Addressing Online Violence Against Women and Girls in the Commonwealth Asia Region

The Role of Bystanders

The Commonwealth

Addressing Online Violence Against Women and Girls in the Commonwealth Asia Region

THE ROLE OF BYSTANDERS

The Commonwealth

Foreign, Commonwealth & Development Office

Commonwealth Secretariat
Marlborough House
Pall Mall
London SW1Y 5HX
United Kingdom

www.thecommonwealth.org

Published by the Commonwealth Secretariat.

Contents

List of Figures and Tables

Acronyms

ARC	Advocating the Rights of Children (Maldives)
ASEAN	Association of Southeast Asian Nations
AWARE	Association of Women for Action and Research (Singapore)
BLAST	Bangladesh Legal Aid and Services Trust
BNWLA	Bangladesh National Woman Lawyers' Association
BPC	Bangladesh Penal Code
CENWOR	Centre for Women's Research (Sri Lanka)
CoECoC	Council of Europe Convention on Cybercrime
CSAM	Child Sexual Abuse Materials
CSO	Civil Society Organisation
DRF	Digital Rights Foundation (Pakistan)
FIA	Federal Investigation Agency (Pakistan)
FIR	First Information Report
GSMA	Global System for Mobile Communications
IBA	Image-Based Abuse
ICRW	International Center for Research on Women
ICT	Information and Communications Technology
IFES	International Foundation for Electoral Systems
IMDA	Infocomm Media Development Authority (Singapore)
IMS	International Media Support
IPC	Indian Penal Code
ISP	Internet Service Provider
IT	Information Technology
ITU	International Telecommunication Union
LGBTIQ	Lesbian, Gay, Bisexual, Transgender, Intersex and Questioning
MCCHR	Malaysian Centre for Constitutionalism and Human Rights
MCMC	Malaysian Communications and Multimedia Commission
MLC	Media Literacy Council (Singapore)
NGO	Non-Governmental Organisation
OVAWG	Online Violence Against Women and Girls
PECA	Prevention of Electronic Crimes Act (Pakistan)
RESURJ	Realizing Sexual and Reproductive Justice
SDJF	Sri Lanka Development Journalist Foundation

SHE	Society for Health Education (Maldives)
SL CERT	Sri Lanka Computer Emergency Readiness Team
STEM	Science, Technology, Engineering and Mathematics
TMVAV	Technology Mediated Violence Against Women
UN	United Nations
UNDP	United Nations Development Programme
UNESCAP	United Nations Economic and Social Commission for Asia and the Pacific
UNICEF	United Nations Children's Fund
VAWG	Violence Against Women and Girls
WIN	Women In Need (Sri Lanka)

Acknowledgements

The Commonwealth Secretariat acknowledges with gratitude the financial support of the United Kingdom Foreign, Commonwealth & Development to the Commonwealth Cyber Capability Programme.

This report on Addressing Online Violence Against Women and Girls in the Commonwealth Asia Region: The Role of Bystanders is part of a series, which investigates the culpability of online bystanders in violence against women and girls in the cyberspace.

This report was authored by Professor Nir Kshetri, Bryan School of Business and Economics, University of North Carolina at Greensboro.

The series was prepared under the general guidance of Dr Tawanda Hondora, Adviser and Head of Rule of Law Section, Governance and Peace Directorate (GPD). Dr Nkechi Amobi, Senior Research Officer, Cyber Capability Programme, GPD, led and co-ordinated the review and editorial process of the report. Ms Emma Beckles, Programme Officer, GPD, and Mr Shakirudeen Ade Alade, Programme Coordinator, GPD, provided valuable feedback while Ms Helene Massaka, Programme Assistant, GPD, provided logistical and administrative support.

The team is grateful to Mrs Elizabeth Bakibinga-Gaswaga, former Legal Adviser Rule of Law Section, GPD, for conceptualising this research project.

The team is grateful for the constructive feedback received from an internal reviewer, Clive Lawson, Publications Assistant, Communications Division.

1. The current state and nature of online violence against women and girls

1.1 Increasing threats of online violence

Online violence is increasing rapidly and is emerging as one of the biggest threats facing the online world today. Acts of online violence take multiple forms, including cyberstalking, cyberbullying, sexual harassment, sex trolling (Davies, 2020), doxing, hate speech, public shaming and intimidation (Vega Montiel, 2020).

Most acts of online violence take place on social media platforms such as Facebook and Twitter. These platforms function in ways that differ dramatically from past media. A key consideration here is that such outlets lack rigorous editors to vet the quality of the posts before they are published (Leong, 2017). Users can share pictures, videos, text messages, news and other content with each other with little or no third-party filtering, fact-checking or editorial judgement. Some who post reach as many followers and readers as major media outlets such as the *New York Times*, Fox News and CNN (Allcott and Gentzkow, 2017).

Cyberbullying, which is a targeted online intentional act by an individual or a group to inflict psychological and emotional harm on Internet users, is among the most pervasive forms of violence. Such an act is repeated over time, against targets who cannot easily defend themselves (Slonje et al., 2013). In a survey conducted in 25 countries, the three countries in which respondents reported the highest rates of cyberbullying were in Asia: China (70 per cent), Singapore (58 per cent) and India (53 per cent). Moreover, China and Singapore were the only countries that reported higher rates of online compared with offline victimisation (Microsoft Corporation, in Bhat et al., 2013). Likewise, a Pew Research Center survey released in September 2018, which was conducted among US teens to understand the impact of cyberbullying, revealed that 59 per cent of US teens had been bullied or harassed online (Anderson, 2018).

Meanwhile, moving to the focus of this report, recent surveys conducted across countries worldwide have indicated that women and girls are victimised disproportionately online as compared with men and boys. For instance, according to the Pew Research Center survey mentioned earlier, 39 per cent of girls reported being victims of false rumours online compared with 26 per cent of boys. Likewise, 29 per cent of girls reported that they had received unwanted explicit images compared with 20 per cent of boys. In the same vein, 15 per cent of teenage girls had become targets of four or more different forms of cyberbullying compared with 6 per cent of boys (Anderson, 2018). Likewise, the Association of Southeast Asian Nations (ASEAN) has reported a growing concern about bullying and discrimination against women and children in mass and social media in its member countries (ASEAN, 2016).

Plan International, which focuses on advancing children's rights and equality for girls, held a global survey of 14,000 girls aged 15-25 in.22 countries, including Commonwealth member countries such as India. This survey found that 58 per cent of girls and women had experienced harassment on social media platforms (Plan International, 2020). The proportions of girls/women reporting that they had been harassed on different social media platforms were as follows: Facebook 39 per cent, Instagram 23 per cent, WhatsApp 14 per cent, Snapchat 10 per cent, Twitter 9 per cent and TikTok 6 per cent (ibid., in Norzom and Balakrishnan, 2020).

Cyberbullies who harass women online are also making use of sophisticated technologies such as deepfake. One Indian journalist was the target of cyber-harassment for many years; the perpetrators posted a porn video with her face superimposed on it (Ayyub, 2018).

Surveys have also found that online violence against women and girls (OVAWG) increased during the pandemic period (Davies, 2020). Indeed, the pandemic led to increases in both online and offline gender-based violence (ITU, 2020).

A large number of users experience OVAWG because of the ease with which content can be distributed online across multiple platforms, and because of the Internet's widespread reach, speed of transmission, encryption and anonymity. These factors also sometimes amplify the harm and lead to bystander participation.

In the context of violent crimes online, bystander participation has been defined as 'third parties who recklessly download, forward and share violent content, whether they are conscious or ignorant of the fact that the content is violent or was disseminated without the consent of the subject' (UN Women, 2020). The action of a primary perpetrator alone is likely to cause much less harm to their target if bystanders do not respond to the content in a way that negatively affects the target. Bystanders can thus be viewed as secondary perpetrators and hence should be held accountable. Primary perpetrators often use secondary perpetrators to worsen the effects of OVAWG (ibid.). In many cases, then, bystanders are 'not so innocent' (Coloroso, 2016). Interventions to prevent and minimise victimisation through OVAWG should focus on both primary and secondary perpetrators.

1.2 The situation in Commonwealth Asia member countries

Broadly speaking, OVAWG and the victimisation pattern in Commonwealth Asia member countries are consistent with the overall global trend. However, given unique formal and informal institutions in these countries, perpetration and victimisation related to OVAWG have many significant aspects that are different from most other countries in the world. As a result of underdeveloped regulations and regulatory infrastructure related to OVAWG, it is difficult to arrest, prosecute and convict the perpetrators in most of these countries. Meanwhile, societal norms tend to make victims of OVAWG feel devalued and excluded.

Table 1.1 presents Internet users and penetration by gender in Commonwealth Asia member countries. While in 2020 37.6 per cent of the population in these countries used the Internet, the proportion varies from the lowest observed for Pakistan at 17.8 per cent to the highest for Brunei Darussalam at 88.7 per cent. It is also worth noting that in Brunei Darussalam and Singapore there are more female than male internet users.

Table 1.2 presents the situation of OVAWG in Commonwealth Asia member countries. As this table makes clear, women and girls are significantly more likely to be victimised through online violence compared with men and boys in these countries.

Just like in other parts of the world, the COVID-19 pandemic has worsened the situation. According to an Indian nationwide survey conducted in 2021 by social media company Bumble, among women, 70 per cent believed that cyberbullying had increased during the COVID-19 lockdown (Nazir, 2021).

Table 1.1. Internet users and penetration by gender in Commonwealth Asia member countries

	Internet users 2020 ('000s)	Population 2020 ('000s)	% of population using Internet 2020	% of male population using Internet 2019	% of female population using Internet 2019
Bangladesh	49,265.7	164,689.4	29.9	N/A	N/A
Brunei Darussalam	388.2	437.5	88.7	91.8	99.8
India	544,666.6	1,344,810.1	40.5	25.0	14.9
Malaysia	25,927.4	32,657.3	79.4	91.3	87.7
Maldives	367.0	540.5	67.9	N/A	N/A
Pakistan	39,371.4	220,892.3	17.8	21.3	12.9
Singapore	4,948.0	5,685.8	87.0	75.0	76.7
Sri Lanka	9,162.6	21,413.2	42.8	N/A	N/A
Total	674,096.9	1,791,126.1	37.6		

Source: www.itu.int/en/ITU-D/Statistics/Pages/stat/default.aspx for the last two columns; Euromonitor International for the first three columns.

Table 1.2. The situation of OVAWG in Commonwealth Asia member countries – some representative statistics

Country	OVAWG situation
Bangladesh	As of December 2017, the Information and Communication Technology Division's Cyber Help Desk had received over 17,000 complaints (70 per cent of victims were women). 2014 study: 11 suicide attempts of OVAWG victims (BNWLA, 2014).
Brunei Darussalam	Royal Brunei Police Force: 300 cases of cyberbullying in 2012 and 182 cases in the first half of 2013 (Kamit, 2016). 2018: about 200 cases of bullying in schools, the majority cyberbullying (Kon, 2019).
India	National Crime Records Bureau report: 4,242 cases of cybercrimes against women in 2017, which increased to 6,030 in.2018 (Norzom and Balakrishnan, 2020). About 90 per cent of cyberstalking victims are women (Roy, 2015). 2019: 777 cases of offences related to cyber-stalking and cyberbullying that victimised women and children (Keelery, 2021). 2021 survey by Bumble: 83 per cent of women experienced online harassment, and one in three experienced such harassment weekly. About 60 per cent felt unsafe, and 48 per cent felt angry. Around 70 per cent believed that cyberbullying increased during the COVID-19 lockdown (Nazir, 2021).
Malaysia	Proportion of adolescents cyberbullied: 26–33 per cent (Lomba et al., 2021). PeopleACT survey (in MCCHR, 2018): 2,333 reported cases of cyber-harassment in 2013–2017. 50.4 per cent harassed online. 20.9 per cent of women and 9.8 per cent of men sexually harassed online. 4.8 per cent of women and 3.3 per cent of men receiving online death or rape threats. 16.4 per cent of women and 13.1 per cent of men victimised by online stalking.
Maldives	April 2018: two cases of cyberbullying reported to the Ministry of Gender, Family and Social Services (Maldives Independent, 2018).
Pakistan	2017 study by Digital Rights Foundation: 40 per cent of women had become victims of online harassment (Abassi, n.d.). First seven months of 2018: FIA Lahore received 4,000 cyber-harassment complaints by women (Business Recorder, 2018).
Singapore	AWARE study: 124 cases of digital sexual violence in 2018 compared with 46 in.2016. More than half of the cases in 2018 involved images (Yi, 2019).
Sri Lanka	OVAWG is the second biggest form of gender-based violence (SDJF, 2020). 2020: about 400 cases of cyber-harassment reported (Fazlulhaq, 2021). Women In Need study reported in February 2021: 32.5 per cent of women reported to have friends who had been victimised by online violence. The share was 16.5 per cent for men (Gunasekera, 2021).

1.3 The nature of perpetration and victimisation in OVAWG

Often, the offenders in online violence are family, friends and other persons that the victim knows and trusts. For example, friends or dating partners are seven times more likely than other people to be offenders in cyberbullying incidents against children and young adults (White, 2017). In a survey conducted in 28 countries, 51 per cent reported that the offenders in cyberbullying were classmates of the cyberbullied children. The proportion was the highest in North America (65 per cent) and the lowest in the Middle East/Africa (39 per cent) (Newall, 2018).

In order to be able to provide further insights and a deeper understanding of this issue, it is important to consider primary and secondary victimisation. Primary victimisation describes a victim of the crime directly. Impacts covered by primary victimisation include physical and psychological suffering and financial losses. Secondary victimisation, on the other hand, takes place in response to the victim's social environment. Key mechanisms involved in secondary victimisation include stigmatisation, social isolation, or intrusive and humiliating questioning (Tandon, 2007). Secondary victimisation also occurs because of journalists' faulty and insensitive practices in gathering or reporting news or because of inappropriate actions by the criminal justice system (ibid.).

1.4 Response of OVAWG victims

Victimisation through OVAWG can have impacts of various forms and various degrees of severity. In extreme cases, OVAWG also results in complex public health issues such as suicide. For instance, cyberbullying victims have been found to be twice as likely to attempt suicide (Hinduja and Patchin, 2010; Mental Health Commission, 2017).

In general, just like for any type of risk, there are four possible response strategies to handle risks related to OVAWG: avoid, reduce, transfer and accept (Williams, 2017).

For many victims of OVAWG incidents, **'avoid'** has been the chosen response strategy. Avoiding a risk means completely quitting a particular action or not starting the action at all. When this option is chosen, potential victims eliminate the possibility that the risk will be a threat. For instance, to avoid cyber-risks, victims may disconnect some activities from the Internet (Kshetri, 2021). Victims are often found to feel more stressed in engaging in social media activities and have a greater desire to stay away from social media to avoid being victimised. In the Plan International global survey noted above, about one-fifth of respondents had quit or reduced their social media use and 12 per cent had changed the way they expressed themselves (Norzom and Balakrishnan, 2020). A 2016 study conducted by the Association of Media Women in Kenya and the international human rights organisation, Article 19, entitled 'Women Journalists' Digital Security', found that online violence often led to self-censorship and discouraged women journalists from writing about issues that might make them targets of online harassment and abuse (article19.org 2016).

As a result of online harassment, many women journalists in Pakistan have shifted patterns of movement, relocated or hidden themselves. They have increased their physical security and some have left the profession (Maas, 2021). Likewise, one Indian journalist explained how cyber-harassment had led to self-censorship: 'From the day the video was published, I have not been the same person. I used to be very opinionated, now I'm much more cautious about what I post online. I've self-censored quite a bit out of necessity' (Ayyub, 2018).

This is an unfortunate situation since, because of decreased access to physical support services during the COVID-19 pandemic, victims of violence against women and girls (VAWG) may need to rely on online resources for support. They are likely to be in an even more vulnerable position if they are reluctant to use online resources owing to fear of online harassment (UNESCAP, 2020).

Some victims of OVAWG incidents have chosen **'reduce'** as the response strategy. Reducing or mitigating entails taking actions to reduce the likelihood of being victimised by OVAWG or the impact from an offence. If the current risk is higher than individuals can absorb, risks could be reduced to within the tolerance level. Individuals and organisations apply various risk mitigation strategies based on their assessment of risks. These include spending money to deal with OVAWG incidents. A study on information and communications technology (ICT) VAWG conducted by UN Women in 2019 in five Asian countries – including three Commonwealth

member countries (India, Malaysia, Pakistan), the Philippines and the Republic of Korea – found that some victims/survivors hired private contractors ('digital undertakers') to delete the violent content (UN Women, 2020).

Seeking bystander intervention could be another way to reduce or mitigate risks related to OVAWG. However, seeking bystander intervention has not been a common response among victims. In the UN Women survey conducted to gauge civil society's perceptions of common responses to ICT VAWG among victims/survivors, the score for 'Seeks collective action/bystander intervention' was 2.6 (1 = never, 2 = rarely, 3 = occasionally, 4 = a great amount, 5 = a great deal). The scores were higher for other categories of responses: 'Authorities resolve the matter' (2.8), 'Ceases using internet or ICT device(s)' (4), 'Reduces online presence' (4.3) and 'Deletes/deactivates social media account' (4.4) (UN Women. 2020).

Women and girls should also consider transfer and accept as cyber-risk management strategies. For instance, they can transfer a cyber-risk to a third party by buying cyber insurance. With this option, they do not eliminate or reduce the risk. Instead, cyber insurance, which transfers cyber risks that are insurable from one party (policyholders) to another (the cyber insurer), is growing rapidly in the West (Kshetri, 2021). It can be expected that cyber insurance will be more common in the future in the countries analysed in this study.

The last option is to accept the cyber risk as it is, which means doing nothing. This strategy is often appropriate for cyber risks that have a low probability of occurrence or lead to a low impact if they occur. For instance, it may not be appropriate for the victims of less serious online harassment to leave the profession completely as discussed above.

2. Institutional factors related to online violence against women and girls

2.1 Viewing OVAWG through an institutional lens

Institutions are defined as the 'macro-level rules of the game' (North, 1990), which include 'formal constraints (rules, laws, constitutions), informal constraints (norms of behaviour, conventions, and self-imposed codes of conduct), and their enforcement characteristics' (North, 1996). Formal and informal institutions can help us understand the behaviours of victims, primary perpetrators, secondary perpetrators (bystanders) and other relevant actors.

W. R. Scott has conceptualised institutions as composed of three pillars: regulative, normative and cognitive. The regulative pillar is related to formal institutions whereas the normative and cognitive pillars are related to informal institutions.

Regulative institutions consist of 'explicit regulative processes: rule setting, monitoring, and sanctioning activities' (Scott, 1995). They are related to regulatory bodies and the existing laws and rules that influence OVAWG. These institutions focus on pragmatic legitimacy concerns in managing the demands of regulators and governments (Kelman, 1987). Individuals and organisations adhere to them so they will not suffer the penalty for noncompliance (Hoffman, 1999).

Normative institutions introduce 'a prescriptive, evaluative, and obligatory dimension into social life' (Scott, 1995). The idea here is that online activities need to be consistent with and to consider different assumptions and value systems of national cultures in order to gain legitimacy. Elements of normative institutions include civil society organisations (CSOs) and trade or professional associations that can use social obligation as a tool to induce certain behaviours.

W.R. Scott suggests that 'cognitive elements constitute the nature of reality and the frames through which meaning is made' (Scott, 1995). Although carried by individuals, cognitive programmes are elements of the social environment (Berger and Luckmann, 1967). Various actors and stakeholders differ in the ways they understand and view OVAWG.

It is also important to note that formal and informal rules are tightly linked. Informal rules provide legitimacy to formal rules (North, 1994). Likewise, Axelrod (1997) comments on the relationship between these two types of institutions: 'Social norms and laws are often mutually supporting. This is true because social norms can become formalized into laws and because laws provide external validation of norms.'

2.2 Formal institutions and OVAWG

In general, in Commonwealth Asia member countries, penal codes have been adopted based on the colonial British mandate law system. Many of these countries exhibit a high degree of similarity in their laws to deal with OVAWG. These countries have realised that perpetrators cannot be effectively punished using laws enacted in the pre-Internet era. They are thus enacting new laws to deal with cybercrime, and data protection and privacy.

Commonwealth Asia member countries are, however, characterised by heterogeneous legislative initiatives in these areas. Table 2.1 presents the status of cybercrime laws, data protection and privacy laws relating to OVAWG in Commonwealth Asia member countries.

Cybercrime laws deal with criminal activities in which computers or computer networks are the principal means of committing an offence (Kshetri, 2009a). In economies that have enacted cybercrime laws, online perpetrators can be tried and convicted based explicitly on such laws. In countries that lack cybercrime laws, existing provisions are stretched to accommodate cybercrimes, or use

is made of provisions enacted for other purposes, which may cover only peripheral acts related to cybercrimes (Schjølberg, 2008). As of August 2021, all Commonwealth Asia member countries except Maldives had such laws; the latter had draft legislation in discussion as of 2020.

Data protection and privacy laws deal with how personally identifiable information of individuals collected by any entity, such as a government or a public or private organisation, is stored and used. As of December 2022, three Commonwealth Asia member countries – Bangladesh, Brunei Darussalam and Sri Lanka – lacked such laws. Two other countries –Maldives and Pakistan – had only draft legislation.

The global nature of some OVAWG incidents means there are important procedural and jurisdictional issues associated with them. Some progress has been made in the international harmonisation and standardisation of norms to deal with such incidents. For instance, the Council of Europe's Convention on Cybercrime (CoECoC), more commonly known as the Budapest Convention, is the first international treaty on cybercrimes.[1] As of October 2022, 67 countries had signed as well as ratified the convention in accordance with their national constitutional or legal requirements, making it enforceable. Two additional countries (South Africa and Ireland) had signed the CoECoC but had not ratified it. Sri Lanka is the only Commonwealth country in Asia to have ratified the CoECoC. The convention came into force in 2004. Among other things, it provides a framework to guide local child protection efforts (UNICEF, 2016). It has been reported that Maldives is in discussions with the Council of Europe to ratify the CoECoC and is working to meet the legislative requirements required. Likewise, Bangladesh's Cybersecurity Strategy states that it is based on the CoECoC (ibid.). Pakistan is also reported to use the CoECoC as a model in its cybercrime legislation (ITU, 2010).

Some regional political and economic organisations have also addressed issues related to OVAWG. Since three of the Commonwealth Asia member countries – Brunei Darussalam, Malaysia and Singapore – are members of ASEAN, it is worth noting that ASEAN has provided recommendations for national and regional actions to address these issues. Key national actions to prevent VAWG include the development of gender-responsive regulatory mechanisms, codes of conduct and guidelines for the media and journalists as well as key industries such as those related to advertising, animation and gaming. The goal should be to eliminate the 'glamorisation and normalisation' of VAWG and harmful gender stereotypes in social as well as mainstream media. At the regional level, ASEAN has recommended regional sharing of good practices and experiences, which includes feasible, practical and successful policy and programme interventions (ASEAN, 2016).

In a World Bank analysis of 17 Asian countries (Song, 2016), Brunei Darussalam and Singapore were among five countries (together with Japan, the Philippines and the Republic of Korea) whose legal systems to deal with violence against children through ICTs (activities related to child pornography, online grooming and cyberbullying) exhibited 'favourable or moderate alignment' with relevant international standards. Brunei Darussalam and Singapore (together with Japan and the Republic of Korea) are classified as developed countries. The high level of economic development in these countries leads to the increased affordability and use of ICTs.

The study also found that countries with a higher level of ICT diffusion may face higher risks associated with ICT use in child abuse and exploitation (Song, 2016). Similar arguments can be made for OVAWG. At the same time, these countries are in a better position to adopt or amend legal measures to fight the use of ICTs to commit violence against children as well as OVAWG (ibid.). Brunei Darussalam lacks comprehensive laws on data protection. The country's Data Protection Policy covers personal data in electronic as well as manual form maintained by government agencies and educational institutions (Deloitte, 2018). However, in the context of adoption or amendment of legal measures to fight OVAWG, the issue has received little attention.

2.3 Informal institutions and OVAWG

Informal institutions can help in understanding how perpetrators of OVAWG justify their offences and how their victims feel after the violent incident. In general, OVAWG may be more justifiable if informal institutions (or social and internalised norms) against them in a society are weaker. Likewise,

1 www.coe.int/en/web/conventions/full-list/-/conventions/treaty/185

Table 2.1. Status of cybercrime, and data protection and privacy laws in Commonwealth Asia member countries

	Cybercrime laws	Data protection and privacy laws	Remarks
Bangladesh[1]	National Digital Security Act No. 46/2018	No legislation	
Brunei Darussalam[2]	Computer Misuse Act, revised 2007	No legislation	
India[3]	Information Telecommunication Act 2000, amended 2008	Personal Data Protection Bill 2019 Information Technology Act 2000	
Malaysia[4]	Computer Crimes Act 1997	Personal Data Protection Act 2010	
Maldives[5]	Draft legislation: bill in discussion as of 2020	Draft legislation: bill; law coming Q3 2020	
Pakistan	Prevention of Electronic Crimes Act 2016 Prevention of Electronic Crime Ordinance 2009	Draft legislation: bill - Electronic Data Protection Act 2005	
Singapore[6]	Cybersecurity Act No. 9/2018	Personal Data Protection Act No. 26/2012	
Sri Lanka[7]	Computer Crime Act No. 24/2007 Payment Devices Frauds Act 2006	No legislation	Signatory of international instrument, Budapest Convention on Cybercrime

[1]https://unctad.org/page/cyberlaw-tracker-country-detail?country=bd
[2]https://unctad.org/page/cyberlaw-tracker-country-detail?country=bn
[3]https://unctad.org/page/cyberlaw-tracker-country-detail?country=in
[4]https://unctad.org/page/cyberlaw-tracker-country-detail?country=my
[5]https://unctad.org/page/cyberlaw-tracker-country-detail?country=mv
[6]https://unctad.org/page/cyberlaw-tracker-country-detail?country=sg
[7]https://unctad.org/page/cyberlaw-tracker-country-detail?country=lk

the societal norms may make victims of OVAWG feel isolated and alone because they do not feel comfortable to share concerns with others.

2.3.1 Internalised and institutionalised norms

Informal institutions can be viewed as consisting of two types of norms or constraints – internalised and institutionalised – that can affect the behaviours of a person (P) (Galtung, 1958). These are captured by what Scott (1995) refers to as normative and cognitive pillars of institutions. Scott observes the existence of external and internal dimensions in institutions by stating that values and norms 'are both internalized and imposed by others'. Institutionalised norms are 'norms from other members from the social system to P' and internalised norms are 'norms from P to himself'. Institutionalised and internalised norms are related to external and internal stigma, respectively (Aguilar-Millan et al., 2008), which increase the psychic cost of feeling embarrassment and shame (Blackwell, 2000).

Internalised norms:

A study conducted in South Asian countries (Bangladesh, India and Pakistan) found that victims of OVAWG such as revenge porn were less likely to

report the incident to the police because of the fear of reputation damage (Halder, 2017). The victims' internalised norms place more emphasis on the importance of reputation than on taking action against offenders,

Institutionalised norms:

Institutionalised norms are related to embarrassment, which is a socially imposed sanction that occurs when individuals violate norms endorsed by the society, especially by significant others (Paetzold et al., 2008). An external or social stigma is related to resentment against a criminal activity, which can lead to a deterrent against crimes (Rasmussen, 1996). There is also fear that family members such as parents, siblings and significant others will attribute blame to the victim for their problems related to social media use. In many cases, such a fear is justified owing to cultural factors that define societal expectations from women. As explained in Chapter 3, one Sri Lankan girl who became a OVAWG victim was beaten by her brother when he knew about the victimisation (Rodrigo, 2020).

2.3.2 Social identity theory and cultural 'Others'

Condemnation of an act such as OVAWG leads to internalisation of norms against the act among the 'condemners' as well as the 'condemned' (Kahan, 1996). From the society's point of view, whether victimisation related to a crime elicits 'a stigma or a sympathy effect may depend on the evaluator's characteristics' (Lyons, 2006). In this regard, social identity theory points to the possibility of ethnocentric bias (Tajfel and Turner, 1986). A central tenet of social identity theory is that in-group victims and offenders are likely to be perceived sympathetically while out-group victims and offenders may be stigmatised (Lyons, 2006). For instance, Hindu fundamentalists who engaged in online violence against Muslim women had a common pattern of content. Many of the perpetrators' accounts followed each other and they interacted and amplified each others' content (Jafri and Aafaq, 2021). In this way, secondary perpetrators or bystanders stigmatise the victims. It is also worth noting that primary and secondary (bystanders) perpetrators view each other as members of in-groups whereas the victim is viewed as a member of an out-group.

The orientation of a culture towards OVAWG may differ depending on who the perpetrators and the victims are. The society may view an OVAWG incident differently when the victim is a part of 'Others'. The idea of cultural Others may help us understand this phenomenon better. It is argued that cultural Others are defined according to 'who they are not' rather than 'who they are' (Jandt and Tanno, 2001). This is based on the assumption that 'all humans may possess the seeds of pseudospeciation, of prejudice against dissimilar groups and values' (Hoare, 1991). For instance, perpetrators may target victims with different religions and may engage in OVAWG against those who challenge their religious beliefs and values (Kshetri and Alcantara, 2015).

2.3.3 OVAWG as an intrinsically motivated offence

Most of the offences related to OVAWG are associated with intrinsic motivation rather than extrinsic motivation (e.g., driven by financial incentives). Intrinsic motivations are tightly related to informal institutions.

The theory of intrinsic motivation is based on the premise that human needs for competence and self-determination are linked with interest and enjoyment (Deci and Ryan, 1985). Intrinsically motivated individuals do activities for 'inherent satisfactions rather than for some separable consequence' (Ryan and Deci, 2000). Intrinsically motivated persons engage in activities 'for the fun or challenge entailed rather than because of external prods, pressures or rewards' (ibid.).

Intrinsic motivation can be divided into two separate constituents: (i) enjoyment-based intrinsic motivation and (ii) obligation/community-based intrinsic motivation (Lindenberg, 2001).

Enjoyment-based intrinsic motivation:

Central to the concept of intrinsic motivation is having fun or enjoying oneself when taking part in an activity (Ryan and Deci, 2000). Some activities are pursued for the sake of enjoyment derived from doing them (Csikszentmihalyi, 1975). For instance, perpetrators who have ethnonationalist beliefs and orientations may justify ethnic superiority over Others to victimise the latter by posting violent content (primary perpetrators). In other cases, individuals with such beliefs may engage in interaction such as sharing and liking violent

content that victimises Others and feel a sense of enjoyment by doing so. These bystanders become secondary perpetrators.

Obligation/community-based intrinsic motivation:

Acting on the basis of principle is also a form of intrinsic motivation (Lindenberg, 2001). Individuals may be socialised into acting appropriately and in a manner consistent with the norms of a group. The goal to act consistently within the norms of a group can trigger a normative frame of action (Lakhani and Wolf, 2005). Perpetrators may associate themselves with various groups, such as a nation, a territory or another ideological group. In general, geography, race, religion, culture and language are the key elements in the justification and legitimisation of extremism (Leidig, 2020). Some of these are also driving factors in some types of OVAWG. The followers of right-wing extremism, for instance, may feel pushed or pressured to share posts or like them. These bystanders (secondary perpetrators) return favours (such as sharing and liking posts and pages) to primary perpetrators and thus are far from innocent. As mentioned, bystanders who further victimise the victim are in groups with the primary perpetrators.

2.4 The role of civil society organisations and trade and professional associations

CSOs and trade and professional associations are considered to be a part of normative institutions (Kshetri and Dholakia, 2009). It is argued that CSOs and trade and professional associations represent an alternative to the coercive state (Walzer, 1993). Most obviously, when the state's regulatory roles are weak, these organisations may fill the regulatory vacuum.

Some CSOs are working towards creating new institutions (e.g., new regulations to criminalise OVAWG). Institutional researchers have come up with the concept of institutional entrepreneurship to examine the role of these actors in creating new institutions. DiMaggio (1988) notes that new institutions arise when organised actors with sufficient resources (institutional entrepreneurs) see in them an opportunity to realise interests that they value highly.

In some situations, the state will collaborate with such organisations to rationalise an arena of activity (Scott, 1992). CSOs and trade and professional associations thus play an important role in strengthening regulatory institutions by providing the state with their expertise in developing new regulatory frameworks and strengthening enforcement mechanisms. To take an example, non-profit online network iProbono works with Sri Lanka's Ministry of Youth Affairs and Ministry of Justice on measures to fight cyberbullying and undertake reforms in the criminal law system to criminalise cyberbullying, revenge porn and cyber-harassment (Family Planning Association 2022).

3. Country case studies

In order to fight OVAWG, it is important to understand the associated actors, institutions and processes. This chapter provides detailed country case studies of OVAWG, covering key regulatory and legislative features and the actions and responses of relevant actors. Specifically, it provides a valuable glimpse of the prevalence of victimisation and perpetration related to OVAWG, describes the regulatory situation, highlights the law enforcement and judiciary response, evaluates the role of CSOs and looks into victims' responses.

3.1 Bangladesh

3.1.1 Prevalence of victimisation and perpetration

As of December 2017, the Bangladesh government's Information and Communication Technology Division's Cyber Help Desk had received over 17,000 complaints. Of the victims, 70 per cent were women (Akter, 2018). A 2018 study by the non-governmental organisation (NGO) Cyber Crime Awareness Foundation found that women between 18 and 30 years old accounted for 73.71 per cent of cybercrime victims in Bangladesh (Mahmud, 2018).

Another study found that at least one-third of mobile phone subscribers were women and 73 per cent of them faced some form of online violence (The Daily Star, 2018). Likewise, 80 per cent of cyberbullying victims are women between 14 and 22 years old. The majority of perpetrators are teenagers (New Age Bangladesh, 2020). Lack of cybersecurity has been a challenge, increasing women's vulnerability to attacks from hackers (IFES, 2021).

A Bangladesh National Woman Lawyers' Association (BNWLA) study published in 2014 found that every year there were around 11 suicide attempts by women who had become victims of cyber-violence (BNWLA, 2014).

In 2019, the international non-profit organisation International Foundation for Electoral Systems (IFES), which supports elections in new and emerging democracies, conducted a study of online violence against politically and civically engaged women in Bangladesh. It detailed a number of key findings (IFES, 2021). Women politicians as well as women engaged in civic activism were found to face online violence threats. Among the major modes of online violence, perpetrators of psychosocial violence were found to engage in character assassination and defamation. In the cultural context of Bangladesh, such activities can harm a woman's reputation and discourage women from running for office. The use of gendered stereotypes was also common. For instance, perpetrators try to give the impression that women lack intelligence to be political leaders.

Women leaders who belong to religious and ethnic minorities are often targeted by perpetrators purportedly belonging to majority religious and ethnic identities. Nonetheless, online violence also targets women political leaders belonging to majority religious and ethnic groups. Perpetrators of online harassment also defame women by questioning their religion. For instance, they may falsely state that a woman belongs to a different religious group than she actually does. As predicted by social identity theory, by falsely stating a woman victim's religious group, perpetrators are likely to get sympathy from bystanders, who are likely to stigmatise the victim (Lyons, 2006).

The study found a correlation between online and offline violence. Some perpetrators combine online harassment with harassment in the real world. Others start from online violence and move to physical and sexual violence (IFES, 2021).

Perpetrators also use homophobia and transphobia to discredit politicians. By doing so, they seek to reinforce the standards of 'heteronormativity and hypermasculinity' that currently dominate politics (IFES, 2021).

3.1.2 The regulatory situation

As noted earlier, while Bangladesh has enacted its National Digital Security Act No. 46/2018 to deal with cybercrimes,there are no data protection and privacy laws. However, various sections of the Bangladesh Penal Code (BPC) 1860 can be used to penalise OVAWG offences.

Section 509 of the BPC 1860 criminalises acts, words and gestures that 'outrage the modesty of a

woman'. Offenders face a prison sentence of up to one year along with fines. This is substantially similar to Section 10 of the Nari-O-Shishu Nirjatan Daman Ain (Prevention of Atrocities against Women and Children Act) 2000, which has introduced an offence *jounopiron*, or 'sexual oppression', which criminalises the act of touching a woman or child (with any part of their body or with an object) or 'violating a woman's modesty' (*narirshilotahanikoren*) in order to 'illegally satisfy their sexual desires'. A person who violates Section 10 of the Nari-O-Shishu Nirjatan Daman Ain can face a prison sentence of two to 10 years (BLAST, 2017).

Section 504 of the BPC criminalises 'intentional insult with intent to provoke breach of the peace'. Section 500 states that, 'Whoever defames another shall be punished with simple imprisonment for a term which may extend to two years, or with a fine, or with both.'

Another relevant law is the Pornography Control Act, 2012. According to the provisions of Section 2, the definition of pornography includes nude or half nude videos and still pictures as well as any material that may 'increase sexual sensation or desires'. Section 8(1) provides a penalty of incarceration for up to eight years and a fine of up to TK 200,000 (about £1,703) for taking an image or a video that is pornographic in nature. Section 8(3) criminalises the distribution of pornographic material using the Internet and mobile phones. It provides for incarceration for up to five years and a fine of up to TK 200,000 (about £1,703).

3.1.3 Law enforcement and the judiciary

Cybersecurity enforcement has been virtually absent in Bangladesh. In some cases, it is misapplied to limit free speech (IFES, 2021). Estimates suggest that about 90 per cent of cyberviolence instances go unreported (Akter, 2018). The IFES study found that, since perpetrators are rarely punished, victims rarely seek redress. Women who do so are reported to face backlash (IFES, 2021). A statement of a victim who reported a harassment case to the police is telling.

> 'I had to go to the cyber crime department where the police officer sat me down with my harasser, and then mocked me in front of him, for wanting to proceed with this case. He said, "People are left with no work during this corona period. Thus this is happening. Why do you want to tarnish your university's name at the court? Please rethink"' (Islam, 2021).

In the study conducted by the Cyber Crime Awareness Foundation (Mahmud, 2018), around 54 per cent of victims expressed dissatisfaction with the response of law enforcement agencies after reporting an incident. The study also found that 39 per cent of victims did not report cybercrime cases to law enforcement agencies: 23 per cent thought they would be harassed instead of getting help and 25 per cent thought it would not help them reporting cybercrime incidents to law enforcement agencies. 30 per cent of victims reported that they did not know how to seek help if they were victimised. Other reasons behind the lack of reporting included protecting social status and the fact that the perpetrator was influential. Victims also reported that instant punishments for criminals, increased implementation of the law and raising awareness among Internet users could help control cybercrime (ibid.).

As of June 2018, the Cybercrime Tribunal had received 520 cases of cyber-violence, of which 328 were dropped. While Bangladesh's police have a cyber wing, which monitors cybercrimes and tracks the criminals, it does not deal with specific cases of gender-based online violence (Akter, 2018).

3.1.4 Women in law enforcement

In November 2020, Bangladesh's police established an all-female unit to fight online abuse and harassment targeting women. It is expected that women victims will be likely to be more comfortable speaking to an all-woman team, which will encourage more women to report online abuse (Aljazeera, 2020).

3.1.5 The roles of civil society organisations and trade and professional associations

The activist women's organisation Bangladesh Nari Progati Sangha announced a plan to conduct a content analysis of news items about the presentation of women in Bangladeshi media, including online media, to understand violence against women from a gender sensitivity as well as a women's human rights perspective. The goal was to raise awareness among journalists and policy-makers for more responsible reporting. The plan was to monitor one week's news coverage of five

newspapers, five TV stations and five online news portals (WACC, 2016).

The international human rights organisation Article 19 organised a consultation, titled Technology Mediated Violence Against Women in Bangladesh (TMVAW) in March 2018 in.Dhaka. The consultation made several recommendations, which included (i) creation of greater awareness regarding TMVAW and existing legal remedies; (ii) implementation of the High Court directives on sexual harassment; and (iii) strengthening investigation procedures for online offences (The Daily Star, 2018). Article 19 Bangladesh and Free Press Unlimited have launched a campaign that aims to bring institutional changes in media outlets so that women's rights are protected (IMS, 2019).

3.2 Brunei Darussalam

3.2.1 Prevalence of victimisation and perpetration

While sexual harassment is believed to be prevalent in the workplace in Brunei Darussalam, it is suspected that victims rarely report such cases (US Department of State, 2016). A similar point can be made about online harassment.

An incident reported by several media outlets was that of a 13-year-old cyberbullying victim who recorded a sex video in 2014 under pressure from her boyfriend. After the video went viral, many social media users harassed the girl online, forcing her to change school. She was bullied in the new school since people recognised her from the video (Kamit, 2016). In this case, the activities of bystanders clearly increased the severity of the victimisation.

3.2.2 The regulatory situation

While Section 509 of the Penal Code 1951 (Cap 22) imposes imprisonment for up to three years and a fine for crimes related to sexual harassment, the definition of sexual harassment does not cover cyber-harassment and other settings such as the workplace, educational establishments, sporting establishments and public places.[2]

In 2013, Brunei Darussalam established a Child Online Protection Framework, based on the International Telecommunication Union (ITU) Child Online Protection Initiative. This helps co-ordinate the actions of different agencies working to ensure child safety online. The Content Advisory Council has members from various government agencies, including the Attorney General's Chambers. Its goal is to protect users from online threats by monitoring online content that is against the 'cultural, social and religious norms of Brunei Darussalam' (Sharbawi, 2018). The Attorney General's Chambers has also established a Cybercrime Focus Group to ensure the country's legal measures to fight cybercrimes follow international standards. The Group is reportedly amending the Computer Misuse Act, the Evidence Act and the Criminal Procedure Code as well as the Penal Code to include new cyber-offences (ibid.).

In order to address gender-based offences, specific legal provisions as well as specialised courts are needed (UN Women, 2020). These conditions are lacking in Brunei Darussalam. The country has no law specifically addressing VAWG. Special provisions are needed to investigate, prosecute and punish perpetrators and provide protection and support services for victims of such violence. These provisions have not yet been developed in the country.[3]

3.2.3 The roles of civil society organisations and trade and professional associations

In 2021, Project Women Brunei organised a webinar series on women's rights in various settings, including violence in the workplace. While OVAWG was not the focus on the series, some speakers covered this topic. For instance, in a Zoom session held in February 2021, a speaker discussed increasing cases of online sexual harassment during the COVID-19 pandemic, when most activities had moved online (Faisal, 2021). Project Women Brunei also organised a workshop titled Ending the Culture of Victim-Blaming in Gender-Based Violence: Busting Myths with Facts. Participants came from various stakeholder groups such as NGOs, self-organised women groups, corporations, government agencies, health care institutions, academia, sports associations, counselling groups and policy-making bodies (Mohamad, 2020).

In 2019, students of Universiti Brunei Darussalam organised a cyberbullying awareness event. The panellists included Brunei Computer Emergency

2 www.genderindex.org/wp-content/uploads/files/datasheets/2019/BN.pdf

3 Ibid.

Response Team's security analyst, a technology company's executive and others, who shared their personal experiences related to online harassment (Borneo Bulletin, 2019).

3.3 India

3.3.1 Prevalence of victimisation and perpetration

India's National Crime Records Bureau reports that there were 4,242 cases of cybercrime against women in 2017, which increased to 6,030 in.2018 (Norzom and Balakrishnan, 2020). In India, about 90 per cent of cyberstalking victims are women (Roy, 2015).

In Himachal Pradesh, on an average, 60 per cent of cybercrimes reported during 2017-2019 were against women. About 60-90 cybercrime-related complaints were received every week. Most of the complaints were related to fake profiles, virtual stalking, sexually explicit material, blackmail by means of morphed photos and fake chatting (Lohumi, 2020).

About one in 10 Indian adolescents become cyberbullying victims every year (Maheshwari, 2020). A 2017 online survey commissioned by cybersecurity firm Norton by Symantec with 1,035 respondents from Tier 1 cities found that 41 per cent of women had faced online sexual harassment (Bhargava, 2017). In 2019, India reported 777 cases of offences related to cyberstalking and bullying, in which women and children were the victims (Keelery, 2021).

However, in general, cybercrime conviction rates have been very low. For instance, in Bangladesh cybercrime conviction rate has been reported to be 3%. India cybercrime conviction rates are 0.33% in the Mahrashtra state and 0.17% in the Karnataka state (Kshetri, 2021).

According to a nationwide survey conducted in 2021 by social media company Bumble, 83 per cent of Indian women have experienced online harassment, and one in three women have experienced such harassment weekly. About 60 per cent of women reported that they felt unsafe and 48 per cent felt angry (Nazir, 2021).

Elite users and traditional participants within political debate, such as politicians and journalists, are more likely to be victimised. According to an Amnesty International report in 2020, women politicians in India receive 113 problematic or abusive tweets per day on average. These included threats and badgering. The report is based on an analysis of 114,716 tweets directed at 95 Indian women politicians during the 2019 Indian general election. This found that 13.8 per cent of the tweets that mentioned 95 women politicians were either 'problematic' or 'abusive', which translated to over 10,000 such tweets every day. The report points out that Indian female leaders deal with almost twice as much harassment as their counterparts in the UK or the US. It concludes that women who try to break into the male-dominated political landscape have to fight against sexism in parliament as well as online.

Online abuse facing Muslim women politicians is reported to be more frequent and severe in India: 55 per cent of the most aggressive trolling targeted Muslim women leaders (Amnesty International, 2020). Muslim women were reported to receive 94.1 per cent more ethnic or religious slurs than women from other religions. Likewise, women from marginalised castes are 59 per cent more likely to face abuse. Amnesty International notes that there are few legal avenues for women to challenge online abuse in the country. It asks Twitter to regulate abuse on its platform. Recommendations include sharing information on a country basis regarding online abuse against women; improving reporting mechanisms; and providing 'more clarity on how the company defines, identifies, and responds to abuse' (Godin, 2020).

At a panel discussion on online violence against women organised by Amnesty International, an India Supreme Court lawyer put the issue this way:

> 'My colour is commented upon. I am called burnt. Connections are made between my sense of dressing and my caste. In addition, when you are a Dalit, a woman and dark in colour, many do not even come forward to raise their voices for you like they would have if you didn't belong to a marginalised community. The response of officials is no different' (Salim, 2018).

Women who belong to marginalised sections of society are likely to be targeted more. The level of support they receive when they are harassed is also lower. One Indian journalist noted: 'Labelling me Islamist, they [online abusers] refer to me as "Jehadi Jane", they call me "didi", they call me Apa. Targeting me on the basis of my gender was not enough it

seems when they found out they also targeted me based on my Muslim identity' (Salim, 2018).

On 13 May 2021, the day before Eid, the national coordinator for the Congress Party found she had been 'sold' in an online 'auction'. She filed a first information report (FIR), hoping the Delhi police would punish the perpetrator. She noted: 'While I kept tagging the police and Twitter authorities, the account continued making insulting remarks about my religion and gender' (Jafri and Aafaq, 2021).

About 80 Muslim women who were active on social media were reported to have been 'auctioned' online in open-source software development platform GitHub '*sulli* deals'.[4] Most of them were artists, researchers, journalists and students. One public health professional victim said: 'They targeted us because we are women, we are Muslim and we are outspoken' (Mihindukulasuriya, 2021). The auctions used titles such as 'Your sulli deal of the day is…'.

The victims alleged that people who belonged to the 'right-wing ecosystem' posted and shared the GitHub posts on Twitter. It was reported that the ex-editor of Op-India and co-founder of Do Politics was one of the persons promoting the website. In a tweet, he stated: 'If someone brings a good deal to general mass, what can be wrong' (Mihindukulasuriya, 2021). Following the GitHub posts, some women were reported to have deactivated their social media accounts. Others filed FIRs and complaints with the police. During Eid in 2020, similar virtual 'bids' took place on YouTube. Pakistani Muslim women's photos were uploaded by the Indian YouTube channel Liberal Doge (ibid.). In July 2021, the person who allegedly ran the Liberal Doge channel uploaded another video and boasted that no action had been taken against them (Kamdar, 2021).

3.3.2 The regulatory situation

The Indian Penal Code (IPC) and the Information Technology (IT) Act have several parallel provisions that can be used to deal with OVAWG. Section 66E of the IT Act 2000 as amended by the IT Act 2008 can be used to punish violators of privacy. This section provides that:

> 'Whoever, intentionally or knowingly captures, publishes or transmits the image of a private area of any person without his or her consent, under circumstances violating the privacy of that person, shall be punished with imprisonment which may extend to three years or with fine not exceeding two lakh rupees [about £1,977] or with both.'

Sections 292 and 509 of the IPC also partially cover such offences (Joseph and Ray, 2020).

Sections 67 and 67A of the IT Act criminalise publishing and circulation of 'obscene' or 'lascivious' content (Dasgupta, 2017). Section 67 states:

> 'If a person publishes or transmits or causes to be published in the electronic form, any material which is lascivious or appeals to the prurient interest or if its effect is such as to tend to deprave and corrupt persons who are likely, having regard to all relevant circumstances, to read, see or hear the matter contained or embodied in it.'

This section punishes the offender with imprisonment of up to three years and a fine for first conviction. For subsequent convictions, the punishment is imprisonment of five years and a fine. A challenge posed by this section is that, in many 'revenge porn' cases, the pictures or videos are often recorded and first shared by the victims themselves. This means that the victims are also liable for transmitting the 'lascivious' content (Yashee, 2018).

Section 67A of the IT Act extends the law to an individual 'who publishes or transmits images containing a sexually explicit act or conduct' (Dasgupta, 2017). This section punishes the offender with imprisonment of up to five years and a fine for first conviction. For subsequent convictions, the punishment is imprisonment of seven years and a fine. Section 67B punishes the publication and transmission of sexually explicit content depicting children.

Before 2013, India had no law to directly tackle online harassment or crimes victimising women in the cyberspace. The 2013 Criminal Amendment Act to the IPC 1860 provided a remedy for OVAWG. Sections 354A through 354D are of particular interest.

Section 354A criminalises the following acts: a demand or request for sexual favours; showing pornography against the will of a woman; or making sexually coloured remarks. Perpetrators 'shall be

4 *Sulli* is a derogatory term for Muslim women.

guilty of the offence of sexual harassment, may be punished with rigorous imprisonment for a term which may extend to three years, or with fine, or with both'.

Section 354C deals with voyeurism. It defines this as 'the act of capturing the image of a woman engaging in a private act, and/or disseminating said image, without her consent'. An act will qualify as voyeurism when the victim would 'usually have the expectation of not being observed either by the perpetrator or by any other person at the behest of the perpetrator'. If the victim consents to the capture of the images or any act, but not to their dissemination to third persons, such dissemination is considered an offence (Yashee, 2018). A person found guilty under this section may face a fine as well as imprisonment up to three years on the first conviction. The prison time is up to seven years for subsequent convictions.

Section 354D introduces a provision for stalking including cyberstalking, which is used to prosecute perpetrators of cyberstalking and bullying (Keelery, 2021). Cyberstalking is defined in the section as an act in which 'a man follows or contacts a woman, despite clear indication of disinterest to such contact by the woman, or monitors the cyber activity or use of the Internet or electronic communication of a woman'. A person convicted of stalking would face imprisonment of up to three years and a fine for the first offence. For any subsequent offence, the perpetrator would be liable for imprisonment up to five years and a fine. If a man is a victim of cyberstalking, Section 354D will not apply (Joseph and Jain, 2020).

In addition to the 2013 amendments made to the IPC, OVAWG and other cyber-offences can be charged using other IPC provisions, specifically Sections 499, 503 and 507.

Section 499 states:

> 'To defame a person is to do an act with the intention of harming the reputation of the person. Defamation by publication of visible representations of an imputation concerning the woman, when done with the intention to harm her reputation, is punishable with imprisonment for a term, which may extend to two years, or with fine, or both.'

Section 503 states:

> 'Threats made to any person with injury to her reputation, either in order to cause alarm to her, or to make her change her course of action regarding anything she would otherwise do/not do is punishable as criminal intimidation.'

This section can be used to punish blackmail on the internet.

Section 507 states:

> 'This provision provides the quantum of punishment for Criminal Intimidation when the same is by a person whose identity is not known to the victim. Any anonymous communication, which amounts to criminal intimidation under Section 503 stated above, is punishable under this section.'

Section 509 states:

> 'Any person who utters any word or makes any sound or gesture, or exhibits any object with the intention that such word, sound or gesture or object be heard or seen by a woman and insult her modesty, or intrudes a privacy, may be charged under this section and imprisoned for a term that may extend to 3 years.'

An offender may also have to pay a fine. Lewd comments or remarks made, or other explicit images and content forcibly online, may also be penalised under this section.

The occurrence of the cyber-offence known as morphing, in which photos of political leaders, journalists and other celebrities are morphed into nude bodies, is rapidly rising. One Indian journalist, who was the target of cyber-harassment for many years, had her face superimposed onto a porn video. Morphing is not defined as an offence under the IPC and the IT Act.[5] While some perpetrators of morphing have been charged, legal provisions dealing with defamation of persons have been used to file charges against them (Nilesh Beliraya K and Abhilasha, 2020).

India lacks laws that specifically criminalise 'revenge porn'. The perpetrators can be charged under different statutory provisions such as the IPC's provisions on defamation (Section 500), criminal intimidation (Sections 504 and 506), outraging the modesty of a woman (Section 354) and sexual harassment (Section 354A).

5 https://debaraticyberspace.blogspot.com/search/label/morphing

India's adoption of a safe-harbour approach to intermediary liability has been a challenge in the fight against OVAWG. With certain exceptions, intermediaries are provided immunity from legal liability. The Supreme Court of India's ruling is that intermediaries should act based only on judicial or executive orders. This is challenging since content related to online VAWG needs to be removed immediately in order to minimise the harm to the subjects involved (RESURJ, n.d.).

Several loopholes in the laws and policies of the Indian judicial system hinder efforts to fight cybercrimes against women (Halder and Jaishankar, 2016). Legislation focusing on the Internet, such as cybercrime laws as well as other existing laws such as the IPC and laws on national security, are used to regulate and criminalise OVAWG. However, these various laws are inconsistent, leading to incoherence and confusion (RESURJ, n.d.). As a result of the existence of various overlapping and inconsistent laws, the fate of the offender and whether justice is served to the victim of online violence are often in the hands of the lawyers and judges of the case concerned (Yashee, 2018).

3.3.3 Law enforcement and the judiciary

In 2004, of the 4,400 police officers in India's Mumbai city, only five worked in the cybercrime division (Duggal, 2004). As of November 2011, the Delhi police cybercrime cell had only two inspectors (Anand, 2011). In June 2012, the Delhi High Court criticised the lack of functionality of the Delhi police website, which according to the court was 'completely useless...obsolete and does not serve any purpose' (Nolen, 2012).

Consequently, congestion and inefficiency in law enforcement is a major concern, and the gap between law on paper and law in action has been substantial. Of reported crimes, about 2 per cent are registered (Hindustan Times, 2006). Most organisations reported doubts about the competence, professionalism and integrity of the police in handling cybercrime cases. In a survey conducted in Gurgaon, where many outsourcing centres are located, about 50 per cent of respondents not reporting crimes thought that cases were not dealt with professionally and 30 per cent noted that they had 'no faith' in the Gurgaon police (The Times of India, 2011).

One reason behind the low rate of registration of cybercrime cases concerns the barriers, hurdles and hassles that confront the victims (Kshetri, 2017). In some cases, the police show unwillingness to do the extra work needed for the investigation (Narayan, 2010). There are reports that the police do not support the victim when they want to report a cybercrime case. Cybercrime victims have also complained that the police follow a long and inefficient process to build a criminal case (Anand, 2011).

The conviction rate in cybercrime cases is as low as 2 per cent (Hindustan Times, 2006). Until 2010, there was not a single cybercrime-related conviction in Bengaluru, the biggest offshoring hub in the country. The total number of convicted cases by 2010 was estimated at under 10 (Narayan, 2010).

3.3.4 Women in law enforcement

Despite India's well-established judicial system and law enforcement procedures, a gender bias is reported in the police force. The proportion of women in police force positions is around 7 per cent, one of the lowest shares in the world. The central government has set a goal to increase this to 33 per cent but it has been challenging to find enough women willing to join the police force (Advani, 2021).

Uttar Pradesh is taking measures to address this situation, specifically to address OVAWG. In order to tackle cases such as cyberstalking and cyberbullying, the Uttar Pradesh government has decided to set up a 'women cyber cell' at each cyber police station in the state. The women cyber cell will deal with women-related cybercrimes. As of March 2021, there were 18 cyber police stations in various cities in the state (Hindustan Times, 2021).

3.3.5 The roles of civil society organisations and trade and professional associations

The Centre for Cyber Victim Counselling develops educational cyber-awareness programmes for various constituencies, such as schools, parents and the police force (Broadband Commission for Digital Development, 2015). One of the goals of the programmes is to tackle violence against women online.

Human rights organisation Breakthrough India is working to fight violence and discrimination against women and girls (Dubey, 2017). One of its initiatives is the use of popular culture and social media to

raise awareness and encourage bystanders to intervene against perpetrators. In December 2020, it launched a social media campaign Dakhal Do ('Intervene') to promote bystander intervention to stop such violence in private and public spaces (DeVries, 2020). The campaigns have also focused on cyberbullying activities victimising women and girls.[6]

3.3.6 Victims' response

In India, about 10 per cent of cybercrimes are reported (Kshetri, 2017). A 2016 survey of 500 social media users in India, part of Freedom House's Hyperlinkers project, found that only one-third of the respondents had reported online harassment to law enforcement agencies. Of those reporting, 38 per cent characterised the response as 'not at all helpful' (Pasricha, 2016). About half of adolescent cyberbullying victims do not report it (Maheshwari, 2020).

3.4 Malaysia

3.4.1 Prevalence of victimisation and perpetration

The proportion of adolescents victimised by cyberbullying in Malaysia is estimated at between 26 and 33 per cent (Lomba et al., 2021). According to the Malaysian Communications and Multimedia Commission (MCMC), there were 3,762 complaints of cyber-harassment between 2018 and January 2019 (Nortajuddin, 2020).

Contents and visuals from the Women's March in 2019 were circulated on social media platforms. The participants were shamed and attacked. Some received death threats for attending the march. Others were doxed – that is, their private and personal information was publicly revealed. Some universities and employers were concerned that their students and employees were associated with LGBTIQ+ issues and gave them warnings. Following the publication of their pictures on social media, some participants also suffered hostility and ill treatment from mainstream media (Lim, 2021).

Owing to certain societal expectations, Muslim women are more likely to be targeted, especially based on how they present themselves. If women wear too much makeup or too tight clothes, they are more likely to become targets of gender-based online violence. In 2017, when a 15-year-old Malaysian girl expressed her dream on Twitter of becoming the country's first female prime minister, she became a victim of online abuse for not putting on the hijab.

Malaysia lacks gender-based laws to protect women from online violence. It is argued that the Communications and Multimedia Act sometimes works against Internet freedoms since the government may punish Internet users for messages that are viewed as incompatible with the line of politics or religion. Political parties also employ cybertroopers who watch online activity to find content that represents 'controversial' political dissent. One women's activities said: 'The counter-propaganda method can be extremely hostile and when they're facing women, it becomes a violent exchange where women are attacked, body-shamed, and policed about their Muslim identities' (BBC, 2017).

3.4.2 The regulatory situation

Cyberstalking perpetrators are prosecuted under the Penal Code and the computer-specific Communications and Multimedia Act 1998 (CMA 1998). Section 503 of the latter, which is punishable through Section 506 of the Penal Code, Act 574 1997, covers stalking and cyberstalking, which are viewed as criminal intimidation. The punishment is incarceration for up to two years or a fine or both. According to Section 503, criminal intimidation is committed if a person threatens another person with the intention of causing harm. As of 2020, no cases of criminal intimidation had involved stalking or cyberstalking. The prosecuted cases under Section 503 have generally been related to physical violence (Hamin and Wan Rosli, 2020).

3.4.3 Other relevant actions of government agencies

The Ministry of Women, Family and Community Development's Child Online Protection Taskforce aims to fight online threats including cyberbullying, pornography, sexting and cyber-grooming. Relevant ministries and agencies contribute to the Taskforce. The Ministry has also developed a Plan of Action on Child Online Protection.

The MCMC's key roles include prohibiting offensive content and promoting public education on content-related issues. The MCMC has collaborated with diverse stakeholders to

6 www.dailymotion.com/video/x7ylnas

implement the Klik Dengan Bijak (the 'Click Wisely' programme). The goal of this is to increase online safety awareness among children, young adults, parents, guardians and other individuals.

The Ministry of Science, Technology and Innovation's Cybersecurity Malaysia, the Ministry of Education and mobile service provider DiGi Telecommunications have implemented the CyberSAFE programme. This aims to raise online safety awareness among children, parents and educators. It also conducts the CyberSAFE in Schools National Survey annually to assess the extent of children's exposure to online risks (Internet Society, 2017).

3.4.4 Law enforcement and the judiciary

A 2017 report submitted to the UN by Malaysian civil society groups Persatuan Kesedaran Komuniti Selangor (Empower), Bersih 2.0, Justice for Sisters, the Malaysian Centre for Constitutionalism and Human Rights, the National Council of Women's Organisations, Malaysia, and Women's Aid Organisation expressed concerns regarding law enforcement agencies' lack of action to stop OVAWG as reported by victims. The report noted that agencies often treated acts of OVAWG as 'normal' and were often ignorant about existing laws to deal with OVAWG. Another complaint was that they failed to understand the severity of the crime. Citing anecdotal cases, the report noted that victims' experiences were often trivialised and normalised. The report expressed concerns that victims struggled to obtain access to justice because police officers failed to recognise online threats and harassment as violence (Malay Mail, 2017).

3.4.5 The roles of civil society organisations

The CSO Empower has been studying cyber-violence and suggests that cyber-violence against women needs specific and specialised attention and understanding. A key challenge concerns securing sufficient evidence to successfully prosecute perpetrators since victimised women often get rid of crucial evidence. For instance, they delete emails, text messages and photos (Skinnider, 2018).

3.4.6 Victims' response

Most victims of online violence do not report to the police (Nortajuddin, 2020). Among key reasons for the low reporting rate, studies have highlighted the negative and unsupportive attitude that law enforcement agencies have towards victims of OVAWG. The 2017 report submitted by Malaysian civil society groups to the UN noted:

> 'Responses by police officers were either dismissive or condescending. Oftentimes the police would tell the victim that there is nothing they could do as it is a "private affair" or that the victim should just delete his/her account' (Malay Mail, 2020).

3.5 Maldives

3.5.1 Prevalence of victimisation and perpetration

Only two cases of cyberbullying were reported during April 2018 to the Ministry of Gender, Family and Social Services in Maldives (Maldives Independent, 2018). However, it is possible that reported crimes represent only the tip of the iceberg. For instance, incidence of online child sexual abuse and online bullying is reported to be growing rapidly in the country (Munavvar, 2020).

Several high-profile incidents of OVAWG have been motivated by religious intolerance. In November 2019, the Maldives police reported that an online harassment case targeted at a young woman for wearing a suit at the Maldives Film Awards was under investigation. A location where the victim had previously worked was also vandalised: a brick was thrown through the window (Moosa, 2019). Meanwhile, a host on Minivan Radio received threats after she criticised the construction of a mosque in Malé that was funded by Saudi Arabia (FORUM-ASIA, 2019).

3.5.2 The regulatory situation

According to the United Nations Conference on Trade and Development's Global Cyberlaw Tracker, Maldives lags behind its peers in terms of legislations for digital development (Table 2.1). This is partly because of the absence of legislation on electronic transactions, privacy, data protection and cybercrime. Maldives lacks officially recognised national cybercrime legislation, which creates a challenge in dealing with OVAWG (World Bank, 2021).

3.5.3 Other relevant actions of government agencies

The Ministry of Education has launched a manual for parents on cyber-safety, which includes minimising the risks associated with cyberbullying (World Bank, 2021). Advocating the Rights of Children (ARC), the Ministry of Education, the Society for Health Education (SHE), the Telecommunications Authority of Maldives and the Cybercrime Unit have launched awareness-raising campaigns to address cyberbullying and blackmail. ARC and the Ministry of Education have teamed up to run a Surf Smart campaign in schools to fight these issues. SHE uses young peer educators in its awareness campaigns. The Cybercrime Unit's awareness-raising campaigns in schools focus on the importance of privacy settings on social media accounts (UNICEF, 2016).

The Telecommunications Authority of Maldives looks to Singapore as a role model for best practices to deal with child sexual abuse materials (CSAM) online. When a website is reported to contain CSAM, the Authority asks the Internet service provider (ISP) to block the content. One of the two mobile service providers in Maldives, Dhiraagu, is also a member of the Global System for Mobile Communications (GSMA) Mobile Alliance Against Child Sexual Abuse Content (UNICEF, 2016). This works with policy-makers, law enforcement, hotline organisations, NGOs and the mobile industry to remove CSAM. All members commit to implementing notice and takedown procedures on CSAM in response to court orders or allegations of CSAM.[7]

3.5.4 Law enforcement and the judiciary

Law enforcement agencies have failed to take effective security measures to protect human rights defenders (FORUM-ASIA, 2019). In Maldives, only one case of sexual harassment had been prosecuted as of November 2019 (Moosa, 2020).

3.5.5 The roles of civil society organisations

Membership-based regional human rights organisation the Asian Forum for Human Rights and Development, previously known as FORUM-ASIA, has expressed concerns regarding online harassment in Maldives, which is becoming increasingly violent. The Forum asked the Maldives Police Service and the Human Rights Commission of the Maldives to investigate online harassment of human rights defenders and ensure their security (FORUM-ASIA, 2019).

In June 2020, Maldives women's rights organisation, Uthema, expressed concern regarding false claims on social media that had been made about its report to the UN Committee on the Elimination of All Forms of Discrimination Against Women. Extremist groups had alleged that the activities of Uthema were anti-Islam and demanded the government ban the organisation. Uthema asked the Ministry of Youth, Sports and Community Empowerment to provide it with a venue to engage with the extremist groups to provide clarifications on the report, and noted that the social media campaign represented a politically motivated effort to misinterpret points raised in its report. It further pointed out that this was an obstruction to efforts to address the country's severe social issues. International NGO Human Rights Watch asked the government to 'investigate and appropriately prosecute those responsible for harassment, intimidation or assault' rather than appeasing the extremist groups, arguing that: 'Islamist extremist groups that are a relic of the previous abusive government persist in their threats and violence against pro-democracy activists. The Solih administration should demonstrate a firm commitment to free expression by taking action against those attacking it' (Civicus, 2020).

3.5.6 Efforts of technology companies

A Maldives mobile operator reported that, in 2017, it had teamed up with one of its peers to raise awareness on call harassment. The two operators issued joint press releases, which focused on the risks of giving personal phone numbers to others. The operator said that this was a large-scale campaign. The campaign made use of mainstream media, social media and SMS as part of the operators' corporate social responsibility strategy. However, the operator also noted that there was a commercial argument, in the sense that people would be less likely to use their mobile devices if they did not feel safe to do so (GSMA, 2018). Initiatives such as this can help promote corporate social responsibility and increase sales and the company's reputation.

7 www.gsma.com/publicpolicy/consumer-affairs/children-mobile-technology/mobile-alliance

3.6 Pakistan

3.6.1 Prevalence of victimisation and perpetration

According to the Federal Investigation Agency (FIA), in the first nine months of 2014 there had been more than 170 complaints of cybercrime against women in Pakistan's most populous province of Punjab (Houreld, 2014). A 2017 study by the Lahore-based research and advocacy NGO Digital Rights Foundation (DRF), which is arguably Pakistan's first study on online violence against women, found that 40 per cent of women in the country had become victims of online harassment (Abassi, n.d.).

In 2018 and 2019, the FIA reported that it had registered 8,500 complaints of women facing online harassment. According to its report to a parliamentary committee, most complaints involved blackmailing and harassment over social media (Gossman, 2020). Likewise, in the first seven months of 2018, the cybercrime circle of the FIA Lahore received 4,000 cyber-harassment complaints from women (Business Recorder, 2018).

The FIA established the Cyber Crime 24/7 helpline 9911 in January 2020. This received 787 complaints in February 2020. More than 100 women had complained regarding online harassment, blackmailing and defamation (Wahab, 2020).

In order to support victims of online harassment, the DRF founded the Cyber Harassment Helpline in December 2016 (DRF, n.d.). This received 2,023 complaints in 2019. About 58 per cent of the complaints were from women, and 70 per cent expressed fear about posting photos online (Bukhari, 2020). In many cases, male members of the family call on behalf of women (Toppa, 2017).

3.6.2 The regulatory situation

On the regulatory front, the Prevention of Electronic Crimes Act (PECA) 2016 is a major legislative effort to fight cybercrimes in general, including OVAWG. On the positive side, the PECA includes special protection of women (Section 21). Among other things, the PECA has criminalised the sharing of pictures without consent. If sexually explicit pictures are used for blackmailing purposes, there are heavy penalties, which may include up to seven years in jail and a fine of 5 million Pakistani rupees (around £37,200) (Toppa, 2017).

However, some problematic aspects of the PECA have been highlighted. Section 20, for instance, makes it a criminal offence to transmit defamatory information. Human rights organisations have expressed concerns that this provision duplicates existing law on defamation in the Penal Code. The section does not outline clear procedures, and provides the Federal Investigation Agency (FIA) with broad discretionary powers over content decisions. In September 2020, the FIA charged nine people under this section, including female witnesses in a sexual harassment case against a man who then lodged a criminal defamation case. Several feminist groups condemned the agency's action: 'Feminist groups across the country are appalled at the blatant weaponisation of the criminal defamation laws in Pakistan to silence victims and survivors of sexual assault and harassment' (Gossman, 2020).

In addition, Pakistan's Penal Code has sections on harassment and defamation (DRF, 2017). For instance, Section 509 covers:

> 'Insulting modesty or causing sexual harassment': '(i) Intending to insult the modesty of any woman, utters any word, makes any sound or gesture, or exhibits any object, intending that such word or sound shall be heard, or that such gesture or object shall be seen, by such woman, or intrudes upon the privacy of such woman; (ii) conducts sexual advances, or demands sexual favours or uses written or verbal communication or physical conduct of a sexual nature which intends to annoy, insult, intimidate or threaten the other person or commits such acts at the premises of work place, or makes submission to such conduct either explicitly or implicitly a term or condition of an individual's employment, or makes submission to or rejection of such conduct by an individual a basis for employment decision affecting such individual, or retaliates because of rejection of such behaviour, or conducts such behaviour with the intention of unreasonably interfering with an individual's work performance or creating an intimidating, hostile, or offensive working environment.'

Section 499 covers:

> 'Defamation: Whoever by words either spoken or intended to be read, or by signs or by visible representations, makes or publishes

> any imputation concerning any person intending to harm, or knowing or having reason to believe that such imputation will harm, the reputation of such person, is said except in the cases hereinafter excepted, to defame that person.'

Section 25-D of the Telegraph Act 1885 also addresses harassment using communication systems (DRF, 2017). It states:

> 'Any person, including a Telegraph Officer, who uses any telephone, public or private, for causing annoyance or intimidation to any person, whether a subscriber or not, or for obnoxious calls shall, without prejudice to any other action which the Telegraph Authority is competent to make under this Act, be punishable with imprisonment for a term which may extend to three years, or with fine, or with both.'

3.6.3 Law enforcement and the judiciary

The FIA's cybercrime wing monitors and investigates cybercrimes in the country. It also deals with all major crimes, such as corruption, trafficking and terrorism, espionage, federal crimes and smuggling (Toppa, 2017). Congestion and inefficiency in law enforcement is thus a major concern. As of 2020, the FIA's cybercrime wing had 346 contract employees and only 82 permanent employees. In the Financial Year 2020–21, Rs 130 million (US$581,000) was allotted for the agency (Hanif, 2022) It was reported in December 2022 that the contracted employees of the FIA's cybercrime wing had not been paid for the past six months (Sajid, 2022). There were only 10 officials to deal with cyber-harassment cases in the cybercrime circle of the FIA in Lahore (Business Recorder, 2018).

The FIA is required by law to submit biannual reports to parliament. Over 2016-2020, it submitted only one (Gossman, 2020). This noted that only 19.5 per cent of complaints related to blackmailing and harassment over social media were investigated (ibid.).

In the province of Punjab, no cybercrime case against women had been successfully prosecuted as of 2014 (Houreld, 2014). In general, the probability that perpetrators of violence against women and girls are prosecuted is 'almost zero' in Pakistan (Gancia, 2020).

Males dominate the FIA, and there is a need to improve their empathy and understanding towards women victims. Men staffers are reported to pursue online harassment cases arbitrarily. Example, in 2017, the DRF submitted a complaint about a Facebook account that harassed its founder, Nighat Dad. When an officer of the FIA was asked for updates on the investigation, he reportedly said: 'A public figure such as yourself must get these threats regularly, no?' (Gossman, 2020).

Until 2018, there were only two women working on the cybercrime help desk (Gossman, 2020). The FIA reported that all major cybercrime stations had a woman 'stress counsellor' who work with women victims in serious cases (Tahir, 2021).

3.6.4 Victims' response

Many victims choose not to report attacks to law enforcement agencies or social media platforms. It is said that the police rarely act when women report cyber-harassment cases (Tahir, 2021). Women find reporting online harassment intimidating and discouraging. In order to register a cybercrime with the FIA, the victim is required to disclose their national identity card number, phone number and father's name; just a trip to a local police station may require revealing one's name. Many families do not allow their daughters to leave home unaccompanied by a male relative. Such a restriction means that crimes may never be reported to police when the perpetrator is a relative of the victim.

Some women journalists noted that, when they reported cybercrimes under the PECA, law enforcement agencies ignored their complaints. Women are reported to be harassed using the law's defamation provisions, making the matter worse (Gossman, 2020). Meanwhile, one estimate suggested that 72 per cent of women lacked awareness about laws dealing with online harassment, such as cybercrime laws, in the country (Pakistan Today, 2019).

Women feel that reporting may lead to reputational damage and create more danger. Factors such as censorship of women's bodies, Internet intermediaries' policies and national laws related to gender expression and identity as well as sexuality have contributed to women's lack of confidence in reporting violent content to social media platforms (RESURJ, n.d.). Bytes for All has reported that, in

2013, an online hate campaign urged the rape and murder of a human rights defender. She received many threats: pictures of her and her daughter as well as the addresses of her family were posted online. Shots were fired at her as well as her husband. Facebook removed the pages but the threats were again posted by a different user. Twitter took a month to act on her complaint (Houreld, 2014).

Social media use in low-resource languages face additional challenges. Most people in Pakistan communicate in Urdu, which is often presented in Roman script on social media. If a victim complains about online abuse in Roman Urdu or in the Urdu script, the content is less likely to be removed compared with complaints filed in English. Complaints in even less prominent languages such as Punjabi, Sindhi, Balochi and Pashto are even less likely to be resolved (GenderIT, 2015).

One Pakistani journalist noted: 'There is no point in us reporting anything because we know nothing is going to get done there. They operate in English, so how do you report threats in Urdu?' (Maas, 2021). Women journalists exhibited even a lower propensity to report attacks to their employer (25 per cent) or to the police (11 per cent). It was reported that most victims felt 'abandoned' by their employers when they became victims of online violence (ibid.).

3.6.5 The roles of civil society organisations

Pakistan's not-for-profit organisation, Media Matters for Democracy, which works on independent journalism and media and digital rights advocacy, expresses solidarity with the women journalists who have become the target of online violence. In August 2020, a group of women journalists released a statement complaining of 'a culture of hateful speech, incitement, harassment, and doxing' that affected their professional and personal lives. The statement highlighted that online violence originated primarily from accounts that allegedly belonged to the supporters and members of the ruling party Pakistan Tehreek e Insaaf. The journalists noted that the comments were aimed at journalists who criticised the government's policies, specifically related to the current pandemic (Media Matters for Democracy, 2020).

The Beyond the Net Funding Programme, under the Internet Society Foundation, supports projects involving the use of the Internet to empower people and transform lives. This has provided funding to create Hamara Internet, which aims to raise awareness of digital violence against women (Metri, 2016).

3.7 Singapore

3.7.1 Prevalence of victimisation and perpetration

According to Singapore's gender equality advocacy group Association of Women for Action and Research (AWARE), there were 124 cases of digital sexual violence in the country in 2018, compared with 46 in.2016. More than half of the cases in 2018 involved images, which included illicit filming, nude photo distribution and upskirting (filming/taking photographs under girls' and women's clothes) (Yi, 2019).

The use of gendered language to harass female politicians online has also been reported. When a People's Action Party member stood for parliament in 2011, she was heavily criticised online for her Facebook photo, in which she stood next to a designer handbag (Ang, 2020).

3.7.2 The regulatory situation

Singapore's Penal Code is about 160 years old, and was inherited from its colonial ruler. It was fully reviewed in 2007. However, it still lacked a specific provision making various forms of online violence a criminal matter. For instance, image-based abuse (IBA), which involves non-consensual production and distribution of intimate images, is a major category of technology-facilitated violence against women. Until recently, Singapore relied on old and outdated regulations to fight IBA and other OVAWG. For instance, sexual voyeurism cases were treated as 'insult of modesty' offences under the Penal Code 2008. Likewise, offenders who possessed or shared images were charged with making, distributing or possessing an obscene film, under the Films Act 1998. These laws were outdated with regard to addressing the new modalities of IBA facilitated by the Internet, such as the distribution of intimate images or threats to do so without consent (Vitis, 2021).

Singapore thus revised and updated its regulations to fight digital violence against women. The Protection from Harassment Act 2014 extended the definition of harassing behaviour to include

electronic means (Goh and Yip, 2014). It criminalises cyber- and other forms of harassment offline as well as stalking (Internet Society, 2017).

In order to reform the Penal Code to better address acts of technology-facilitated violence, in February 2019 the Criminal Law Reform Bill was introduced into the parliament. This was passed in May 2019, and this amended the Penal Code. The Bill noted that its purpose was to:

> '...amend the Penal Code and certain other Acts, to update the criminal offences, keep up with technological changes and emerging crime trends, enhance protection for minors and vulnerable victims, harmonise the criminal laws and update the sentencing framework' (James-Civetta, 2019).

One of the aims of the Criminal Law Reform Bill 2019 has been to recognise different forms of IBA as unique offences (Vitis, 2021).

In May 2019, Singapore's parliament passed a bill that made distributing or threatening to distribute intimate images a crime. Such a crime is punishable by up to five years in jail, a fine and caning. The bill also made 'cyber-flashing' – sending unsolicited images of one's private parts – punishable by up to one year in prison or a fine. If the recipient of such an image is younger than 14, the crime is punishable by up to two years in jail, a fine or caning (The Jakarta Post, 2019).

3.7.3 Other government actions

Singapore's second director of information policy at the Ministry of Communications and Information has noted that the country's approach has been to educate citizens so they can protect themselves as well as to raise awareness about online safety through public information campaigns (Branson, 2021).

In 2021, Singapore announced a plan to officially launch a new initiative, the Singapore Together Alliance for Action. The goal of this is to keep women and girls safe online. The country's senior minister of state for communications and information led two engagement sessions, in February and March of 2021, which were attended by more than 60 participants (Teng, 2021).

The portal Awareness, Connect, Take Precaution, or A.C.T Against Violence, launched by the Singapore Council of Women's Organisations in November 2020, provides resources for women to fight against violence and harassment (Menon, 2020).

The Ministry of Communications and Information's Cyber Security Agency has launched the website GOsafeonline. This provides tips on the safe use of social networks and resources for parents. The agency has also collaborated with the Singapore Personal Data Protection Commission to develop student activity books that aim to raise awareness on cybersecurity and personal data protection (Internet Society, 2017).

3.7.4 Public–private partnership

The government has established a public-private partnership called the Media Literacy Council (MLC). This educates the public on cyberbullying, scams, misinformation and other areas. It also advises the government on policy. In 2020, the MLC launched its Better Internet Campaign 2020.[8] A key part of this involved projects with big technology companies to promote online safety. The campaign worked with Instagram to develop a guide for parents to use the platform safely. Among the features highlighted in the guide included the importance of adding two-factor authentication measures and updating account settings to increase protection. Another project, developed with TikTok, emphasised the importance of thinking before posting (Branson, 2021).

3.8 Sri Lanka

3.8.1 Prevalence of victimisation and perpetration

About 400 cases of cyber-harassment were reported in 2020 in.Sri Lanka. They included cases of revenge pornography, blackmailing for money/sexual favours, selling videos to pornography websites, sharing of obscene photos and videos, and editing photos posted on social media websites (Fazlulhaq, 2021).

Likewise, about 200 complaints related to unauthorised dissemination of private content are made daily in the country, a majority of them from women (RESURJ, n.d.). Most incidents in the country take place on Facebook.

OVAWG is the second biggest form of gender-based violence reported in Sri Lanka. Harassment

8 www.betterinternet.sg/

by partners or spouses constitutes the majority of the complaints, with online content provided by the subject voluntarily or involuntarily used to manipulate them. Some complaints are related to the use of 'catfishing' on social media platforms, especially among girls between the ages of 14 and 18 years (SDJF, 2020).

The NGO Women In Need (WIN) notes that cyberviolence is the fastest growing form of gender-based violence in Sri Lanka. According to a WIN study in 2000, 32.5 per cent of women reported that they had friends who had been victimised by online violence. The proportion was 16.5 per cent for men (Gunasekera, 2021).

Studies by the United Nations Children's Fund (UNICEF) and the Centre for Women's Research (CENWOR), commissioned by the National Committee on Women, found that adolescent unmarried girls and young women were the main victims of online violence in Sri Lanka. Among the most common medium used by perpetrators are Internet-based communication platforms such as social media, peer-to-peer networks and mobile phones (UNDP, 2021).

According to the Criminal Investigation Department, offences in which ex-partners circulate intimate photographs and videos of girls and women with whom their relationships have come to an end account for 70 per cent of the cases dealt with (also referred to as 'revenge porn'). Images are distributed or published online without the consent of the subject. A 16-year-old girl's boyfriend circulated her nude photos on social media and the Internet when the girl ended their relationship. The girl was beaten by her brother when he received a message from an anonymous number that his sister's nude photos were circulating on social media and the Internet and he was also sent the pictures (Rodrigo, 2020).

In Sri Lanka, women are expected to fulfil the traditional roles of 'reproducers, nurturers and disseminators of "tradition", "culture", "community" and "nation"' (de Alwis, 2002). Women who go against such roles online become victims of harassment. For instance, women who post pictures on Facebook wearing western outfits such as jeans have reportedly faced abuse and harassment on the platform for not wearing a sanwara, which is viewed as respectable attire for women in the country. Perpetrators are also reported to invite other Facebook users to express their opinions on women's outfits and engage in photo-sharing competitions. Such actions lead to further harassment and hate speech on the platform (de Costa, 2021).

3.8.2 The roles of civil society organisations and trade and professional associations

In April 2018, 13 Sri Lankan CSOs wrote an open letter to Facebook in which they expressed 'deep frustration' that the platform provides 'little to no support' to deal with content related to gender-based violence, violence against the LGBTIQ+ community and hate speech when such offences are reported. Facebook responded that it would increase content reviewers and work with government and civil society to address hate speech. The platform also promised that it would take additional measures such as training its staff to understand the local context better to identify objectionable content in local languages, especially Sinhalese. In 2021, however, the problem reportedly persisted (Wickrematunge, 2021).

Most victims reporting online violence receive no response. The main body responsible for online violence issues is the cybercrimes division of the Criminal Investigation Department. This is based in the capital, Colombo. Victims living outside Colombo thus need to travel to the capital to report offences (Wickrematunge, 2021).

A British Council-funded project focused on social media initiatives to combat OVAWG in Dikyaya village. This was a component of a broader initiative in which 37 community projects were implemented to raise awareness of VAWG.[9]

Non-profit online network iProbono, which helps connect organisations that need legal assistance with lawyers and law students, was reported to be working with the Ministry of Youth Affairs and the Ministry of Justice on measures to fight cyberbullying and to undertake reforms in the criminal law system to criminalise cyberbullying, revenge porn and cyber-harassment (Family Planning Association 2022).

The research and advocacy organisation Centre for Policy Alternatives, the feminist initiative to

9 www.britishcouncil.org/partner/international-development/track-record/vawg-sri-lanka

'support, promote and create women's voices on the internet' Ghosha and youth group Hashtag Generation started a research project in 2017 on technology-related violence against women and girls in Sri Lanka. The focus was on Facebook (Groundviews, 2018a).

3.8.3 The regulatory situation

Several sections in Sri Lanka's Penal Code can be used to address technology-based violence. Section 345 deals with sexual harassment, which is defined as the use of words or actions to cause 'annoyance or harassment to a person'. Section 372 deals with extortion, which is defined as 'the intentional act of putting another person in fear of injury, inducing a person to deliver property or valuable security'. Section 483 focuses on criminal intimidation, or 'threatening a person to act or omit an action in order to avoid some sort of punishment'.

Section 372 and Section 483 can be used to charge perpetrators who engage in blackmail to share personal photos or videos. Likewise, the Obscene Publications Act can be used to charge offenders who share personal, intimate images without the subject's consent. The acts of sharing images that have been explicitly altered using editing software can also be challenged under this Act. Section 2 of this Act criminalises the distribution or public exhibition of 'obscene' photographs as well as the possession of such photographs. The Payment Devices Frauds Act's Section 3(r) makes receiving money or goods through a payment device with intent to defraud punishable. This can be used to address cases involving online blackmail of women. The Computer Crimes Act's Section 7 makes obtaining information from a computer without the owner's permission an offence. It can be used to charge perpetrators who download, upload or make copies of illegally acquired content. There are thus many pieces of legislation, regulations and acts in place to fight OVAWG. However, most women victims choose not to pursue the perpetrators of online offences as a result of flaws in the system of reporting online violence to law enforcement authorities (de Sayrah, 2017).

3.8.4 Law enforcement and the judiciary

Victims who had reported instances of leaked intimate images complained about the insensitivity of officers handling their cases; this can lead to further trauma and create feelings of apprehension. The officers involved were reported to have discussed survivors' cases in a casual way and exhibited a tendency to implicitly shame victims for sharing content online. Consequently, fewer victims report their cases (Groundviews, 2018b).

Most local police stations lack the capacity and expertise to handle cyberbullying cases. In 2020, a Standard Operating Procedure was introduced for the police on handling sexual harassment of women on social media. The procedure was introduced by WIN and other agencies handling harassment of women, such as the police Cyber Crimes Unit and Children and Women's Bureau, the Criminal Investigation Department, the Sri Lanka Computer Emergency Readiness Team (SL CERT) and the Telecommunication Regulatory Commission. The pandemic disrupted the operation of these efforts. They were planned to be relaunched in 2021. In February 2021, training for officers of the Children and Women's Bureau desks started in the Western Province (Fazlulhaq, 2021).

3.8.5 Victims' response

Most victims of OVAWG do not report their cases because they do not know how to file complaints. Others fear that their personal details and content will be exposed (Fazlulhaq, 2021). Some victims have filed complaints with the SL CERT, which has reportedly asked them to report directly to Facebook. This is viewed as an ineffective solution since Facebook lacks the capacity to moderate posts in local languages (RESURJ, n.d.).

While Internet companies have introduced methods of reporting and removing online violence-related contents, especially unauthorised dissemination of private content, various challenges have been reported in utilising such services (RESURJ, n.d.).

Language has been a major barrier in reporting incidents related to online harassment and violence. Social media platforms such as Facebook especially lack support when offensive content in local languages such as Sinhalese and Tamil is reported (Wickrematunge, 2019).

3.9 Discussion of findings from the country-level cases

In general, regulations in Commonwealth Asia member countries have been slow to catch up and respond to the circumstances facing the victims of OVAWG. National legislation is mostly silent on the issue of harm caused by bystander participation to the victims of OVAWG. Some countries have not even enacted laws to deal with cybercrime, and data protection and privacy. Criminalising bystander acts to minimise OWAVG has been an even lower legislative priority. Congestion in law enforcement and judiciaries as a result of a shortage of human resources and lack of training is an even bigger challenge.

In some Commonwealth member countries, efforts to minimise online violence and victimisation have been directed at offences that target children. For instance, the Telecommunications Authority of Maldives asks ISPs to block CSAM content if a website is found to contain this. In this way, bystanders do not have the opportunity to act in a way that further victimises the target of online violence. This practice protects children from online violence but not young adults and women in general.

Some countries have special legal provisions that recognise the higher levels of online violence that women face. For example, in India, the IPC's Section 354D is used to prosecute perpetrators of cyberstalking and bullying if the victim is a woman; it is not used for a male victim. Most other Commonwealth Asia member countries lack such provisions. On the law enforcement front, more women are being recruited to handle OVAWG at national and sub-national levels in Bangladesh, India and Pakistan. Best practice models such as these need to be considered when enacting new legislation to deal with online violence and developing law enforcement capacities.

An encouraging aspect is that Commonwealth Asia member countries are also copying best practices from others in the region, which can reduce the impacts of the acts of perpetrators and bystanders for some types of OVAWG. For instance, the Telecommunications Authority of Maldives considers Singapore a role model for best practices in dealing with CSAM online. The Broadcasting Act of Singapore has given the Infocomm Media Development Authority (IMDA) power to direct Internet content providers to remove and block prohibited material such as violent content that can be accessible by children and youths. The IMDA can also require that ISPs block access to websites that contain such content. ISPs are also required to offer Internet parental control services to their subscribers, which can be used to manage children's access to websites and online services (Government of Singapore, 2021).

Meanwhile, some countries that are implementing aggressive regulations against some forms of online violence have faced criticism. For instance, Singapore's law against cyberbullying (the Protection from Harassment Act 2014) has been criticised on the grounds that children are often the perpetrators of cyberbullying. By criminalising children, the law becomes inconsistent with children's right to freedom of expression (Internet Society, 2017). If actions of bystanders (secondary perpetrators) in cyberbullying are criminalised, more children and young adults are likely to face criminal charges. This concern is especially valid in settings where teenagers account for a large proportion of perpetrators, both primary and secondary. For instance, the majority of cyberbullying perpetrators in Bangladesh are teenagers. Informal institutions such as family and other social networks and resources within institutions, such as teachers or counsellors can play a key role in fighting such offenses.

While several CSOs and NGOs have been engaged in issues related to OVAWG, these interventions lack explicit focus on the role of bystander participation. The only exception is Breakthrough India's social media campaign Dakhal Do, which is promoting bystander intervention to stop such violence in private and public spaces. Bystanders possess significant potential power to inhibit criminal acts (Staub, 1990). From a victim's perspective, asking bystanders for help could be an effective way to reduce or mitigate risks related to OVAWG. However, seeking bystander intervention has not been a part of most victims' strategy.

4. Discussion, conclusion and recommendations

4.1 Online technologies stimulating more violence against women and girls

The rapid growth of the Internet, especially social media, has encouraged the emergence of violent behaviours, with women and girls are disproportionately affected. Gul Bukhari of Bytes for All notes: 'These technologies are helping to increase violence against women, not just mirroring it. A lot of the crime we are witnessing would not have been possible without the use of these technologies' (in Houreld, 2014).

The cases of Malaysia and Maldives suggest that women are harassed online for simple things such as the way they dress or their external appearance (Moosa, 2019). In some of the countries covered in this report, many high-profile OVAWG cases are perpetrated by supporters of the political party ruling the country.

For instance, social media platforms' algorithms are designed to exploit users' habits and interests. The match between a person and content delivered is based on the person's preferences as determined by algorithm. Very little consideration is given to whether the content is harmful to certain groups or inaccurate. Some politicians and civil rights activists have argued that technology firms need to be held accountable for amplifying online violence (Zakrzewski, 2022).

It is important to invest in 'social, legal and practical tools' for women and girls to protect themselves from online violence (Article 19, 2016). In order to make victims of OVAWG feel safe in coming forward, the support of family members, law enforcement agencies and other relevant actors is critical.

Measures should be taken at various levels so that victims of OVAWG can put the experience behind them and take back control of their lives. In order to achieve this, as prior research in criminology and criminal justice has shown, victims need to feel they have been treated fairly (Wemmers and Cyr, 2005).

Measures and initiatives need to be taken at various levels in order to create and improve perceptions of fairness among OVAWG victims. For instance, at the national level, it is important to undertake legal reforms and improve complaints handling processes (Article 19, 2016).

Mental health issues such as suicide and depression among OVAWG victims are likely to worsen when passive bystanders witness their suffering and do nothing (The Conversation, 2018). Bystanders thus play a key role in instilling a feeling of fairness among OVAWG victims. Bystander interventions and other types of collective actions can help empower victims to 'fight back' against online violence (UN Women, 2020). While bystanders have no legal obligation to stop a wrongful online act, when they view and re-transmit violent content without the consent of the subject their actions can perpetuate OVAWG (ibid.).

4.1.1 Institutionalisation issues in interactive social media behaviours

With respect to violent online content, interactive social media behaviours such as 'liking' and sharing content are at a nascent stage of institutionalisation. Institutionalisation is defined as the process by means of which a practice acquires legitimacy and achieves a taken-for-granted status (Kshetri, 2009b).

It is important to understand a wide range of actors' perceptions of interactive social media behaviours with respect to violent online content and the complex process of negotiation and interaction among them. Institutional theory frames this process as the evolution of an institutional field. Note that a field is 'formed around the issues that become important to the interests and objectives of specific collectives of organizations' (Hoffman, 1999).

Institutional fields evolve constantly and thus are not static in nature (Hoffman, 1999). Regarding the evolution of fields, institutional theorists argue that a field is a dynamic system characterised

by the entry and exit of various members and constituencies with competing interests and disparate purposes and a change in interaction patterns among them (Barnett and Carroll, 1993). For a field formed around interactive social media behaviours, the members include regulatory authorities, law enforcement agencies, technology firms such as social media platforms, international institutions (e.g., UNDP), CSOs such as Pakistan's DRF and Sri Lanka's WIN, Internet users and the general public. As is the case for any issue-based field, these field members continuously negotiate over issue interpretation and engage in what is referred to as 'institutional war', leading to institutional evolution (ibid.). The 'content, rhetoric, and dialogue' among the field members influence the nature of intellectual property rights diffusion and institutionalisation (Hoffman, 1999).

Prior research indicates that institutional evolution entails a sequence of evolutionary development among the three institutional pillars – regulative, normative and cognitive. Building a regulative/law pillar system is the first stage of field formation. For instance, a regulative/law pillar related to interactive social media behaviours is considered to be formed if posting and sharing violent content become a criminal offence. According to Hoffman (1999), it is followed by the formation of normative institutions, which view responsible interaction with violent online content as an ethically appropriate behaviour. Finally, cognitive institutions are formed, which means that responsible interaction with violent online content becomes a culturally supported belief.

4.2 The vicious circle of OVAWG

The characteristics and actions of perpetrators, victims and law enforcement agencies have a reinforcing effect on each other, leading to a vicious circle of OVAWG.

4.2.1 Law enforcement agencies

There are serious law enforcement challenges in addressing offences related to OVAWG. First, agencies such as police forces are inexperienced with these new forms of crimes. OVAWG investigations are highly complex as well as resource- and expertise-intensive.

Unsupportive attitudes and an unwillingness to help victims have contributed to a low reporting rate of cyberbullying and other OVAWG cases (Roy, 2015) as well as cybercrime incidents in general (Anand, 2011). Most countries covered in this report do not investigate all reported OVAWG.

Among reported cybercrimes, arrest rates are very low. Arrest entails identifying the pool of potential suspects and narrowing it down by eliminating those who are innocent. The structure of cybercrimes makes it difficult to identify this pool.

The conviction phase, which requires proof beyond reasonable doubt, is equally complex. Difficulties related to furnishing documentation and proof to establish that an offence has been committed compound the problem. Additionally, OVAWG's newness presents a challenge to the court system.

Some OVAWG offences have international and cross-border implications and consequences. An example of this is Indian YouTube channel Liberal Doge's virtual 'bids' on Pakistani Muslim women during Eid 2020 (Kamdar, 2021). Local police forces in most countries are unequipped to deal with the global nature of OVAWG. National boundaries have thus created serious obstacles for law enforcement agencies. Collaboration and co-operation among agencies in different jurisdictions can help but are far from sufficient.

4.2.2 Victims

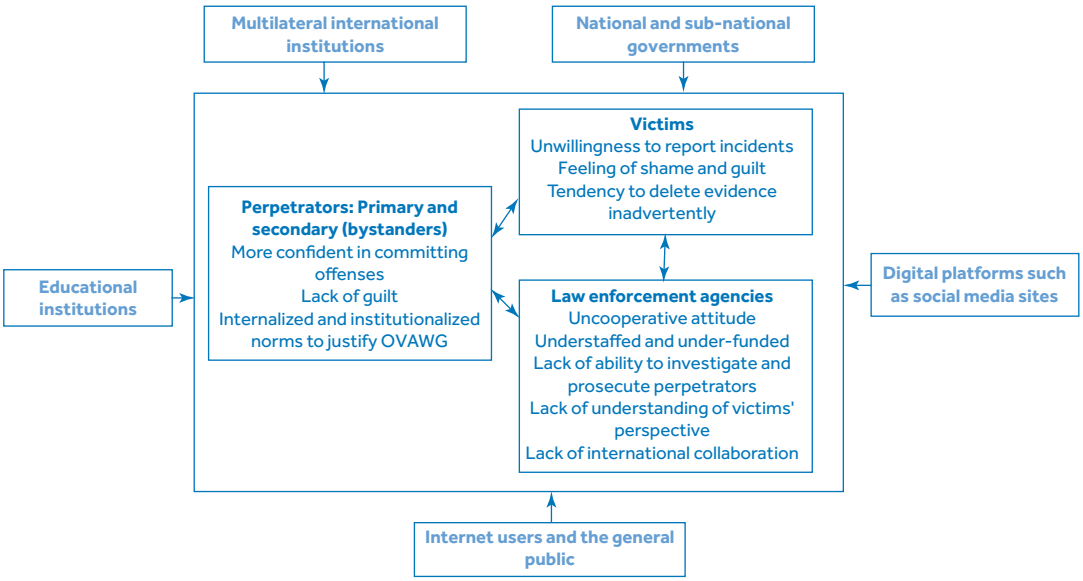
The weakness of defence mechanisms increases the likelihood of attacks. Although some weaknesses are technological, others are behavioural or perceptual in nature. According to a 2013 Pew Research Center survey, 40 per cent of young Facebook users and 64 per cent of teen Twitter users did not activate privacy settings on their social media accounts (Madden et al., 2013). It is also important to avoid interaction with bullies by logging off social media websites or 'blocking' bullies.

As noted above, only a small proportion of OVAWG is reported to law enforcement agencies. In general, cybercrimes are among the most underreported forms of criminality. Law enforcement agencies' inability to solve OVAWG incidents reinforces victims' unwillingness to report such crimes, which, in turn, further encourages OVAWG perpetrators.

4.2.3 Perpetrators (primary and secondary)

Law enforcement agencies' inability to solve OVAWG incidents reinforces perpetrators' confidence. Increased success is making OVAWG

Figure 4.1. The vicious circle of OVAWG



perpetrators more brash and more disrespectful of law enforcement agencies. Moreover, from the perspective of perpetrators, when the victims are 'Others', OVAWG is likely to entail less guilt and more enjoyment. The result is likely to be higher numbers of such offences, more serious offences and offences that are more difficult to solve (e.g., victimising women and girls from other countries). All this leads to further inefficiency and congestion in the law enforcement system.

4.3 Mechanisms for combating OVAWG

Without appropriate measures to combat cybercrimes, the vicious circle's elements reinforce each other and lead to public distrust of law enforcement agencies and increased confidence among OVAWG perpetrators, resulting in more and more serious offences. In order to break this circle, micro- and macro-level measures combining policy, technological and non-technological fixes are needed at various levels.

Figure 4.1 presents key actors who can intervene and overcome existing barriers to fight against OVAWG.

4.3.1 Multilateral international institutions

Multilateral international institutions such as UNDP can play a key role in fighting OVAWG. The UNDP's HackaDev initiative (the National Youth Social Innovation Challenge) in Sri Lanka aims to help alleviate and prevent cyberviolence affecting youth of all genders in Sri Lanka. The HackaDev Learning and Skills Academy established by UNDP Sri Lanka aims to respond to the 'need of imparting knowledge, building skills and changing mindsets'.[10]

In partnership with UNDP, Sri Lankan startup Team Cyberwarders created a mobile application Cyber Care, which was launched on World Safer Internet Day, 9 February 2021. Team Cyberwarders had successfully completed the incubation phase of HackaDev, which is a crowd-sourcing exercise for sustainable development solutions. The app aims to raise awareness on cyberviolence and help fight online hate faced by young people in Sri Lanka. It includes relevant laws and regulations related to cybercrimes in Sri Lanka. It uses interesting gaming features to increase awareness of and learning about cyberviolence. It provides important information on victims, authorities and organisations engaged in assisting victims. It also provides news on incidents relating to cyberviolence (UNDP, 2021).

Multilateral institutions have also conducted studies and shared recommendations to fight OVAWG. Based on studies in Sri Lanka, UNICEF and CENWOR highlighted the need to increase awareness on prevention of and responses to cyberviolence (UNDP, 2021). Meanwhile, UNICEF in Maldives has emphasised the importance of 'engaging children and parents to ensure the

10 www.hackadev.lk/academy/

internet is a safe place for all children' (Munavvar, 2020). Additionally, though, UNICEF has noted that, while Maldives has launched awareness-raising campaigns, these do not focus on the behaviour of the perpetrator. Nor do they emphasise the criminal nature of blackmail and child pornography. UNICEF has recommended that new awareness campaigns be launched to focus on prevention by addressing perpetrator behaviour online (UNICEF, 2016).

4.3.2 National and sub-national governments

National and sub-national governments should take measures to strengthen regulations and enforcement infrastructure by enacting and implementing stronger cybercrime, and privacy and data protection laws. It is also important to ensure that existing laws on gender-based violence are effectively applied to OVAWG (Brudvig, 2019).

In addition, it is important to revise and adjust protocols, codes and laws to address the increase in OVAWG. Issues related to secondary perpetration, whereby bystanders help perpetuate online violence by downloading, forwarding and sharing content created and uploaded by principal perpetrators, are unique to cyberspace. Secondary perpetrators disregard or are ignorant of the fact that the violent content has been disseminated without the subject's consent. Bespoke laws are thus needed to address secondary perpetration and other issues related to OVAWG. A study on ICT VAWG conducted by UN Women in 2019 in five Asian countries (including three Commonwealth member countries – India, Malaysia and Pakistan – as well as the Philippines and the Republic of Korea) found that, while the countries had established courts and trained investigators and prosecutors for ICT-related offences, they lacked specialisation in ICT VAWG (UN Women, 2020). It is thus critical to provide training to investigators and prosecutors to deal with OVAWG.

Civil society advocates have also emphasised the importance of enacting new regulations that require perpetrators to take down harmful content. Additional sanctions may include 'apology, restitution, compensation and ways to assist victims/survivors to rebuild their lives and online presence'. The goals of such punishments should also be to 'prevent recidivism, deter others and rehabilitate the perpetrator'. Depending on the harm and gravity of ICT VAWG, ICT intermediaries can also implement sanctions that can include 'apology, suspension and banning from the platform' (UN Women, 2020).

Regarding harmful content, the question of whether social networking sites should play the role of gatekeeper for the information their users consume is arguably more philosophical than technological (Ohlheiser, 2017). In light of the adverse social consequences of OVAWG, it is important to challenge this philosophical position and enact strict laws to ban content that promotes OVAWG.

Regulators should also look to the moves in some jurisdictions towards stricter laws and regulations to discourage cyberbullying activities. For instance, in Michigan state of the US, a 'pattern of repeated harassment' is a felony that carries a penalty of up to five years in prison, and a $5,000 fine (Devito, 2018). Likewise, in the Netherlands, cyber-offenders who engage in cyberbullying and harassment may face a prison sentence of up to 10 years. In 2018, a Dutch appeals court upheld this maximum prison sentence for a convicted cyberbully (Associated Press, 2018).

Efforts should be directed towards collecting and disseminating meaningful data and information concerning OVAWG. In the cases of Brunei Darussalam and Maldives, for instance, the data have not been disaggregated by gender.

Creation of informal networks to fight cross-border OVAWG:

One possibility to fight against cross-border online crimes is to form informal networks of law enforcement agencies. Informal networks and agreements among states and transnational actors are becoming an important feature of world politics (Lipson, 1991). Such networks are found in areas such as financial markets, aviation, antitrust, data privacy, pharmaceuticals and the environment. State and sub-state officials from a number of countries work together to share information with each other, develop harmonised guidelines and best practices, and reduce friction associated with globalisation (Bach and Newman, 2010).

Public–private partnership:

The public and private sectors' different strengths, expertise and experience could lead to complementary roles in meeting developmental and social needs (Linder, 1991). A unique strength of the state is its ability to impose harsh sanctions

and penalties on violators of laws and regulations. The state is thus in the best position to fight criminal conducts related to OVAWG, such as hate crimes.

Private sector players such as social media platforms, on the other hand, often have technical expertise and resources to fight OVAWG. Also, the private sector controls most online communication technologies. These platforms can play a key role in addressing acts that do not necessarily break existing laws, such as hate speech based on gender. For instance, they can provide guidance for safe bystander interventions (UN Women, 2020). States, ICT intermediaries and CSOs can thus work together to fight various forms of OVAWG such as hate speech.

Already, there has been some work in this direction in some countries. For instance, the Government of Singapore has established the public-private partnership MLC, which educates the public about cyberbullying, scams, misinformation and other issues. It also advises the government on policy. In September 2020, Pakistan's FIA announced that it had started collaboration with Facebook to obtain data related to cybercrimes against women and children (The International, 2020).

4.3.3 Educational institutions

Educational institutions such as schools and universities, where a high proportion of cyberbullying acts take place, should also develop strategies for addressing such offences in the institutions (Cantone et al., 2015). It is important to examine how cyberbullying may be related to the general social climate in the institution and focus on revisiting and addressing relationships, environments, and policies and practices in order to reduce perpetration and victimisation (ibid.). For instance, in the state of Illinois in the US police officers assigned to protect schools, known as school resource officers, are required to undergo training focused on cyberbullying (5 Chicago, 2018).

Educational institutions also need to invest in technological solutions such as monitoring or blocking software to detect cyberbullying activities on school networks (Page, 2006). They need to teach students about cyberbullying's psychological and legal implications and show them cases of cyberbullying (Clifford, 2012). To take an example, Seattle Public Schools participated in a pilot programme with iCanHelpLine.org in which subscribers can discuss issues related to student cyberbullying on social media. iCanHelpline.org works with social media organisations such as Instagram, Snapchat and Twitter to delete content (Seattle Public Schools, 2017).

4.3.4 Digital platforms such as social media sites

Victims of OVAWG have complained that reporting mechanisms are often available only in English, and reporting guidelines lack transparency. There has also been limited reporting of the same perpetrators on multiple platforms.

Technology firms should take measures to increase transparency in reporting mechanisms, and should make reporting accessible to a broader audience. It is also important to build stronger networks with policy-makers and NGOs to provide counselling and other support services to victims, and identify perpetrators (Quilt.AI and ICRW, 2021).

4.3.5 Internet users and the general public

Internet users, especially social media users, and the general public can take various actions to avoid being victimised and fight OVAWG, depending on the context and their roles. Technological and behavioural measures can effectively reduce perpetration and victimisation, especially among youth. Some technology companies have developed advanced technological tools and solutions to fight cyberbullying. Credit report and identity theft protection company Identity Guard uses artificial intelligence to monitor social media feeds to identify behaviours that can be considered cyberbullying. It utilises IBM Watson to enable 'natural language processing' and 'natural language classifiers'. Complex algorithms identify potential cyberbullying instances and send alerts to parents. These alerts also include screenshots with dates and times of related content that triggered the warnings. Parents are then guided to resources such as relevant laws and school policies so they can respond effectively (Elosua, 2018)

Behavioural measures include the use of assertiveness or humour and avoiding interaction with the bullies (e.g., by logging off a social media website or 'blocking' bullies). Victims also need to seek help from a parent, caretaker or teacher (Cross et al., 2016).

Parents and caregivers can also play a key role in helping children deal with cyberbullying. It is

important to teach young people various strategies to respond to this issue. One study found that 'authoritative' parents who listen to their children and provide guidance can help reduce the impacts of cyberbullying (Baird, 2010). It is also important to seek bystander intervention to reduce or mitigate an offence related to OVAWG.

Internet users can provide pressure to social media platforms by demanding actions to minimise OVAWG as a part of corporate social responsibility (Avlon, 2017). Such pressures need to focus on the actions of primary perpetrators but also secondary perpetrators (bystanders).

The seriousness of this issue has led to the emergence of new forms of cyber-insurance to protect against cyberbullies. Insurers such as AIG and the Arbella Insurance Group cover for cyberbullying, including costs incurred after a cyberbullying attack such as those associated with legal expenses, temporary relocation expenses and private tutoring. AIG's new product Family CyberEdge includes coverage for one year of psychiatric services if a family member is victimised by cyberbullying. Also covered is lost salary if the victim loses a job within 60 days (Kshetri, 2018).

4.4 Bystanders' actions leading to further victimisation in OVAWG: Motivations and measures to fight against and discourage such actions

As mentioned, bystanders' actions lead to further victimisation in OVAWG. This section addresses the questions of why online bystanders choose acts that victimise women and girls and what measures can be taken to fight against and discourage such acts.

In most cases, bystanders encourage perpetrators (Staub, 1990). This is especially true in OVAWG. Many people who are viewed as bystanders do not simply view or watch OVAWG incidents without doing anything. For instance, if a viewer clicks 'Like' on a Facebook page, this means that they agree with what has been suggested in the post (Maynard, 2019). In this way, the viewer provides legitimacy to the primary perpetrator's action. By recklessly downloading, forwarding and sharing violent content, these bystanders are actively participating in activities, helping continue or worsen the victimisation.

In general, an offence (crime) is committed if:

$$M_b + P_b > I_c + O_{1c} + P_c + O_{2c}\pi_{arr}\pi_{con} \quad (1)$$

where

M_b = the monetary benefits of committing the crime;

P_b = the psychological benefits of committing the crime;

I_c = direct investment costs;

O_{1c} = opportunity costs to engage in crime;

P_c = psychological costs of committing a crime;

O_{2c} = monetary opportunity costs of conviction;

π_{arr} = the probability of arrest;

π_{con} = the probability of conviction.

The product term on the right side in the equation: $O_{2c}\ \pi_{arr}\ \pi_{con}$, is also referred to as the expected penalty effect. Legislative and law enforcement actions would affect this term.

Offenders in OVAWG do not engage in such activities for monetary benefits. Thus, $M_b = 0$. It can be assumed that the engagement in such an offence normally **is not their full-time** job ($O_{1c} = 0$) and no investment is needed ($I_c = 0$).

Equation (1) in the context of OVAWG can be written as:

$$P_b > P_c + O_{2c}\pi_{arr}\pi_{con} \quad (2)$$

In equation (2), the actions of victims and civil society actors would affect P_b and P_c.

Equation (2) is applicable for cell [I] in Table 4.1.

If the existing laws do not criminalise certain bystander acts, the expected penalty effect ($O_{2c}\ \pi_{arr}\ \pi_{con}$)=0. In this case, an offence is committed if:

$$P_b > P_c \quad (3)$$

Equation (3) is applicable for cell [II] in Table 4.1.

4.4.1 Stigmatising bystanders

One way to reduce OVAWG would be to stigmatise bystanders. In this context, to understand the roles of the various players and constituencies, a central concept is arbiter. The theories of

socially situated judgement (Kahneman, 2003) maintain that 'constituent-minded sensemaking' of key intermediaries or arbiters influences the stigmatisation process. Three categories of arbiters – social, legal and economic – have been identified (Wiesenfeld et al., 2008), which include the key actors presented in Figure 4.1 above.

Social arbiters:

Social arbiters include members of the press, governance watchdog groups, academics and activists. So far, bystanders' actions have received very little explicit attention from various groups of social arbiters. Efforts of these actors need to focus on making bystanders understand that their behaviours lead to physical and psychological suffering, which can increase the psychological costs (P_c) of engaging in actions that amplify victimisation.

Legal arbiters:

Legal arbiters are those who play a role in enforcing rules and regulations. Law enforcement agencies and government agencies could be legal arbiters that enact and enforce rules and regulations but fighting OVAWG is a low-priority area for them. There are complaints that law enforcement officials in some countries stigmatise victims of OVAWG instead of punishing perpetrators. Stigmatisation of bystanders is given even lower priority. There is little or no law enforcement against bystanders.

The enactment of appropriate legislation to criminalise bystander acts that worsen the victimisation in OVAWG and the improvement of law enforcement and judicial systems could change bystanders' cost-benefit calculus regarding engaging in such acts. In Table 4.1, criminalisation of bystanders' acts moves bystanders' position from cell [II] to cell [I] and adds additional costs into the equation: the expected costs of legal punishment. With the enactment of such regulations, an individual who recklessly downloads, forwards and shares violent content is viewed as a 'guilty bystander' (Raffles, 1992). By improving law enforcement and judicial systems, the probability of arrest (π_{arr}) and the probability of conviction (π_{con}) can be increased, which increases the costs of recklessly downloading, forwarding and sharing violent content.

There is a need to improve empathy and understanding of women victims among the currently male-dominated law enforcement in most countries. Some countries have increased the amount of female law enforcement officials in handling OVAWG cases, which can be seen as a positive step (cell [III] in Table 4.1).

Economic arbiters:

Economic arbiters make decisions about engaging in economic exchange with individuals. The business models of social media companies such as Facebook are based on users' engagement, interaction and content consumption. The more users read, click, share and engage with content, the more profit there is. Consequently, relatively less emphasis is placed on controlling bystanders' activities that lead to increased victimisation. If social media platforms remove OVAWG content as soon as possible, negative effects on victims associated with the actions of primary perpetrators and bystanders can be minimised. A complaint is that, when women victims report abuse on social media platforms, the most common response is that the action reported does not 'violate their community standards'. When one journalist reported death threats on Instagram in 2018, she received the same initial response. The threat clearly violated the guidelines of Instagram, which stated that 'serious threats of harm to public and personal safety aren't allowed. This includes specific threats of physical harm' (Salim, 2018). Social media platforms thus need to follow their own standards and guidelines. They should also provide guidance for safe bystander interventions (cell [III] in Table 4.1).

4.5 Increasing women's participation in ICT fields

The discussion in this report makes it clear that social media platforms lack sufficient mechanisms to prevent OVAWG. Designs of such platforms require a trade-off between privacy/cybersecurity and usability. Female cybersecurity professionals can make better-informed decisions about such trade-offs for products and services that are targeted at female Internet users. For instance, apps such as Cyber Care, launched by Sri Lankan startup Team Cyberwarders, can be made more effective in fighting OVAWG by including more women and girls in the development team.

Women are highly underrepresented in science, technology, engineering and mathematics (STEM) fields and particularly in the field of cybersecurity.

Table 4.1. Measures to be taken by various actors to prevent bystander effects in OVAWG

	Criminal acts related to OVAWG ($P_b > P_c + O_{2c}\ \pi_{arr}\ \pi_{con}$)	OVAWG acts that do not necessarily break existing laws ($P_b > P_c$)
Why bystanders engage in such acts	**[I]** • Expected psychological benefits of the banned behaviour exceed the **expected costs of legal** punishment plus psychological costs of victimising the target • May not realise their acts break existing laws	**[II]** • Psychological benefits exceed psychological costs • May not understand the seriousness of the impact on the victim
Roles of arbiters and victims to discourage bystander behaviours that lead to and/or amplify OVAWG	**[III]** • Law enforcement agencies and government agencies: strictly enforcing rules and regulations • Victims: preserving evidence	**[IV]** • Governments: revising laws to criminalise bystander acts • Digital platforms such as social media sites: providing guidance for safe bystander interventions • Internet users and the general public: (i) engaging in responsible use of social media; (ii) stepping forward as immediate responders to support the victims (criticising offensive content); (iii) refraining from sharing, liking and commenting positively on the content • Victims: seeking help from bystanders

While data for specific countries studied in this report are not available, women account for only 10 per cent of the cybersecurity workforce in the Asia-Pacific region. The societal view is that internet security is 'a job that men do'. While this is a worldwide phenomenon, it is particularly pronounced in Asia. A study conducted in Singapore that focused on female leadership in STEM fields found that the Confucian culture emphasised the roles of men as household providers. Women are thus highly underrepresented in the STEM fields (Ceia, 2021).

More efforts should be made to increase women's participation in technology fields, particularly in cybersecurity. Some industry groups have collaborated with big companies in this regard. In 2018, Microsoft India and the Data Security Council of India launched the CyberShikshaa programme, in order to create a pool of skilled female cybersecurity professionals (Kshetri, 2020). Other countries can benefit by implementing similar programmes.

4.6 Concluding comments

Micro- and macro-level measures combining technological and nontechnological fixes are needed to combat OVAWG. At the macro level, developing national technological and human resource capabilities, enacting new laws, promoting a higher level of industry–government collaboration and pushing for international co-ordination are critical to combating cybercrime.

Formal and informal institutions in most Commonwealth Asia member countries have created a fertile ground for OVAWG. In some cases, victims of OVAWG are further subjected to ill treatment by groups of actors such as family members and law enforcement agencies.

It is important to develop and implement global, regional and national action plans. Commonwealth Asia member countries are also characterised by a high degree of heterogeneity in laws to deal with OVAWG, such as cybercrime laws and data privacy laws. Stronger cybercrime laws and data privacy laws must be enacted and properly enforced to prevent this form of violence.

There is a special need for bespoke laws for OVAWG because women are the main targets of online violence in the countries studied. This is especially true for women with voices, such as journalists and politicians. In the absence of comprehensive laws, courts' judgments are likely to depend on individual judges' discretion, and the punishments for OVAWG are likely to be unpredictable and unclear.

Increased preparedness of law enforcement officials to deal with OVAWG is key in fighting the problem. Investing in training of law enforcement authorities could enhance such preparedness and nations' abilities to fight OVAWG. It is also important to increase industry–government collaboration. Since some perpetrators victimise women and girls in foreign countries, international collaboration and co-operation in law enforcement is also needed to address such offences.

In the conventional world, research has indicated, the time it takes a victim to report a crime is one of the most important factors in increasing the probability of arrest. This is especially important for offences for which preserving evidence is critical for a successful prosecution. For many OVAWG offences, successfully prosecuting offenders may require victims to preserve physical as well as digital evidence. It is thus important to report OVAWG incidents to law enforcement authorities as soon as possible.

It is important to help the victims of OVAWG adapt to the normal practice of engaging in social media activities by accepting the risks. The support of key actors such as bystanders, family members, social networks and law enforcement agencies is critical for victims to be able move into the world as survivors. Increased collaboration among diverse actors such as national policy-makers, law enforcement agencies, international developmental institutions, ICT intermediaries, researchers, educational institutions and survivors is needed to counter OVAWG.

Bystanders are key actors in helping stop OVAWG. In OVAWG incidents, the presence of active bystanders who step forward as immediate responders to support the victims (e.g., by criticising their offensive social media posts) can reduce a perpetrator's intrinsic motivation to engage in such offences. On the other hand, bystanders may encourage perpetrators' actions by sharing, liking and commenting positively on the content.

Finally, while many programmes have been implemented to educate adolescents and young adults as well as women, teachers and parents about the risks associated with online violence and ways to protect themselves, much less attention has been devoted to educating potential perpetrators about the potential risks they face when they engage in online violence. It is important to implement education and awareness-raising programmes targeted at primary perpetrators as well as secondary perpetrators (bystanders) focusing on the potential legal risks they face as well as the moral and ethical aspects of OVAWG. As discussed with reference to Singapore's law against cyberbullying, criminalising children can lead to adverse social consequences. Thus, instead of creating a legal remedy for the victims of cyberbullying, schools and parents can play a vital role in teaching moral and ethical values to reduce cyberbullying.

References

5 Chicago (2018) 'Illinois School Resource Officers to Undergo Training'. 20 August. www.nbcchicago.com/news/local/illinois-school-resource-officers-to-undergo-training/155653/

Abassi, S. (n.d.) 'The Unsocial Media: Is Online Abuse Silencing Women in Pakistan?' www.geo.tv/latest/225431-the-unsocial-media-is-online-abuse-silencing-women-in-pakistan

Advani, P. (2021) 'In This Digital Era, India Needs New-Age Policing to Protect Women From Crime'. 5 January. https://scroll.in/article/982718/in-this-digital-era-india-needs-new-age-policing-to-protect-women-from-crime

Aguilar-Millan, S., J.E. Foltz, J. Jackson and A. Oberg (2008) 'The Globalization of Crime'. *Futurist* 42(6): 41–50.

Akter, F. (2018) 'Cyber Violence Against Women: The Case of Bangladesh'. GenderIT, 17 June. https://genderit.org/articles/cyber-violence-against-women-case-bangladesh

Aljazeera (2020) 'Bangladesh Launches All-Female Police Team to Fight Online Abuse'. 17 November. www.aljazeera.com/news/2020/11/17/police-in-bangladesh-launch-all-woman-team-to-fight-digital-abuse

Allcott, H. and M. Gentzkow (2017) 'Social Media and Fake News in the 2016 Election'. *Journal of Economic Perspectives* 31(2): 211–236.

Amnesty International (2020) 'New Study Shows Shocking Scale Of Abuse On Twitter Against Women Politicians In India'. 23 January. www.amnestyusa.org/press-releases/shocking-scale-of-abuse-on-twitter-against-women-politicians-in-india/

Anand, J. (2011) 'Cybercrime up by 700% in Capital'. *Hindustan Times*, 8 October. www.hindustantimes.com/India-news/NewDelhi/Cyber-crimeup-by-700-in-Capital/Article1-766172.aspx (Accessed 12 January 2012)

Anderson, M. (2018) 'A Majority of Teens Have Experienced Some Form of Cyberbullying'. Pew Research Centre, 27 September. www.pewinternet.org/2018/09/27/a-majority-of-teens-have-experienced-some-form-of-cyberbullying/

Ang, K. (2020) 'Singapore's Record 40 Female Candidates Change Election Discussion'. Nikkei Asia, 9 July. https://asia.nikkei.com/Politics/Singapore-election/Singapore-s-record-40-female-candidates-change-election-discussion

Article 19 (2016) *Women Journalist's Digital Security*. Nairobi: Article 19. www.article19.org/data/files/medialibrary/38757/Women-Journalist's-Digital-Security-Kenya-2016.pdf

ASEAN (Association of Southeast Asian Nations) (2016) 'ASEAN Regional Plan of Action on the Elimination of Violence Against Women (ASEAN RPA on EVAW)'. www.asean.org/wp-content/uploads/2012/05/Final-ASEAN-RPA-on-EVAW-IJP-11.02.2016-as-input-ASEC.pdf

Associated Press (2018) 'Dutch Court Upholds Maximum Sentence for Cyberbully'. 14 December. https://calgary.citynews.ca/2018/12/14/dutch-court-upholds-maximum-sentence-for-cyberbully/

Avlon, J. (2017) 'How Corporate Citizens Can Stop Fake News and Hate News—and Help Save Quality Journalism in the Process'. *The Daily Beast*, 1 May.

Axelrod, R. (1997) *The Complexity of Cooperation*. Princeton, NJ: Princeton University Press.

Ayyub, R. (2018) 'I Was the Victim of a Deepfake Porn Plot Intended to Silence Me'. *Huff Post*, 27 November. www.huffingtonpost.co.uk/entry/deepfake-porn_uk_5bf2c126e4b0f32bd58ba316

Bach, D. and A.L. Newman (2010) 'Transgovernmental Networks and Domestic Policy Convergence: Evidence from Insider Trading Regulation'. *International Organization* 64(3): 505–528.

Baird, A. (2010) 'Best Defenses against Cyber Bullies'. *Scientific American*, 24 August. www.scientificamerican.com/article/best-defenses-cyber-bullies/

Barnett, W.P. and G.R. Carroll (1993) 'How Institutional Constraints Affected the Organization of Early U.S. Telephonies'. *Journal of Law, Economics and Organization* 9: 98–126.

BBC (2017) 'The Online Abuse Hurled at Malaysia's Muslim Women'. 21 August. www.bbc.com/news/world-asia-40337326

Berger, P.L. and T. Luckmann (1967) *The Social Construction of Reality: A Treatise in the Sociology of Knowledge*. New York: Doubleday.

Bhargava, Y. (2017) '8 out of 10 Indians Have Faced Online Harassment'. *The Hindu*, 5 October. www.thehindu.com/news/national/8-out-of-10-indians-have-faced-online-harassment/article19798215.ece

Bhat, C.S., S.H. Chang and M.A. Ragan (2013) 'Cyberbullying in Asia'. *Education About Asia* 18(2): 36–39.

Blackwell, B.S. (2000) 'Perceived Sanction Threats, Gender, and Crime: A Test and Elaboration of Power-Control Theory'. *Criminology, Beverly Hills* 38(2): 439–489.

BLAST (Bangladesh Legal Aid and Services Trust) (2017) 'Cyber Violence Booklet: Legal Actions on Cyberviolence Against Women'. www.blast.org.bd/content/publications/Cyber-violence.pdf

Borneo Bulleting (2019) 'Raising Awareness on Cyberbullying'. 30 October. https://borneobulletin.com.bn/raising-awareness-cyberbullying/

BNWLA (Bangladesh National Women Lawyers' Association) (2014) 'Survey on Psychological Health of Women'. Dhaka: BNWLA.

Branson, A. (2021) 'Collaboration, Education and Legislation: pnHow Governments Are Tackling Online Harms'. Global Government Forum, 26 April. www.globalgovernmentforum.com/collaboration-education-and-legislation-how-governments-are-tackling-online-harms/

Broadband Commission for Digital Development (2015) *Cyber Violence Against Women and Girls a World-Wide Wake-Up Call.* https://en.unesco.org/sites/default/files/genderreport2015final.pdf

Brudvig, I. (2019) 'The Great Threat to Women's Rights Online: Reflections from World Press Freedom Day'. World Wide Web Foundation, 25 May. https://webfoundation.org/2019/05/the-great-threat-to-womens-rights-online-reflections-from-world-press-freedom-day/

Bukhari, A. (2020) 'Silent Battles: How Pakistani Women Counter Harassment in Cyberspace'. *The Diplomat*, 21 October. https://thediplomat.com/2020/10/silent-battles-how-pakistani-women-counter-harassment-in-cyberspace/

Business Recorder (2018) 'FIA Receives 4,000 Complaints of Cyber Crimes from Women'. 3 August. https://fp.brecorder.com/2018/08/20180803396061/

Cantone, E., A.P. Piras, M. Vellante et al (2015) 'Interventions on Bullying and Cyberbullying in Schools: A Systematic Review'. *Clinical Practice and Epidemiology in Mental Health 11(Suppl 1 M4)*: 58–76.

Ceia, V. (2021) 'Gender and Technology: A Rights-Based and Intersectional Analysis of Key Trends'. *Research Backgrounder*. Washington, DC: Oxfam America.

Civicus (2020) 'Civil Society Group's Funds Seized in the Maldives While Women's Rights Organisation Smeared Online'. Monitor, 9 July. https://monitor.civicus.org/updates/2020/07/09/civil-society-groups-funds-seized-maldives-while-womens-rights-organisation-smeared-online/

Clifford, M. (2012) '15 Strategies Educators Can Use to Stop Cyberbullying'. InfoEd, 26 October. www.opencolleges.edu.au/informed/features/15-strategies-educators-can-use-to-stop-cyberbullying/

Coloroso, B. (2016) *Bully, the Bullied, and the Not-So-Innocent Bystander: From Preschool to High School and Beyond: Breaking the Cycle of Violence and Creating More Deeply Caring Communities*. New York: HarperCollins.

Cross, D., T. Shaw, K. Hadwen et al (2016) 'Longitudinal Impact of the Cyber Friendly Schools Program on Adolescents' Cyberbullying Behavior'. *Aggressive Behavior* 42(2): 166–180.

Csikszentmihalyi, M. (1975) *Beyond Boredom and Anxiety: The Experience of Play in Work and Games*. San Francisco, CA: Jossey-Bass, Inc.

Dasgupta, P. (2017) 'What Can Victims Of Revenge Porn In India Do To Get The Criminals Punished? A Long and Tricky Road to Justice'. *Huffington Post*, 14 July. www.huffingtonpost.in/2017/07/13/what-can-victims-of-revenge-porn-in-india-do-to-punish-the-perpe_a_23027563/

Davies, S. (2020) 'Risk of Online Sex Trolling Rises as Coronavirus Prompts Home Working'. Reuters, 18 March. www.reuters.com/article/uswomen-rights-cyber~ashing-trfn-idUSKBN2153HG

De Alwis, M. (2002) 'The Changing Role of Women in Sri Lankan Society'. *Social Research* 69(3): 675–690.

Deci, E.L and R.M. Ryan (1985) *Intrinsic Motivation and Self-Determination in Human Behavior*. New York: Plenum Press.

De Costa, M. (2021) 'Gendering Abuse on Social Media: A Study of Cyber Violence Against Women on Facebook'. *Proceedings of the 7th International Research Conference on Humanities & Social Sciences*, 22 March. https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3808961

Deloitte (2018) 'Data and Privacy Protection in ASEAN: What Does It Mean for Businesses in the Region?'. www2.deloitte.com/content/dam/Deloitte/sg/Documents/risk/sea-risk-data-privacy-in-asean.pdf

De Sayrah, A. (2017) 'Beyond the Report Button: Tackling Cyber-Violence in Sri Lanka'. Groundviews, 13 November. https://groundviews.org/2017/11/13/beyond-the-report-button-tackling-cyber-violence-in-sri-lanka/

Devito, L. (2018) 'Cyberbullying Is Now a Crime in Michigan Punishable by Jail Time'. *Metro Times*, 28 December. www.metrotimes.com/news-hits/archives/2018/12/28/cyberbullying-is-now-a-crime-in-michigan-punishable-by-jail-time

DeVries, K.O. (2021) 'The Drum Beat 796 - Silent No More: Violence against Women and Children'. The Communication Initiative Network,16 February. www.comminit.com/drum_beat_796.html

DiMaggio, P.J. (1988) 'Interest and Agency in Institutional Theory'. In Zucker, L.G. (ed) *Institutional Patterns and Organizations: Culture and Environment*. Cambridge, MA: Ballinger.

DRF (Digital Rights Foundation) (2017) 'Online Violence Against Women in Pakistan'. Submission to UNSR on Violence Against Women. https://digitalrightsfoundation.pk/wp-content/uploads/2017/12/UNSR-Submission-by-DRF.pdf

DRF (n.d.) 'Addressing Online Violence Against Women and Gender Minorities in Pakistan'. https://worldjusticeproject.org/world-justice-challenge-2021/addressing-online-violence-against-women-and-gender-minorities

Dubey, A. (2017) 'When Women Can Do What Men Can, It's Time for Men to Return the Favour!' Women's Web, 19 December. www.womensweb.in/2017/12/working-women-from-madhya-pradesh/

Duggal, P. (2004) 'What's Wrong with Our Cyber Laws?' 12 October. www.expresscomputeronline.com/20040705/newsanalysis01.shtml

Elosua, Pablo (2018) With Watson, Guardio helps parents protect kids from cyberbullying June 14, https://www.ibm.com/blogs/cloud-computing/2018/06/14/guardio-watson-cyberbullying/

Faisal, R. (2021) 'Raising Awareness on Women's Rights'. *Borneo Bulletin*, 12 April. https://borneobulletin.com.bn/raising-awareness-on-womens-rights/Family

Planning Association (2022). Ministry Of Youth and Sports Led Committee Meets To Finalize Penal Code Reforms, https://www.fpasrilanka.org/content/ministry-youth-and-sports-led-committee-meets-finalize-penal-code-reforms

Fazlulhaq, N. (2021) 'Sri Lanka "Groping in the Dark" on How to Deal with Cyber-Bullies'. *Sunday Times*, 7 March. www.sundaytimes.lk/210307/news/sri-lanka-groping-in-the-dark-on-how-to-deal-with-cyber-bullies-434821.html

FORUM-ASIA (2019) 'The Maldives: Ensure Security for Human Rights Defenders and Stop Online Harassment'. 8 February. www.forum-asia.org/?p=28079

Galtung, J. (1958) 'The Social Functions of a Prison'. *Social Problems* 6: 127–140.

Gancia, G. (2020) 'Perpetrator of International Child Abuse Images Freed 5 June 2020'. Question for Written Answer E-003387/2020/rev.1 to the Vice-President of the Commission/High Representative of the Union for Foreign Affairs and Security Policy, Rule 138. www.europarl.europa.eu/doceo/document/E-9-2020-003387_EN.html

GenderIT (2015) 'Of Cultural Controls and Gender Inequality: Talking about Technology-Related Violence Against Women in Pakistan'. 29 May. www.genderit.org/articles/cultural-controls-and-gender-inequality-talking-about-technology-related-violence-against

Godin, M. (2020) 'From Threats of Gang Rape to Islamophobic Badgering, Indian Women Politicians Face High Levels of Online Abuse, Says Report'. *Time*, 23 January. https://time.com/5770213/india-women-politicians-twitter/

Goh, Y. and M. Yip (2014) 'The Protection from Harassment Act 2014: Legislative Comment'. *Singapore Academy of Law Journal* 26:703–726.

Gossman, P. (2020) 'Online Harassment of Women in Pakistan'. Human Rights Watch, 22 October. www.hrw.org/news/2020/10/22/online-harassment-women-pakistan

Government of Singapore (2021) 'MCI's Response to PQ on Proactive Policing of Internet and Blocking of Violent Content Accessible to Children and Youths in Singapore'. 3 May. www.mci.gov.sg/pressroom/news-and-stories/pressroom/2021/8/mci-response-to-pq-on-proactive-policing-of-internet-and-blocking-of-violent-content-accessible-to-children-and-youths-in-singapore

Groundviews (2018a) 'Technology-Related Violence Against Women and Girls in Sri Lanka: Key Trends'. 15 January. https://groundviews.org/2018/01/15/technology-related-violence-against-women-and-girls-in-sri-lanka-key-trends/

Groundviews (2018b) 'Digital Battlefield: Launch of Digital Security Wiki'. 20 June. https://groundviews.org/2018/06/20/digital-battlefield-launch-of-digital-security-wiki/

GSMA (Global System for Mobile Communications) (2018) 'A Framework to Understand Women's Mobile-Related Safety Concern'. www.gsma.com/mobilefordevelopment/wp-content/uploads/2018/05/A-framework-to-understand-women%E2%80%99s-mobile-report_march.pdf

Gunasekera, D. (2021) 'Online Gender-Based Violence: The New Normal of Sexual Harassment'. *The Morning*, 28 February. www.themorning.lk/online-gender-based-violence-the-new-normal-of-sexual-harassment/

Halder, D. (2017) 'Revenge Porn Against Women and the Applicability of Therapeutic Jurisprudence: A Comparative Analysis of Regulations in India, Pakistan, and Bangladesh'. In Halder, D. and J. Karuppannan (eds) *Therapeutic Jurisprudence and Overcoming Violence Against Women*. Hershey, PA: IPI Global.

Halder, D. and K. Jaishankar (2016) *Cyber Crimes Against Women in India*. New Delhi: SAGE.

Hamin, Z. and W. Wan Rosli (2020) '"Every Breath You Take I'll be Watching You": Governing Cyberstalking in Malaysia'. www.scitepress.org/Papers/2018/100518/100518.pdf

Hanif, Urva (2022). Authorities lacks capabilities to trace social media misusers November 11, https://thereporters.pk/authorities-lacks-capabilities-to-trace-social-media-misusers/

Hinduja, S. and J. Patchin (2010) 'Cyberbullying Research Summary: Cyberbullying and Suicide'. https://cyberbullying.org/cyberbullying_and_suicide_research_fact_sheet.pdf

Hindustan Times (2006) 'Securing the Web'. 22 October.

Hindustan Times (2021) 'Women Cyber Cell to Be Set up in Cyber Police Stations across UP'. 7 March. www.hindustantimes.com/cities/noida-news/women-cyber-cell-to-be-set-up-in-cyber-police-stations-across-up-101615139773850.html

Hoare, C.H. (1991) 'Psychosocial Identity Development and Cultural Others'. *Journal of Counseling & Development* 70(1): 45–53.

Hoffman, A.J. (1999) 'Institutional Evolution and Change: Environmentalism and the US Chemical Industry'. *Academy of Management Journal* 42(4): 351–371.

Houreld, K. (2014) 'Online Abuse of Women in Pakistan Turns into Real-World Violence'. Reuters, 30 September. www.reuters.com/article/pakistan-women-internet/online-abuse-of-women-in-pakistan-turns-into-real-world-violence-idINKCN0HP0PQ20140930

IFES (International Foundation for Electoral Systems) (2021) 'Assessment of Online Violence Against Politically and Civically Engaged Women in Bangladesh'. 6 April. www.ifes.org/publications/assessment-online-violence-against-politically-and-civically-engaged-women-bangladesh

IMS (International Media Support) (2019) *Defending Journalism: The Safety of Women Journalists: Breaking the Cycle of Silence and Violence*. www.mediasupport.org/wp-content/uploads/2019/10/2871-Gender-safety_FINAL_31.10.19_spreads-1.pdf

Internet Society (2017) 'Mapping Online Child Safety in Asia-Pacific'. www.internetsociety.org/wp-content/uploads/2021/01/Online-Child-Safety-in-Asia-Pacific-report-final.pdf

Islam, Z. (2021) 'Women in Bangladesh Face a Flurry of Online Attacks'. *My Republica*, 8 March. https://myrepublica.nagariknetwork.com/news/women-in-bangladesh-face-a-flurry-of-online-attacks/

ITU (International Telecommunication Union) (2012) *Understanding Cybercrime: Phenomena, Challenges and Legal Response*. Geneva: ITU.

ITU (2020) *Measuring the Information Society Report*. Geneva: ITU.

Kamit, R. (2016) 'Youth: Cyber Bullying a Worrying Trend in Brunei'. *The Brunei* Times, 25 July. https://btarchive.org/news/national/2016/01/25/youth-cyber-bullying-worrying-trend-brunei

Jafri, A. and Z. Aafaq (2021) 'Unchecked Tsunami of Online Sexual Violence by Hindu Right Against India's Muslim Women'. Article 14, 21 May. www.article-14.com/post/unchecked-tsunami-of-online-sexual-violence-by-hindu-right-against-india-s-muslim-women

James-Civetta, G. (2019) '6th May 2019 Bill Amendments to Singapore's Penal Code'. Singapore Criminal Lawyer, 22 May. www.singaporecriminallawyer.com/bill-amendments-singapores-penal-code/

Jandt, F. and D. Tanno (2001) 'Decoding Domination, Encoding Self-Determination'. *Howard Journal of Communication* 12(3): 10.1080/106461701753210411

Joseph, V. and M. Jain (2020) 'India: Anti-Cyber Bullying Laws In India – An Analysis', Mondaq, 1 October. www.mondaq.com/india/crime/989624/anti-cyber-bullying-laws-in-india--an-analysisSWAE4567%20N12390OP

Joseph, V. and D. Ray (2020) 'India: Cyber Crimes Under The IPC And IT Act - An Uneasy Co-Existence'. Mondaq, 10 February. www.mondaq.com/india/it-and-internet/891738/cyber-crimes-under-the-ipc-and-it-act--an-uneasy-co-existence

Kahan, D.M. (1996) 'What Do Alternative Sanctions Mean?' *University of Chicago Law Review* 591: 603–604.

Kahneman, D. (2003) 'A Perspective on Judgment and Choice: Mapping Bounded Rationality'. *American Psychologist* 58: 697–720.

Kamdar, B. (2021) 'Muslim Women in India "Auctioned" Online Using GitHub'. *The Diplomat*, 7 July. https://thediplomat.com/2021/07/muslim-women-in-india-auctioned-online-using-github/

Kamit, R. (2016) 'Youth: Cyber Bullying a Worrying Trend in Brunei'. 25 January. https://btarchive.org/news/national/2016/01/25/youth-cyber-bullying-worrying-trend-brunei

Kelman, S. (1987) *Making Public Policy: A Hopeful View of American Government*. New York: Basic Books.

Keelery, S. (2021) 'Cyber Stalking and Bullying Cases Reported in India 2019, by Leading State'. Statista, 25 February. www.statista.com/statistics/1097724/india-cyber-stalking-bullying-cases-against-women-children-by-leading-state/

Kon, J. (2019) 'HPC to Conduct New Survey on Bullying in schools'. *Borneo Bulletin*, 20 August. https://borneobulletin.com.bn/hpc-conduct-new-survey-bullying-schools/

Kshetri, N. (2009) 'Positive Externality, Increasing Returns and the Rise in Cybercrimes'. *Communications of the ACM* 52(12): 141–144.

Kshetri, N. (2009b) 'Institutionalization of Intellectual Property Rights in China'. *European Management Journal* 27(3): 155–164.

Kshetri, N. (2017) 'Cybersecurity in India: Regulations, Governance, Institutional Capacity and Market Mechanisms'. *Asian Research Policy* 8(1): 64–76.

Kshetri, N. (2018) 'As Digital Threats Grow, Will Cyber Insurance Take Off?" The Conversation, 26 October. https://theconversation.com/as-digital-threats-grow-will-cyber-insurance-take-off-104371

Kshetri, N. (2020) 'The Lack of Women in Cybersecurity Leaves the Online World at Greater Risk'. The Conversation, 15 May. https://theconversation.com/the-lack-of-women-in-cybersecurity-leaves-the-online-world-at-greater-risk-136654

Kshetri, N. (2021) *Cybersecurity Management: An Organizational and Strategic Approach*. Toronto: The University of Toronto Press.

Kshetri, N. and L.L. Alcantara (2015) 'Cyber-Threats and Cybersecurity Challenges: A Cross-Cultural Perspective'. In Holden, N., S. Michailova and S. Tietze (eds) *The Routledge Companion to Cross-Cultural Management*. London and New York: Routledge.

Kshetri, N. and N. Dholakia (2009) 'Professional and Trade Associations in a Nascent and Formative Sector of a Developing Economy: A Case Study of the NASSCOM Effect on the Indian Offshoring Industry'. *Journal of International Management* 15(2): 225–239.

Lakhani, K.R. and R.G. Wolf (2005) 'Why Hackers Do What They Do: Understanding Motivation and Effort in Free/Open Source Software Projects'. In Feller, J.,

B. Fitzgerald, S. Hissam and K.R. Lakhani (eds) *Perspectives on Free and Open Source Software*. Cambridge, MA: MIT Press.

Leidig, E. (2020) 'Hindutva as a Variant of Right-Wing Extremism'. *Patterns of Prejudice* 54(3): 215–237.

Leong, L. (2017) 'Fighting Fake News: How Google, Facebook, and Others Are Trying to Stop It'. TechRadar, 25 May. bit.ly/2fO52Se

Lim, S. (2021) 'Queering Malay Identity Politics in the Malaysian Digital Space'. Heinrich Böll Stiftung, 14 May. https://th.boell.org/en/2021/05/14/queering-malaysian-digital-space

Lindenberg, S. (2001) 'Intrinsic Motivation in a New Light'. *Kyklos* 54(2/3): 317–342.

Linder, S.H. (1999) 'Coming to Terms with the Public–Private Partnership: A Grammar of Multiple Meanings'. *American Behavioral Scientist* 43(1): 35–51.

Lipson, C. (1991) 'Why Are Some International Agreements Informal?' *International Organization* 45(4): 495–538.

Lohumi, B.P. (2020) 'In Himachal, Women Targeted in 60% Cyber Crimes'. *The Tribune*, 20 November. www.tribuneindia.com/news/himachal/in-hp-women-targeted-in-60-cyber-crimes-172989

Lomba, N., C. Navarra and M. Fernandes (2021) 'Combating Gender-Based Violence: Cyber Violence European Added Value Assessment'. *European Parliamentary Research Service*. www.europarl.europa.eu/RegData/etudes/STUD/2021/662621/EPRS_STU(2021)662621_EN.pdf

Lyons, C.J. (2006) 'Stigma or Sympathy? Attributions of Fault to Hate Crime Victims and Offenders'. *Social Psychology Quarterly* 69(1): 39–60.

Maas, D. (2021) 'Online Violence against Women Journalists Is Intensified by Other Forms of Discrimination, New Research Finds'. *International Journalists' Network*, 29 April. https://ijnet.org/en/story/online-violence-against-women-journalists-intensified-other-forms-discrimination-new-research

Madden, M., A. Lenhart, S. Cortesi et al (2013) 'Teens, Social Media, and Privacy'. Pew Research Center, 21 May. www.pewresearch.org/internet/2013/05/21/teens-social-media-and-privacy/

Maheshwari, R. (2020) '1 in.10 Indian Adolescents Faces Cyberbullying, Half Don't Report: Study'. India Spend, 12 March. www.indiaspend.com/1-in-10-indian-adolescents-faces-cyberbullying-half-dont-report-study/

Mahmud, F. (2018) 'Women Increasingly Falling Prey to Cyberbullying'. 25 October. https://m.theindependentbd.com/post/171850

Malay Mail (2017) 'Law Enforcers Downplay Reports of Online Violence Against Women, Report Shows'. 13 November. www.malaymail.com/news/malaysia/2017/11/13/law-enforcers-downplay-reports-of-online-violence-against-women-report-show/1508981

Maldives Independent (2018) 'More than 100 Child Abuse Cases Reported in April'. 24 May. https://maldivesindependent.com/crime-2/more-than-100-child-abuse-cases-reported-in-april-138386

Maynard, M. (2019) 'Better Be Careful What You "Like"'. *Kentucky Today*, 28 September. www.kentuckytoday.com/stories/better-be-careful-what-you-like,21791

MCCHR (Malaysian Centre for Constitutionalism and Human Rights) (2018) 'Cyberharassment in Malaysia: What Do We See Happening?' MCCHR, 31 January. https://mcchr.org/2018/01/31/cyberharassment-in-malaysia-what-do-we-see-happening

Media Matters for Democracy (2020) 'Pakistan: Solidarity with Women Journalists Calling for an End to Online Violence'. 16 August. https://ifex.org/pakistan-solidarity-with-women-journalists-calling-for-an-end-to-online-violence/

Menon, M. (2020) 'Women Victims of Violence Offered Help from New Singapore Website'. *The Straits Times*, 30 November. www.straitstimes.com/singapore/women-victims-of-violence-offered-help-from-new-singapore-website

Mental Health Commission (2017) 'Bullying and Suicide'. www.mentalhealthcommission.ca/sites/default/files/2017-11/CSP_Fact_Sheets_bullying_eng.pdf

Metri, N. (2016) 'Digital Abuse Against Women. Nighat's Fight in Pakistan'. Internet Society, 7 March. www.internetsociety.org/blog/2016/03/digital-abuse-against-women-nighats-fight-in-pakistan

Mihindukulasuriya, R. (2021) 'Muslim Women Being "Auctioned" on Social Media, Congress Leader

Named Files Complaint'. *The Print*, 16 May. https://theprint.in/india/muslim-women-being-auctioned-on-social-media-congress-leader-named-files-complaint/659063/

Mohamad, L. (2020) 'Ending the Victim-Blaming Culture'. *Borneo Bulletin*, 17 December. https://theworldnews.net/bn-news/ending-the-victim-blaming-culture-borneo-bulletin-online

Moosa, H. (2019) 'Police Probes Online Harassment of Barista'. *Maldives Independent*, 25 November. https://maldivesindependent.com/crime-2/police-probes-online-harassment-of-barista-149481

Munavvar, R. (2020) 'Maldives Marks "Safer Internet Day 2020". 11 February. https://edition.mv/adb/14955

Narayan, V. (2010) 'Cyber Criminals Hit Esc Key for 10 Yrs'. *The Times of India*, 20 September. https://timesofindia.indiatimes.com/city/mumbai/cyber-criminals-hit-esc-key-for-10-yrs/articleshow/6587847.cms

Nazir, T. (2021) 'Online Sexual Abuses among Women on Rise amid Covid-19 Crisis'. The Logical Indian, 3 July. https://thelogicalindian.com/gender/online-sexual-abuses-among-women-on-rise-29332

New Age Bangladesh (2020) 'Majority of Cyberbullying Victims in Bangladesh Are Women'. 10 December. www.newagebd.net/article/123926/majority-of-cyberbullying-victims-in-bangladesh-are-women

Newall, M. (2018) 'Cyberbullying: A Global Advisor Survey'. www.ipsos.com/sites/default/files/ct/news/documents/2018-06/cyberbullying_june2018.pdf

Nilesh Beliraya, KAbhilasha (2020) 'Cyber Crime Against Women in India: Legal Challenges and Solutions'. *International Journal of Law Management & Humanities* 3(5): 1012–1022.

Nolen, S. (2012) 'India's IT Revolution Doesn't Touch a Government That Runs on Paper'. *The Globe and Mail* (Canada), 13 June.

Nortajuddin, A. (2020) 'Does Malaysia Have a Cyberbullying Problem?' The ASEAN Post, 22 July. https://theaseanpost.com/article/does-malaysia-have-cyberbullying-problem

North, D.C. (1990) *Institutions, Institutional Change and Economic Performance*. Cambridge: Cambridge University Press.

North, D.C. (1994) 'Economic Performance Through Time'. *American Economic Review* 84(3): 359–368.

North, D.C. (1996) 'Epilogue: Economic Performance Through Time'. In Alston, L.J., T. Eggertsson and D.C. North (eds) *Empirical Studies in Institutional Change*. Cambridge: Cambridge University Press.

Norzom, T. and R. Balakrishnan (2020) 'The Crisis of Internet Safety: How Free Are Women to Enjoy the Wilderness of the Web?' 7 October. https://yourstory.com/herstory/2020/10/crisis-internet-safety-women-social-media-cybercrime/amp

Ohlheiser, A. (2017) 'Even Mark Zuckerberg Can't Stop the Meme that He Is Running for President'. *Washington Post*, 3 August.

Paetzold, R.L., R.L. Dipboye and K.D. Elsbach (2008) 'A New Look at Stigmatization in and of Organizations'. *Academy of Management Review* 33(1): 186–193.

Page, C. (2006) 'Striking Back at the Cyberbullies'. BBC, 16 April. http://news.bbc.co.uk/2/hi/uk/4912766.stm

Pakistan Today (2019) 'FIA Registers 8,500 Complaints Concerning Women Harassment'. 6 May. www.digitalrightsmonitor.pk/fia-registers-8500-complaints-concerning-women-harassment/

Pasricha, J. (2016) 'Cyber Violence Against Women In India – A Research Report'. 15 November. https://feminisminindia.com/2016/11/15/cyber-violence-against-women-india-report/

Plan International (2020) 'Abuse and Harassment Driving Girls off Facebook, Instagram and Twitter'. 5 October. https://plan-international.org/news/2020-10-05-abuse-and-harassment-driving-girls-facebook-instagram-and-twitter

Quilt.AI and ICRW (International Center for Research on Women) (2021) 'COVID-19 and Online Violence in India: Digital Intelligence Report'. April. www.icrw.org/wp-content/uploads/2021/04/Ex-Summary-Online-Violence-during-Covid-in-India.pdf

Raffles, T. (1992) 'The Guilty Bystander: Leet v. State'. *Stetson Law Review* 22(1), Fall.

Rasmussen, E. (1996) 'Stigma and Self-Fulfilling Expectations of Criminality'. *Journal of Law and Economics* 39: 519–543.

RESURJ (Realizing Sexual and Reproductive Justice) (n.d.) 'Submission on Technology-Related and Online Violence Against Women'. https://resurj.org/resource/submission-on-technology-related-and-online-violence-against-women/

Rodrigo, S. (2020) 'A Cybercrime Victim Needs to Know She Can Seek Justice'. *Sunday Times*, 8 March. www.sundaytimes.lk/200308/magazine/a-cybercrime-victim-needs-to-know-she-can-seek-justice-394957.html

Roy, P.K. (2015) 'Why Online Harassment Goes Unpunished in India'. BBC News, 17 July. www.bbc.com/news/world-asia-india-33532706

Ryan, R.M. and E.L. Deci (2000) 'Intrinsic and Extrinsic Motivations: Classic Definitions and New Directions'. *Contemporary Educational Psychology* 25(1): 54–67.

Sajid, Asma (2022) FIA Hasn't Been Paying Its Employees for Past 6 Months Dec 12, 2022 https://propakistani.pk/2022/12/12/fia-hasnt-been-paying-its-employees-for-past-6-months/

Salim, M. (2018) 'Online Trolling of Indian Women Is Only an Extension of the Everyday Harassment They Face'. *The Wire*, 8 July . https://thewire.in/women/online-trolling-of-indian-women-is-only-an-extension-of-the-everyday-harassment-they-face

Schjølberg, S. (2008) 'The History of Global Harmonization on Cybercrime Legislation – The Road to Geneva'. *Cybercrime Law*, December.

Scott, W.R. (1992) *Organizations: Rational, Natural and Open Systems*. New York: Prentice Hall.

Scott, W.R. (1995) *Institutions and Organizations*. Thousand Oaks, CA: Sage.

SDJF (Sri Lanka Development Journalist Forum) (2020) 'How to Block Online Gender-based Violence?' https://ldjf.org/news/65/how_to_block_online_gender_based_violence

Seattle Public Schools (2017) 'Seattle Public Schools, District Partners to Stop Bullying on Social Media'. www.seattleschools.org/district/calendars/news/what_s_new/district_partners_to_stop_bullying_on_social_media (accessed 12 February 2018)

Sharbawi, Z.H. (2018) 'Keynote Speech'. *The 11th China-ASEAN Prosecutors-General Conference', Bandar Seri Begawan*. www.agc.gov.bn/conference/Secretariat%20Documents/Speech%20and%20Key%20Notes/Brunei%20Key%20Note%20Speech%2011%20CAPGC.pdf

Skinnider, E. (2018) 'Towards Gender Responsive Criminal Justice: Good Practices from Southeast Asia in Responding to Violence Against Women'. https://icclr.org/wp-content/uploads/2019/06/Towards-Gender-Responsive-Criminal-Justice.pdf

Slonje, R., P.K. Smith and A. Frisén (2013) 'The Nature of Cyberbullying, and Strategies for Prevention'. *Computers in Human Behavior* 29(1):26–32.

Song, J.K. (2016) *Protecting Children from Cybercrime: Legislative Responses in Asia to Fight Child Pornography, Online Grooming, and Cyberbullying*. Washington, DC: World Bank.

Staub, E. (1990) 'Moral Exclusion, Personal Goal Theory, and Extreme Destructiveness'. *Journal of Social Issues* 46(1): 47–64.

Tajfel, H. and J.C. Turner (1986) 'The Social Identity Theory of Intergroup Behavior'. In Worchel, S. and W.G. Austin (eds) *Psychology of Intergroup Relations*. Chicago, IL: Nelson-Hall.

Tahir, Z. (2021) 'Justice Elusive for Many at FIA Cybercrime Wing'. Dawn, 16 May. www.dawn.com/news/1623910/justice-elusive-for-many-at-fia-cybercrime-wing

Tandon, N. (2007) 'Secondary Victimization of Children by the Media: An Analysis of Perceptions of Victims and Journalists'. *International Journal of Criminal Justice Sciences* 2(2): 119–135.

Teng, A. (2021) 'Shine a Light on Dark Online Spaces for Women and Girls: Sim Ann'. *The Straits Times*, 8 March. www.straitstimes.com/singapore/shining-a-light-on-dark-online-spaces-for-women-and-girls-sim-ann

The Conversation (2018) 'Don't Be a Bystander: Five Steps to Fight Cyberbullying'. 20 February. https://theconversation.com/dont-be-a-bystander-five-steps-to-fight-cyberbullying-91440

The Daily Star (2018) 'Online Violence Against Women on the Rise'. 16 March. www.thedailystar.net/city/online-violence-against-women-the-rise-1548898

The International (2020) 'FIA, Facebook Agree to Collaborate on Cyber Crimes Against Women, Children'. 18 September. www.thenews.com.pk/latest/716664-fia-facebook-agree-to-collaborate-on-cyber-crimes-againt-women-children

The Jakarta Post (2019) 'Singapore Outlaws "Revenge Porn", "Cyber-Flashing"'. 7 May. www.thejakartapost.com/seasia/2019/05/07/singapore-oulaws-revenge-porn-cyber-flashing.html

The Times of India (2011) 'Most Gurgaon IT, BPO Companies Victims of Cybercrime: Survey'. 6 November.

Toppa, S. (2017) 'Abuse in Pakistan: "I'm More Scared of Harassment Online than Offline"'. *The Guardian*, 9 August. www.theguardian.com/global-development-professionals-network/2017/aug/09/abuse-in-pakistan-im-more-scared-of-harassment-online-than-offline

UNDP (United Nations Development Programme) (2021) 'Cyber Care App Launched to Combat Cyber Violence in Sri Lanka'. Press Release, 25 February. www.lk.undp.org/content/srilanka/en/home/presscenter/pressreleases/2021/Cyber_Care_App_launched_to_combat_cyber_violence_in_Sri_Lanka.html

UNESCAP (United Nations Economic and Social Commission for Asia and the Pacific) (2020) *The Covid-19 Pandemic and Violence Against Women in Asia and the Pacific*. Bangkok: UNESCAP.

UNICEF (United Nations Children's Fund) (2016) *Victims Are Not Virtual: Situation Assessment of Online Child Sexual Exploitation in South Asia*. New Delhi: UNICEF Regional Office for South Asia.

UN Women (2020) *Online Violence Against Women in Asia: A Multicountry Study*. New York: UN Women.

US Department of State (2016) 'Human Rights Report – Brunei Darussalam'. www.state.gov/wp-content/uploads/2019/01/Brunei.pdf

Vega Montiel, A. (2020) 'Latinx Feminist Activism for the Safety of Women Journalists'. In Goins, M.N., J. Faber McAlister and B.K. Alexander (eds) *The Routledge Handbook of Gender and Communication*, 1st Edition. London: Routledge.

Vitis, L. (2021) 'Technology-Facilitated Violence Against Women in Singapore: Key Considerations'. In Bailey, J., A. Flynn and N. Henry (eds) *The Emerald International Handbook of Technology Facilitated Violence and Abuse*. Emerald Studies in Digital Crime, Technology and Social Harms. Bingley: Emerald Publishing Limited.

WACC (2016) 'Communication Projects Address Violence Against Women'. 2 February. https://waccglobal.org/communication-projects-address-violence-against-women/

Wahab, N. (2020) 'Cyber Crime Helpline: Over 100 Women Complain Against Online Harassment in a Month'. *The News*, 10 March. www.thenews.com.pk/print/626813-cyber-crime-helpline-over-100-women-complain-against-online-harassment-in-a-month

Walzer, M. (1993) 'Between Nation and World: Welcome to Some New Ideologies'. *Economist* 328(7828): SS49–SS52.

Wemmers, J.-A. and K. Cyr (2005) 'Can Mediation Be Therapeutic for Crime Victims? An Evaluation of Victims' Experiences in Mediation with Young Offenders'. *Canadian Journal of Criminology and Criminal Justice* 47(3): 527–544.

White, J. (2017) 'How to Keep Cyberbullies Out of Your Life'. Inc.com. www.inc.com/john-white/how-to-keep-cyberbullies-out-of-your-life.html

Wickrematunge, R. (2019) 'Sexism, Slander, Hatred: Sri Lanka's Culture of Online Abuse'. 28 May. www.theguardian.com/global-development/2019/may/28/sexism-slander-hatred-sri-lankas-culture-of-online-abuse

Wiesenfeld, B.M., K.A. Wurthmann and D.C. Hambrick (2008) 'The Stigmatization and Devaluation of Elites Associated with Corporate Failures: A Process Model'. *Academy of Management Review* 33(1): 231–251.

Williams, C. (2017) '4 Risk Response Strategies You Will Have to Consider after Assessing Risks'. ERM Insights, 10 January. www.erminsightsbycarol.com/risk-response-strategies/

World Bank (2021) *The Maldives Development Update: April 2021*. Washington, DC: World Bank.

Yashee (2018) 'Man Getting 5 Years in Jail for Sharing Nude Video of Ex Shows India Is Waking up to Revenge Porn'. Daily O, 12 March. www.dailyo.in/variety/revenge-porn-midnapore-cyber-crime-crimes-against-women-22796

Yi, B. (2019) '"Pervasive" Digital Sexual Violence Against Women Skyrockets in Singapore'. Reuters, 25 November. www.reuters.com/article/us-singapore-crime-technology-women/pervasive-digital-sexual-violence-against-women-skyrockets-in-singapore-idUSKBN1XZ1NB

Zakrzewski, Cat (2022) White House announces tech company efforts to combat violent extremism September 15, https://www.washingtonpost.com/technology/2022/09/15/white-house-tech-extremism/

Commonwealth Secretariat
Marlborough House, Pall Mall
London SW1Y 5HX
United Kingdom

thecommonwealth.org

The Commonwealth

D19100