTR-REPORT-VAWG-22Nov2021.pdf

Athreya, B. (2021), 'Bias In, Bias Out: Gender and Work in the Platform Economy', Women, Work, and the Gig Economy (WWGE) initiative paper. Ottawa:

International Development Research Centre. https://idl-bnc-idrc.dspacedirect.org/handle/10625/60354

Aziz, Z.A. and G. Hassanein (2020), Online Violence Against Women in Asia: A Multicountry Study. Bangkok: UN Women Regional Office for Asia and the Pacific. https://asiapacific.unwomen.org/en/digital-library/publications/2020/12/online-violence-against-women-in-asia

Belen, K.M. (2021), Ending Violence against Women in ASEAN Member States: Mid-Term Review of the ASEAN Regional Plan of Action on the Elimination of Violence against Women (ASEAN RPA on EVAW 2016–2025). Jakarta: ASEAN Secretariat and UN Women Regional Office for Asia and the Pacific. https://asiapacific.unwomen.org/sites/default/files/Field%20Office%20ESEAsia/Docs/Publications/2021/11/ap-evaw-MTR-REPORT-VAWG-22Nov2021.pdf

Blume, G. (n.d.), 'Contributing Policy Analysis to Ocean Nexus: A Primer on Our Approach'. Unpublished manuscript.

Council of Europe (2001), 'Convention on Cybercrime', European Treaty Series, No. 185. https://rm.coe.int/1680081561

Council of Europe (2011), 'Council of Europe Convention on Preventing and Combating Violence Against Women and Domestic Violence', https://rm.coe.int/168008482e

Cruz, A. and S. Klinger (2011), 'Gender-Based Violence in the World of Work: Overview and Selected Annotated Bibliography', ILO Working Paper, No. 3/2011. Geneva: International Labour Organization.

Economist Intelligence Unit (2021), 'Measuring the Prevalence of Online Violence Against Women', Infographic. https://onlineviolencewomen.eiu.com/

ESCWA (2019), Guidelines to Estimate the Economic Cost of Domestic Violence in the Arab Region. Beirut: United Nations Economic and Social Commission for Western Asia.

Fraser, E. and L. Martineau-Searle (2018), 'Nature and Prevalence of Cyber Violence against Women and Girls', VAWG Helpdesk Research Report, No. 211. London: VAWG Helpdesk. https://www.gov.uk/research-for-development-outputs/nature-and-prevalence-of-cyber-violence-against-women-and-girls

Generation Equality (2021), Technology and Innovation for Gender Equality, Gender Equality Forum, Mexico, March. https://forum.generationequality.org/sites/default/files/2021-03/TIGE_FINAL_VISUAL_EN.pdf

Haarr, R. (2018), ASEAN Regional Guidelines on Violence against Women and Girls: Data Collection and Use. Bangkok: United Nations Entity for Gender Equality and the Empowerment of Women (UN Women). https://asiapacific.unwomen.org/sites/default/files/Field%20Office%20ESEAsia/Docs/Publications/2018/04/ASEAN-VAWG-Data-Guidelines.pdf

Hicks, J. (2021), 'Global Evidence on the Prevalence and Impact of Online Gender-Based Violence (OGBV)', K4D Helpdesk Report. Brighton, UK: Institute of Development Studies. https://doi.org/10.19088/K4D.2021.140

ILO (2019), 'Convention C190 – Violence and Harassment Convention, 2019', No. 190. https://www.ilo.org/dyn/normlex/en/f?p=NORMLEXPUB:12100:0::NO::P12100_ILO_CODE:C190

ILO (2021), Violence and Harassment in the World of Work: A Guide on Convention No. 190 and Recommendation No. 206. Geneva: International Labour Organization. http://www.ilo.org/global/topics/violence-harassment/resources/WCMS_814507/lang--en/index.htm

Kasliwal, R. (2020), 'Gender and the Gig Economy: A Qualitative Study of Gig Platforms for Women Workers', ORF Issue Brief, No. 359. New Delhi: Observer Research Foundation. https://www.orfonline.org/research/gender-and-the-gig-economy-a-qualitative-study-of-gig-platforms-for-women-workers-65948/

Khumalo, B., S. Msimang, and K. Bollbach (2014), Too Costly to Ignore – The Economic Impact of Gender-Based Violence in South Africa. KPMG Human and Social Services. http://www.ci.uct.ac.za/overview-violence/reports/too-costly-to-ignore-the-economic-impact-of-GBV-in-SA

Lomba, N., C. Navarra, and M. Fernandes (2021), Combating Gender-Based Violence: Cyber Violence, European Added Value Assessment. Brussels: European Added Value Unit and Directorate-General for Parliamentary Research Services. https://data.europa.eu/doi/10.2861/23053

Millar, K., J. Shires, and T. Tropina (2021), Gender Approaches to Cybersecurity: Design, Defence and Response. Geneva: United Nations Institute for Disarmament Research. https://doi.org/10.37559/GEN/21/01

NORC at the University of Chicago and the International Center for Research on Women (2022a), Landscape Analysis of Technology-Facilitated Gender Based Violence – Findings from the Asia Region. Washington, DC: United States Agency for International Development.

NORC at the University of Chicago and the International Center for Research on Women (2022b), Technology-Facilitated Gender Based Violence in Asia – Indonesia. Washington, DC: United States Agency for International Development.

Plan International (2020), 'Free to Be Online?', Plan International. https://plan-international.org/publications/free-to-be-online/

Posetti, J., N. Shabbir, D. Maynard, K. Bontcheva, and N. Aboulez (2021), 'The Chilling: Global Trends in Online Violence Against Women Journalists', Research Discussion Paper. Paris: United Nations Educational, Scientific and Cultural Organization.

Republic of the Philippines, (2018), Republic Act No. 11313. https://ppp.gov.ph/wp-content/uploads/2022/06/20190417-RA-11313-RRD.pdf

SAFEnet (2021), 'Against the Rampant Cases of Online Gender-Based Violence – Increase the Role of Law Enforcement', Joint Press Release, 10 March. https://safenet.or.id/joint-press-release-against-the-rampant-case-of-online-gender-based-violence-increase-the-role-of-law-enforcement/

Sey, A. (2021), 'Gender Digital Equality Across ASEAN', ERIA Discussion Paper Series, No. 358. Jakarta: Economic Research Institute for ASEAN and East Asia. http://www.eria.org/publications/gender-digital-equality-across-asean/

Sharland, L., N. Goussac, E. Currey, G. Feely, and S. O'Connor (2021), System Update: Towards a Women, Peace and Cybersecurity Agenda. Geneva: United Nations Institute for Disarmament Research. https://www.unidir.org/sites/default/files/2021-09/UNIDIR_System%20Update.pdf

Simonovic, D. (2018), 'Report of the Special Rapporteur on Violence against Women, Its Causes and Consequences on Online Violence Against Women and Girls from a Human Rights Perspective', Prepared for the Human Rights Council, 38th Session, 18 June–6 July. https://digitallibrary.un.org/record/1641160

Tech Policy Design Lab (2021), Online Gender-Based Violence and Abuse: Outcomes and Recommendations. https://techlab.webfoundation.org/ogbv/overview

The Australian Institute (2019), 'Trolls and Polls – The Economic Costs of Online Harassment and Cyberhate', January 2019. https://australiainstitute.org.au/wp-content/uploads/2020/12/P530-Trolls-and-polls-surveying-economic-costs-of-cyberhate-5bWEB5d_0.pdf

Timur, F.B. (2022), 'ASEAN and Gendered Violence in Cyberspace', in G. Haciyakupoglu and Y. Wong (eds.) Gender and Security in Digital Space: Navigating Access, Harassment, and Disinformation. London: Routledge, pp. 51–68.

UN Women (n.d.), 'Social Media Monitoring on COVID-19 and Misogyny in Asia and the Pacific'.

https://asiapacific.unwomen.org/sites/default/files/Field%20Office%20ESEAsia/Docs/Publications/2020/10/ap-wps-BRIEF-COVID-19-AND-ONLINE-MISOGYNY-HATE-SPEECH_FINAL.pdf

UN Women, UNFPA, and Quilt.ai (2021), COVID-19 and Violence Against Women: The Evidence Behind the Talk. https://asiapacific.unfpa.org/en/publications/covid-19-and-violence-against-women-evidence-behind-talk

US Department of State (2022), '2022 Roadmap for the Global Partnership for Action on Gender-Based Online Harassment and Abuse', Press Release, 16 March. https://www.state.gov/2022-roadmap-for-the-global-partnership-for-action-on-gender-based-online-harassment-and-abuse/

Vitis, L. (2021), 'Technology-Facilitated Violence Against Women in Singapore: Key Considerations', in J. Bailey, A. Flynn, and N. Henry (eds.) The Emerald International Handbook of Technology-Facilitated Violence and Abuse. Bingley: Emerald Publishing Limited, pp. 407–25. https://doi.org/10.1108/978-1-83982-848-520211031

World Bank (2019), 'Gender-Based Violence (Violence Against Women and Girls)', Brief, 25 September. https://www.worldbank.org/en/topic/socialsustainability/brief/violence-against-women-and-girls

World Wide Web Foundation and World Association of Girl Guides and Girl Scouts (2020), 'Survey—Young People's Experience of Online Harassment'. http://webfoundation.org/docs/2020/03/WF_WAGGGS-Survey-1-pager-1.pdf

ERIA Discussion Paper Series

No.	Author(s)	Title	Year
2022-35 (No. 464)	Araba SEY and Sara KINGSLEY	Women and Leadership in the ASEAN Digital Economy: Mapping the Rhetorical Landscape	December 2022
2022-34 (No. 463)	Upalat KORWATANASAKUL and Tran Thi HUE	Global Value Chain Participation and Labour Productivity in Manufacturing Firms in Viet Nam: Firm-Level Panel Analysis	October 2022
2022-33 (No. 462)	Fusanori IWASAKI and Keita OIKAWA	The Role of the Economic Research Institute for ASEAN and East Asia (ERIA) in Promoting the Regional Comprehensive Economic Partnership (RCEP)	October 2022
2022-32 (No. 461)	Mie OBA	Japan and the Regional Comprehensive Economic Partnership (RCEP)	October 2022
2022-31 (No. 460)	Chandra T. PUTRA	Global Value Chain Indicators: A Survey and Application to RCEP	October 2022
2022-30 (No. 459)	Cassey LEE	Economic and Technical Cooperation in the Regional Comprehensive Economic Partnership: Focus Areas and Support for Small and Medium-sized Enterprises	October 2022
2022-29 (No. 458)	Joseph Wira KOESNAIDI and Yu Yessi LESMANA	Trade Remedies Chapter	October 2022
2022-28 (No. 457)	Toshiyuki MATSUURA	Investment Liberalisation in East and Southeast Asia	October 2022
2022-27 (No. 456)	Christopher FINDLAY, Xianjia YE, and Hein ROELFSEMA	RCEP and Modern Services	October 2022
2022-26 (No. 455)	Archanun KOHPAIBOON and Juthathip JONGWANICH	Restrictiveness of RCEP Rules of Origin: Implications for Global Value Chains in East Asia	October 2022
2022-25 (No. 454)	Shiro ARMSTRONG and Peter DRYSDALE	The Implications of the Regional Comprehensive Economic Partnership (RCEP) for Asian Regional Architecture	October 2022
2022-24 (No. 453)	Shandre M THANGAVELU, Vutha HING, Ea Hai KHOV, Bunroth KHONG, and Seychanly TITH	Potential Impact of RCEP and Structural Transformation on Cambodia	October 2022
2022-23 (No. 452)	Mitsuyo ANDO, Fukunari KIMURA, and Kenta YAMANOUCHI	International Production Network in the Next Generation and the Role of RCEP	October 2022

ERIA discussion papers from the previous years can be found at:

http://www.eria.org/publications/category/discussion-papers