July 2017

Mapping Online Child Safety in Asia-Pacific

Internet Society

Acknowledgments

This report is the outcome of a three-month research fellowship programme supported by Google. Research for the report, as well as the initial draft, was done by Jee Eun Choi. The report was revised by Noelle Francesca de Guzman and Rajnesh Singh, and was edited by Christine Apikul.

Internet Society – APAC Bureau
9 Temasek Boulevard
#09-01 Suntec Tower 2
Singapore 038989
Tel: +65 6407 1470
Fax: +65 6407 1501
Email: apac@isoc.org
www.internetsociety.org

Follow us on Twitter @ISOCapac
Follow us on Scoopt.it! http://www.scoop.it/t/internet-in-asia-pacific

Executive Summary

In today’s age, the Internet has become essential for developing and strengthening the capacities of children. But at the same time, use of the Internet can come with some risks for young Internet users. It can create new challenges with regards to their safety and protection - both in the physical and virtual worlds. However, quick-fix interventions that limit children’s online access tend to result in a loss of opportunity for them to take advantage of the benefits of the Internet.

There is limited research on child online safety in Asia-Pacific --this report outlines some of the resources that are currently available. It provides an overview of initiatives, focusing on policies that are in place to tackle child online safety in selected economies in the region, and an introduction to the different actors involved in addressing the various risks that children can face online. Based on an analysis of these findings, emerging priority issues are identified and some policy recommendations are proposed.

To frame the analysis, this study divides Asia-Pacific economies into three clusters by Internet penetration level (high, moderate and low), which generally has a positive correlation with the income level of an economy, i.e. a high-income economy tends to have higher Internet penetration. Eleven economies have been selected based on the ease of obtaining data and information on child online safety. The study is based on secondary research online, by using key search terms related to child online protection.

Findings

The study found that all selected economies are working to protect children from online sexual abuse and exploitation. Regardless of their level of Internet penetration, all criminalise the production and distribution of child pornography under domestic law.

However, the quality of legislation—when present--vary. Relevant laws in economies with high Internet penetration tend to have a clear and consistent definition of “child” and “child pornography”, and include offenses facilitated by all Internet-enabled platforms.

Economies with high Internet penetration have also enacted laws and developed interventions on other aspects of child online safety, such as children’s exposure to harmful content, cyberbullying and Internet addiction. But there does not seem to be any targeted legislative response to the online privacy of children and the protection of children from information security risks. Moreover, comprehensive measures to equip children with the knowledge, tools and skills necessary for them to manage these risks are still lacking, particularly in developing countries in the region.

Recently, in Australia, New Zealand, the Philippines and Singapore, laws have been passed to protect children against cyberbullying. These laws are being criticised for criminalising children and being inconsistent with the right to freedom of expression. Some believe that it is more effective to tackle cyberbullying through awareness-raising and education programmes with parents, guardians, schools and young people themselves.

It must be emphasised that drafting and implementing legislation are only one among the many steps that can be taken by governments. The study found that countries have used a mix of measures to address these concerns, including technical tools to filter content, end-user empowerment, and cooperation between multiple stakeholders, including children.

The number of measures, policies and programmes in place suggest that economies with high Internet penetration are actively working to address child online safety issues. Most of the actors are from the public sector, but many of the initiatives involve public-private-civil society partnerships. As these are generally high-income economies, the public sector tends to be better resourced to lead and coordinate child online safety issues.

Emerging economies included in this report, which tend to have moderate Internet penetration, typically do not have as much resources at their disposal. In these countries, the public sector has taken initiatives to address child online safety issues, albeit less rigorously than those with high Internet penetration. But non-governmental organisations are stepping up to fill any gaps. It is worth noting that many of the initiatives are public-private-civil society partnerships. UNICEF has likewise been working in these countries to address child online safety, mainly to support research that will guide policymaking and help raise awareness on the issues.

Generally, there is limited English-language information on the child online safety initiatives of economies with low Internet penetration. Information on India was drawn largely from a recent UNICEF study. India, when compared with economies of moderate and high Internet penetration has weaker legislation, and actors are less coordinated in tackling child online safety issues.

Policy Recommendations

Based on the study, the following policy recommendations are proposed:

- In domestic laws, clearly define terms based on international legal standards and include offenses facilitated by all Internet-enabled platforms. Harmonisation of terminology used is critical.
- Ensure that policies to protect children online are consistent with other important policy objectives, such as the preservation of fundamental rights, including privacy and freedom of expression.
- Collaborate among relevant ministries, agencies and institutions, adopt a multi-stakeholder approach, and ensure international cooperation.
- Make digital citizenship a priority in online child protection policies. Digital skills, including safety online, must be taught from the earliest stage possible. In practice, for today's environment, this means from early primary (or elementary) school age.
- Develop a coordinated strategy for awareness-raising and education on child online safety for different actors. This includes engaging with and empowering parents, guardians, teachers and other authority figures with whom young people regularly interact.
- Strengthen the child protection and technological capacity of law enforcement agencies.
- Engage with children to develop robust research on child online safety and integrate findings in child protection systems.
- Develop consistent indicators to assess and monitor child online safety.

Table of contents

Introduction

Studies, largely on developed economies in Europe and the North America, show that an increasing number of children[1] are using the Internet. They are starting at a younger age, using a variety of devices and spending more time online. For instance, 53% of children aged 3-4 years in the United Kingdom are using a tablet to go online. Some markets are reaching saturation with nearly 100% Internet penetration among children in northern Europe.[2]

As the Internet, particularly mobile broadband, becomes more accessible and affordable in Asia and the Pacific, the abovementioned trend is also becoming evident in the region. In India, it is estimated that 134 million children have mobile phones.[3] In Indonesia, roughly 60% of children access the Internet through mobile devices.[4] In the Philippines, around half of the 44 million Internet users are children aged 17 years old and below.[5] In Thailand, 58% of children aged 6-14 years are using the Internet.[6] Meanwhile a study conducted by the China National Youth Palace Association in 2014 in 18 cities found that 72% of children aged 10 or under in China owned a mobile phone, and 30% of children under 6 years have used a tablet. It also noted that age 10 was the turning point when children used the Internet not only for online gaming, but also for entertainment, communication, learning and self-expression. By age 13, children become not only online content consumers, but also creators.[7]

The Internet brings opportunities for children's education, self-expression and social development. But its use also carries threats and risks, such as access to inappropriate content, harmful interactions with other children or with adults, and exposure to aggressive marketing practices. Moreover, children online can share their personal data without understanding the potential long-term privacy consequences. In some instances, children have lost their lives because of cyberbullying, and while the Internet has not created crimes involving sexual abuse and exploitation of children, it has enhanced their scale and potential.

Social media has transformed how society creates and consumes news and information today, but it has also allowed for new ways to facilitate people trafficking, distribution of child abuse materials and new avenues for recruiting victims. It has provided new – and often large scale ways - in which children are able to bully and shame others. It is estimated that nearly one quarter of children reported missing in Indonesia had been lured into trafficking by their captors through Facebook.[8] The Indonesia National Center for

[1] The definition of "child" may be different in the economies in this report, UNICEF's definition is used, and "child" refers to a person who is under 18 years old except for any country that legalised the concept of adulthood younger than the standard.

[2] Jutta Croll, "Let's Play it Safe: Children and Youths in the Digital World - Assessment of the Emerging Trends and Evolutions in ICT Services," White Paper for the ICT Coalition for Children Online, 11 January 2016.

[3] UNICEF, Child Online Protection in India (New Delhi, 2016), http://unicef.in/Uploads/Publications/Resources/pub_doc115.pdf.

[4] GSMA and NTT DOCOMO, "Children's use of mobile phones: An international comparison 2012," http://www.gsma.com/publicpolicy/wp-content/uploads/2012/03/GSMA_ChildrensMobilePhones2012WEB.pdf.

[5] UNICEF, "Globe, UNICEF Philippines, Ateneo sign MoU on online child protection," https://www.unicef.org/philippines/media_25571.html#.WDsg91zvccQ.

[6] Rattana Jaroonsaksit, "Kingdom of Thailand: Child Online Protection Initiatives," presentation made on 13 September 2016, http://www.itu.int/en/ITU-D/Regional-Presence/AsiaPacific/Documents/Events/2016/Sept-COP/Presentation/Thailand_COP_Initiative.pdf.

[7] Ng Ki Chun and Bianca Caroline Ho, "APrIGF 2015 Workshop Report," http://www.dotkids.asia/wp-content/uploads/2015/07/APrIGF2015-Workshop-Report.pdf.

[8] MTV Exit cited in A. R. Mubarak, "Child Safety Issues in Cyberspace: A Critical Theory on Trends and Challenges in the ASEAN Region," *International Journal of Computer Applications*, Vol. 129, No. 1 (November 2015), pp. 48-55,

Children reports that 18,747 had been sexually exploited through the Internet from 2011-2015,[9] while in Singapore, a 2014 McAfee survey revealed that one in three children have had experience with cyberbullying.[10] Despite these incidents, a 2015 study by Stairway Foundation and the Department of Education in the Philippines found that half of the children polled lacked awareness of the risks and dangers that they face on the Internet.[11]

Connected products, services and technologies are developing at a rapid pace, bringing about evolving opportunities, as well as threats and challenges. Law-making and enforcement authorities are often seriously challenged to cope with emerging online techniques used to target and harm children.

For example, bitcoin is an innovative payment network that allows users to send and receive money and protects against identity theft. But because payments in bitcoin can be made and finalised without one's personal information being tied to the transaction, it can be conveniently used to purchase child sexual abuse materials. Several other anonymised or difficult-to-trace forms of electronic payment can be used as a means for crimes involving the exploitation of children, but the extent of the threat these present has not been researched and is as yet unquantifiable.[12]

Addressing the risks that children face online without reducing their access to the opportunities and benefits of the Internet is a complex global challenge. In Lalpur, a village in the northern state of Uttar Pradesh in India, leaders recently ordered mobile phones confiscated from every girl under the age of 18 years after a local teacher, who had used a smartphone, was arrested on charges of molesting one of his students.[13]

How can we better tackle these concerns? According to a global study by UNICEF,[14] the online risks that children face are generally not well integrated in the great majority of child protection systems and responses. As a starting point, policymakers should not get side-tracked into blaming the medium: coordination and cooperation with different stakeholders is key to building a safer Internet, including the active participation of children themselves in developing effective safety strategies. As the report points out:[15]

We have discovered that many children are comfortable navigating the Internet and are able to avoid risks. They may see themselves as protectors of younger children and are themselves agents for change. Children

http://www.ijcaonline.org/research/volume129/number1/mubarak-2015-ijca-906925.pdf.

[9] Rizki Ameliah, "Indonesia's Perspective on Child Online Protection," presentation of Indonesia's Ministry of Communication and Information Technology on 13 September 2016, http://www.itu.int/en/ITU-D/Regional-Presence/AsiaPacific/Documents/Events/2016/Sept-COP/Presentation/MCIT%20Indonesia%2c%20ASEAN%20ITU-Manila%2c13%20September%202016-FINAL%20Rizky.pdf.

[10] Liang Hwei, "McAfee Study Reveals 1 In 9 Singaporean Teens Have Been Cyberbullied," Vulcan Post, 2 September 2014, https://vulcanpost.com/18939/1-9-singaporean-teens-cyberbullied-mcafee-study-reveals/

[11] Stairway Foundation, "Cybersafe Survey 2015," http://www.cybersafe.asia/wp-content/uploads/2016/03/Cybersafe-Survey_LOWRES.pdf

[12] ECPAT, "Briefing Paper: Emerging Global Threats Related to the Sexual Exploitation of Children Online," http://www.ecpat.org/wp-content/uploads/2016/05/Briefing-Paper_Emerging-global-threats-related-to-the-sexual-exploitation-of-children-online.pdf.

[13] Eric Bellman and Aditi Malhotra, "Why the vast majority of women in India will never own a smartphone," *The Wall Street Journal*, 13 October 2016, http://www.wsj.com/articles/why-the-vast-majority-of-women-in-india-will-never-own-a-smartphone-1476351001.

[14] UNICEF, *Child Safety Online: Global Challenges and Strategies - Technical Report* (Florence, 2012), https://www.unicef-irc.org/publications/pdf/ict_techreport3_eng.pdf.

[15] Ibid., p. iii.

should be allowed to express their views on how to mitigate risks, and they should be listened to and empowered to safely exploit the benefits of the Internet. However, despite children's agency, we should not overestimate their ability to protect themselves. Ultimately, the onus lies with adults to put in place a framework that ensures children equal and equitable access to the Internet, along with a safer online environment.

These findings are corroborated by a recent UNESCO report on digital citizenship in Asia-Pacific, which calls for a balance between fostering safety through the empowerment of children, and top-down policies to minimise risk. The other actors that need to be involved in addressing child online safety include policymakers, law enforcement agencies, social workers, teachers, parents and the private sector.

Framework for Analysis

To frame the analysis, this study divides Asia-Pacific economies into three clusters by Internet penetration level:

High = >70%
Moderate = 25%-70%
Low = <25%

In general, Internet penetration level has a positive correlation with the income level of an economy, i.e., a high-income economy tends to have high Internet penetration.

The Internet Society's 2015 Global Internet Report provides Internet penetration levels for 19 Asia-Pacific countries, and two to five economies per cluster are selected out of these based on the ease of obtaining data and information on child online safety (see Table 1).

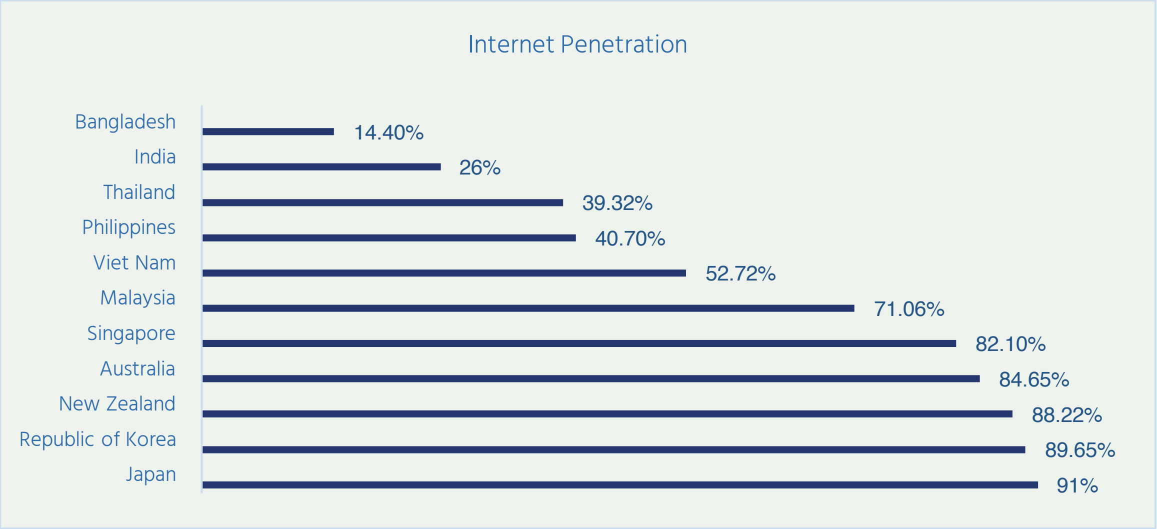

Figure 1. Internet penetration in selected Asia-Pacific economies[16]

[16] Source: ITU Facts and Figures 2016, http://www.itu.int/en/ITU-D/Statistics/Pages/stat/default.aspx accessed on 18 May 2017. Please note that the figures may have changed since the publication of this report.

Economies with High Internet penetration	Japan	Republic of Korea	Australia	New Zealand	Singapore
Economies with Mid Internet penetration	Malaysia	Viet Nam	Thailand	Philippines	
Economies with Low Internet penetration	India	Bangladesh			

Table 1. Selected economies for the different levels of Internet penetration

Methodology and Limitations

The methodology used to collect data and resources mainly secondary research online, using key search terms related to online child safety (See Table 2). The key terms are assembled with the economy's name. For example, "child online policy Malaysia" and "child online protection Australia".

Areas	**Searched Terms**			
Child-Related Terms	Child	Young	Kid	Juvenile
	Adolescent	Teenager		
Internet-Related Terms	Online	Cyber	Internet	
Safety-Related Terms	Safety	Protection		
Other Key Terms	Policy	Legal	Registration	Act
	Implementation			

Table 2. Key terms used for online research

In instances when academic research was not available, non-academic sources such as reports, websites, presentations, news articles and blogs by United Nations agencies, and governmental and non-governmental organisations were used.

Literature Review

The risks that children encounter on the Internet are diverse, but can be divided into three groups:[17]

Content – The types of content that children encounter online may be inappropriate, potentially dangerous and illegal, such as websites that promote self-harm, hate speech and pornography.

Usage/Conduct – The way that children use the Internet may put them at risk. This includes the types of content that children create and share with others. The risks range from cyberbullying, sexting,[18] fraudulent transactions, to privacy and security concerns. Internet addiction is also a concern for many countries.

Interaction/Communication – Interacting with individuals especially on social media networks and chatrooms, can expose children to risks such as online grooming,[19] and arranging to meet with potentially or actually abusive strangers.

A. R. Mubarak*, "Child Safety Issues in Cyberspace: A Critical Theory on Trends and Challenges in the ASEAN Region," International Journal of Computer Applications, Vol. 129, No. 1 (November 2015), pp. 48-55*[20]

This is one of the few academic papers that provide an analysis of child online safety in the region. It covers the ASEAN sub-region, including several economies from all three clusters in this study, as well as all three groups of risks described above.

The study provides some information on legislation and policies that are in place to address child online safety. It focuses on the following themes:

Content –

- Children's access to sexual images and pornography that could lead to them engaging in risky sexual acts

Usage/Conduct –

- Using mobile phone cameras for inappropriate purposes
- Online gaming and gambling, and Internet addiction

[17] London School of Economic and Political Science Media Policy Project Blog, "Children's safety on the Internet: A Guide to Stakeholders," 31 March 2015, http://blogs.lse.ac.uk/mediapolicyproject/2015/03/31/childrens-safety-on-the-internet-a-guide-to-stakeholders/.

[18] Sexting is the sending of sexually explicit messages or images. The phenomenon of sexting has increased among adolescents who willingly produce erotic/pornographic images of themselves, typically to share with their current "partner". These partners, however, often disseminate the images, which then end up in possession of child pornography collectors. Research shows that 88% of self-generated sexually explicit content online was taken from its original location and uploaded to a different Internet site. ECPAT, "Briefing Paper: Emerging Global Threats Related to the Sexual Exploitation of Children Online," http://www.ecpat.org/wp-content/uploads/2016/05/Briefing-Paper_Emerging-global-threats-related-to-the-sexual-exploitation-of-children-online.pdf.

[19] Grooming is defined as actions deliberately undertaken with the aim of befriending and establishing an emotional connection with a child, in order to lower the child's inhibitions in preparation for sexual activity with the child. To "groom" a child a paedophile must have a way of communicating with a child effectively in private. To do this they are exploiting the popularity with children of chat rooms and social networking websites. INHOPE, "Online Grooming," http://www.inhope.org/gns/internet-concerns/overview-of-the-problem/online-grooming.aspx.

[20] http://www.ijcaonline.org/research/volume129/number1/mubarak-2015-ijca-906925.pdf.

- Cyberbullying

Interaction/Communication –

- Social networking sites and child grooming
- Online prostitution and the production and distribution of child pornography

Due to the borderless nature of the Internet, the Mubarak study urges ASEAN member countries to develop a region-wide, if not a uniform, policy on child protection issues. It suggests that many countries need to define the legal obligation of Internet service providers (ISPs) to protect children online. Community capacity building is identified as important for the sub-region, particularly the need to empower children to protect themselves and each other. The author notes that the sub-region's economic, social and cultural diversity may pose a short-term challenge to developing a coordinated strategy for child online safety.

UNICEF, *Child Protection in the Digital Age: National Responses to Online Child Sexual Abuse and Exploitation in ASEAN Member States* (Bangkok, 2016)[21]

The UNICEF report takes stock of existing legislation and programmes and identifies gaps and opportunities to better prevent and respond to child sexual abuse and exploitation in Southeast Asia. It uses the #WePROTECT Model National Response framework, which elaborates on 21 capabilities that a country needs to have in place to address child online sexual abuse and exploitation.

The report highlights the lack of adequate resources to support interventions and activities, and the absence of monitoring mechanisms to assess implementation and impact of plans to tackle online child abuse. It calls for better monitoring of media coverage and reporting on children, as well as education and public awareness-raising on the harmful impact of child sexualisation.

It also illustrates the lack of data and information on many aspects of child online sexual abuse and exploitation. Except for a 2011 study on commercial sexual exploitation in selected provinces and cities in Viet Nam, there have not been any other national situational analyses of risks and responses in the ASEAN sub-region.

UNICEF has published a number of reports related to child online safety issues over the past decade, including a similar study, *Child Safety Online: Global Challenges and Strategies* in 2012,[22] focusing on abuse and exploitation online, but also touching upon cyberbullying and the impact of pornographic content on children.

The report considers how children across the world use the Internet, and examines specific online activities and experiences that have the potential to place them at risk. It outlines relevant international law and key challenges to governments and law enforcement agencies, and concludes by proposing a strategic protection framework with four main objectives: (1) empowering children and promoting their resilience; (2) removing impunity for abusers; (3) reducing availability of harmful material from the Internet; and (4) promoting recovery and rehabilitation for children who have experienced harm.

[21] https://www.unicef.org/eapro/Child_Protection_in_the_Digital_Age.pdf.

[22] UNICEF, *Child Safety Online: Global Challenges and Strategies - Technical Report* (Florence, 2012), https://www.unicef-irc.org/publications/pdf/ict_techreport3_eng.pdf.

A Policy Review: Building Digital Citizenship in Asia-Pacific through Safe, Effective and Responsible use of ICT[23]

In 2016, UNESCO surveyed 22 UN member states in the Asia-Pacific to map government-driven policies, specifically national initiatives in the education sector, to foster digital citizenship in schools, and among children, parents and caregivers.

The survey found that government policies to promote ICT opportunities mature alongside those that address potential risks. But while 75% of surveyed states have policies promoting basic ICT literacy skills to children—specifically those in secondary school—less attention is given to training beyond basic ICT literacy, including skills to 'enhance….interactive and critical use of media', as well as constructive online participation and content creation.

More than two-thirds of member states involve multiple sectors, such as law enforcement, health, education and security, in developing cyber safety and privacy policies. What is missing are initiatives to engage with children to gain a better understanding of their perspectives on the opportunities and risks of ICTs. Indeed, the study underlines the lack of rigorously obtained data on children's behaviours and perceptions online among member states in the region, potentially leading to the development and implementation of policy based on general and untested assumptions.

Meanwhile, almost all respondent member states employ content filtering and/or monitoring systems at the local, provincial and/or national levels, viewing these as an essential means of dealing with the risks of ICT use among children. Many do not have assessment programmes in place to measure the efficacy of their policies and procedures.

The report concluded that a balance needs to be struck between issues of safety, mitigation of risk and protection, along with taking up opportunities and benefits provided by ICTs for young persons. Notably, it points out that although learners who seek opportunities in the digital space do face greater threats, a growing body of research suggests that they are also able to learn to cope with them, thus the benefits they gain can ultimately outweigh the risks.

OECD*, The Protection of Children Online* (Paris, 2012)[24]

The Organisation for Economic Co-operation and Development (OECD) member countries include four of the five selected economies with high Internet penetration level—Australia, Japan, Republic of Korea and New Zealand. This publication includes recommendations from the OECD Council on the protection of children online, and a report on the risks faced by children and the policies to protect them. It covers all the all three groups of risks described above—content, usage/conduct and interaction/communication.

The report examines policy measures available to OECD member and non-member countries, compares existing and planned policy approaches, and explores how international cooperation can enhance the protection of children on the Internet.

[23] http://unesdoc.unesco.org/images/0024/002468/246813e.pdf

[24] http://www.oecd.org/sti/ieconomy/childrenonline_with_cover.pdf.

It notes that government policies to protect children online are in their infancy. To catch up with children's rapid Internet adoption, governments need to:

- Manage policy complexity through enhanced coordination, consistency and coherence;
- Adopt an evidence-based policymaking approach; and
- Take advantage of international cooperation to improve the efficiency of national policy frameworks and foster capacity building.

World Bank and the International Centre for Missing & Exploited Children, *Protecting Children from Cybercrime: Legislative Responses in Asia to Fight Child Pornography, Online Grooming, and Cyberbullying* (Washington, D.C., 2015)[25]

Jointly conducted by the World Bank and the International Centre for Missing & Exploited Children, this study provides an overview of 17 Asian countries' legislative responses to online child abuse and exploitation, with a focus on child pornography (or child abuse images), online grooming and cyberbullying. The report covers all but two of the economies –Australia and New Zealand--selected for this study.

It (1) analyses the extent to which existing legislative measures are in line with relevant international practices; (2) presents examples of good practices; and (3) recommends measures to strengthen the national legal framework to address child abuse and exploitation. These include the following:

- Provide a definition of child pornography
- Enact new laws and/or amend existing laws to criminalise activities with specific regard to child pornography, and ensure implementation
- Criminalise an act that aids or abets the commission of child pornography offenses, as well as an attempt to commit such offenses
- Provide appropriate penalties for child pornography offenses
- Take necessary measures to establish extraterritorial jurisdiction over child pornography offenses
- Require ISPs to report child pornography to relevant authorities, and take steps to prevent further transmission of the discovered child pornography
- Criminalise the use of ICTs to commit illicit activities related to child pornography, including downloading, viewing and accessing child pornography
- Criminalise advertising child sex tourism through the Internet and associated technologies
- Adopt legislation to criminalise online grooming
- Introduce legislation regarding cyberbullying
- Raise awareness around the issue of sexting, and develop legislation to combat and prevent sexting

UNICEF, *Child Online Protection in India*, (New Delhi, 2016)[26]

One of the country-specific reports published by UNICEF, this study assesses child online safety in India, and covers children's online usage/conduct and interaction/communication. It focuses on cyberbullying,

[25] http://documents.worldbank.org/curated/en/652251468206670506/pdf/94492-WP-REVISED-PUBLIC-Box385442B-Protecting-Children-from-Cybercrime-Legislative-Responses-in-Asia-to-Fight-Child-Pornography-Online-Grooming-and-Cyberbull.pdf.

[26] http://unicef.in/Uploads/Publications/Resources/pub_doc115.pdf.

online sexual abuse and exploitation, cyberextremism, online commercial fraud, online grooming, habit formation and online enticement to illegal behaviours.

The report examines India's response system to online sexual abuse and exploitation, and takes note of prevention efforts through education, as well as the limitations of existing policies to protect children on the Internet.

Lina Acca Methew, "Online Child Safety from Sexual Abuse in India," Journal of Information Law and Technology, Vol. 1 (2009)[27]

Published in 2009, this academic paper focuses on online grooming, access to sexually explicit content, and the production and reception of online child sexual abuse materials. It compares India's online child safety efforts with those of other countries and calls for a multi-stakeholder approach to child online protection at local, regional and national levels, involving parents, educators, social workers, health care practitioners, law enforcement officers, and businesses.

Chris Berg and Simon Breheny, "Enhancing Online Safety for Children," Institute of Public Affairs, Australia, March 2014[28]

The Institute of Public Affairs in Australia, an independent, non-profit public policy think tank wrote this paper in response to the Australian government's proposal to appoint a Children's e-Safety Commissioner and introduce a new cyberbullying offense. It argues that bullying is not a technological or legal problem, but an educational and social one:

Remedies for bullying that target the medium in which bullying occurs or the legal framework will be ineffective. The only effective way to tackle bullying is through parents, guardians and schools. … New legal remedies for cyberbullying offenses are excessive, in part duplicate existing law, and represent an unacceptable threat to freedom of speech.

It cites institutional and technology tools that children can use to empower themselves to prevent or mitigate bullying, as well as programmes offered by social networks to take down serious abuse.

[27] http://www2.warwick.ac.uk/fac/soc/law/elj/jilt/2009_1/mathew/.

[28] http://ipa.org.au/portal/uploads/submission_to_Enhancing_Online_Safety_for_Children.pdf.

Policy and Actor Analysis

This section examines the legislation and policies, as well as the different actors involved in addressing child online safety issues, and identifies emerging priorities in the selected Asia-Pacific economies.

A. Legislation and Policies

Child Pornography

All selected economies, regardless of their level of Internet penetration, criminalise the production and distribution of child pornography in domestic law:

Economies with High Internet Penetration	Economies with Moderate Internet Penetration	Economies with Low Internet Penetration
• Australia - -Divisions 273 and 474 of the Criminal Code	• China -Article 366 of the Criminal Law	• Bangladesh -Articles 292 and 294 of the Criminal Code -Pornography Control Act 2012 -Article 57 of the ICT Act
• Japan - -Articles 174 and 175 of the Criminal Code -Act on Punishment of Activities Relating to Child Prostitution and Child Pornography, and the Protection of Children -Act on Development of an Environment that Provides Safe and Secure Internet Use for Young People 2008 -Online Dating Site Regulation Law 2003	• Malaysia -Child Act 2001 -Section 293 of the Penal Code -Sections 211 and 233 of the Communications and Multimedia Act 1998	• India -Protection of Children from Sexual Offenses Act 2012 -Sections 67, 67A and 67B of the Information Technology (Amendment) Act
• Republic of Korea - -Articles 243-245 of the Criminal Code -Act of the Protection of Children and Juveniles from Sexual Abuse	• Philippines -Articles 201 and 355 of the Criminal Code -Anti-Child Pornography Act of 2009 -Cybercrime Prevention Act of 2012	• Indonesia -Article 295(1) of the Criminal Code -Law No. 44 of 2008 about Pornography -Law No.11 of 2008 concerning Electronics Information and Transaction
• New Zealand - -Sections 124 and 131B of the Crimes Act -Sections 3 and 127 of the Films, Video and Publications Classficiation Act	• Thailand -Anti-Child Pornography Act of 2009 -Computer Crime Act 2007	• Sri Lanka -Section 3 of the Penal Code (Amendment) Act
• Singapore - -Sections 293 and 376E of the Criminal Code -Section 32 of the Films Act -Sections 11 and 12 of the Publications Act	• Viet Nam -The Law on Information Techonology	

Table 3. List of national legislations related to child pornography in selected economies

According to the International Centre for Missing & Exploited Children (ICMEC)'s Global Review of Child Pornography:[29]

The commercial trade of child pornography online has been significantly reduced due to a variety of successful efforts to combat its growth. There has, however, been an increase in the trade of illicit content between individuals and groups via peer-to-peer networks. The problem has proven to be a persistent one, and strong anti-child pornography legislation is needed in every country to combat it.

The maturity of relevant legislation varies across the region. Those in high Internet penetration economies tend to have a clear and consistent definition of "child" and "child pornography", and include offenses facilitated by all Internet-enabled platforms. Australia, the Philippines and Singapore have gone a step further, introducing legal measures to deal with offenses related to online child grooming.[30]

Laws on child pornography in moderate and low Internet penetration economies are not as comprehensive. In China, Indonesia, Malaysia, Sri Lanka, Thailand and Viet Nam the term "child pornography" is not defined in law.[31]

One of the contentious barriers to a uniform definition of child pornography is the age of consent to sexual relations, which differs from country to country. In addition, legislation differs on whether possession of child pornography is a crime or whether an actual child had to be involved—such as in instances where artificially created images of children are used. In some economies the term "child sexual abuse material" (CSAM) is used instead to emphasise the fact that behind images of child pornography is the sexual abuse of real children. These materials involve children who cannot or would not consent to such acts, and are victims of a crime.

Child pornography is a transnational problem that demands a global response. It is important to harmonise national and international legal standards as inconsistent policies weaken prevention and prosecution efforts, and allow child predators to target countries where they would be best able to exploit children.

The main international legal instrument that addresses child pornography is the **Optional Protocol to the Convention on the Rights of the Child on the Sale of Children, Child Prostitution and Child Pornography (OPSC).** The OPSC defines child pornography as "any representation, by whatever means, of a child engaged in real or simulated explicit sexual activities or any representation of the sexual parts of a child for primarily sexual purposes." It requires countries to criminalise (1) child pornography, whether committed domestically or transnationally, on an individual or organised basis, as well as (2) simple possession regardless of intent to distribute. All the economies in this study have signed and/or ratified the OPSC, except Singapore.

The **Convention on Cybercrime** includes offenses related to child pornography. It recommends that countries prohibit the production, distribution or transmission, procurement, or possession of child pornography in a computer system or on a computer-data storage medium. It also states that "child" should

[29] ICMEC, *Child Pornography: Model Legislation & Global Review*, Eighth Edition (2016), http://www.icmec.org/wp-content/uploads/2016/02/Child-Pornography-Model-Law-8th-Ed-Final-linked.pdf.

[30] UNICEF, *Child Safety Online: Global Challenges and Strategies - Technical Report* (Florence, 2012), https://www.unicef-irc.org/publications/pdf/ict_techreport3_eng.pdf.

[31] ICMEC, *Child Pornography: Model Legislation & Global Review*, Eighth Edition (2016), http://www.icmec.org/wp-content/uploads/2016/02/Child-Pornography-Model-Law-8th-Ed-Final-linked.pdf.

be anyone under the age of 18. Only two of the economies in this study have signed and/or ratified it—Australia and Japan.

Acts for Other Child Online Safety Issues

Economies with high Internet penetration are more likely to have enacted laws on other aspects of child online safety, such as children's exposure to harmful content, cyberbullying and Internet addiction. They are also more likely to have a broad strategy for empowering children to protect themselves online, with government agencies, the private sector and not-for-profit groups working together to provide young Internet users the skills and tools they need to take control of their well-being and strengthen their resilience to risks on the Internet. There however does not seem to be any targeted legislative response to children's online privacy and their protection from information security risks.

Harmful Content

In Japan, the Act on Development of an Environment that Provides Safe and Secure Internet Use for Young People was passed in 2008 and amended a year later.[32] It mandates [33] the:

- Establishment of a national plan for measures to provide safe and secure Internet use for children;
- Promotion of education and awareness-raising activities on appropriate Internet use at the national and local levels; and
- Provision of service to filter harmful content.

The Act compels businesses related to the Internet to filter content harmful to children. These include Internet service providers, mobile service providers, manufacturers of equipment with functions to access the Internet, and software developers.

Content filtering and blocking, often involving blanket takedowns at the national level, is increasingly being used as a risk reduction measure in the region. However, these come with a corresponding danger of restricting Internet users, including young people, from exploring and making full use of the digital space for their personal, educational and social growth[34]. Filtering technologies are prone to two simple inherent flaws: under-blocking and over-blocking. Under-blocking refers to the failure of filtering to block access to all targeted content. On the other hand, they likewise often block content they do not intend to censor, also known as over-blocking[35].

[32] Japan Act on Development of an Environment that Provides Safe and Secure Internet Use for Young People (Act No. 79 of 2008), Latest Amendment (Act No. 71 of 2009), http://www8.cao.go.jp/youth/youth-harm/law/pdf/english.pdf.

[33] In the Act, young people is defined as persons under 18 years of age.

[34] Content blocking and censorship also runs into the risk of making intermediaries such as Internet access providers, social networks and search engines liable for the content hosted on their servers and platforms. It is thus equally important to integrate transparency and accountability into measures that involve third-party filtering or takedowns. For more information on intermediary liability, see the Manila Principles at https://www.manilaprinciples.org/

[35] For more information on the uses and limits of content blocking techniques, see Internet Society, *Perspectives on Internet Content Blocking* (2017), https://www.internetsociety.org/doc/internet-content-blocking; and Internet Society*, Children and the Internet* (2012), https://www.internetsociety.org/sites/default/files/bp-childrenandtheinternet-20129017-en.pdf

Cyberbullying

Recently, Australia, New Zealand, the Philippines and Singapore, have passed laws to protect children against cyberbullying. Australia's Enhancing Online Safety for Children Act 2015.[36]:

- Establishes the office of the Children's e-Safety Commissioner;
- Creates a mechanism whereby harmful cyberbullying material targeted at an Australian child can be removed from social media sites quickly;
- Sets up a scheme for the receipt and investigation of complaints relating to harmful content; and
- Provides the Commissioner with various enforcement powers with respect to both the social media site on which harmful content is posted, and the end-user who posted the harmful content.

New Zealand's Harmful Digital Communications Act in 2015.[37]:

- Establishes a set of guiding Communication Principles under which the Act operates;
- Sets up a government-approved agency to help Internet users who believe themselves harmed by digital communications;
- Creates a new set of court orders that New Zealand's District Courts can serve against Internet hosts or authors, on referral from the Approved Agency;
- Constructs a new set of civil and criminal offenses for creating or propagating "harmful digital communications"; and
- Introduces a new 48-hour content takedown process, whereby individuals can demand online hosting providers to remove content they believe is harmful.

The Philippine Anti-Bullying Act of 2013 requires schools to develop and implement anti-cyberbullying policies, and the Department of Education to issue administrative sanctions for non-compliance.[38]

Singapore 's Protection from Harassment Act, passed in 2014 and revised the following year[39] criminalises cyber- and other forms of harassment offline, including stalking.

These laws however face criticism for criminalising children and for being inconsistent with the right to freedom of expression. Some stakeholders believe that it is more effective to tackle cyberbullying through awareness-raising and education programmes with parents, guardians and schools.[40]

[36] Australia Enhancing Online Safety for Children Act 2015, https://www.legislation.gov.au/Details/C2016C00781.

[37] New Zealand Harmful Digital Communications Act 2015, http://legislation.govt.nz/act/public/2015/0063/latest/whole.html#DLM5711836.

[38] UNICEF, *Child Protection in the Digital Age: National Responses to Online Child Sexual Abuse and Exploitation in ASEAN Member States* (Bangkok, 2016), https://www.unicef.org/eapro/Child_Protection_in_the_Digital_Age.pdf.

[39] Singapore Protection from Harassment Act 2014, Revised Edition 2015, http://statutes.agc.gov.sg/aol/download/0/0/pdf/binaryFile/pdfFile.pdf?CompId:5c68d19d-19ad-49d8-b1a9-5b8ca8a15459.

[40] Chris Berg and Simon Breheny, "Enhancing Online Safety for Children," Institute of Public Affairs,Chris Berg and Simon Breheny, "Enhancing Online Safety for Children," Institute of Public Affairs, Australia, March 2014, http://ipa.org.au/portal/uploads/submission_to_Enhancing_Online_Safety_for_Children.pdf.

Internet Addiction

Chapter 3 of the Republic of Korea Juvenile Protection Act, passed in 2014.[41] deals with preventing juvenile addiction to Internet games. In addition, Article 23 of the Act aims to protect children from harmful content online.

Chapter 3 consists of four articles on Internet addiction:

- Article 24 requires a parental authority's consent prior to a minor's use of Internet games;
- Article 25 requires Internet game providers to specify the game's appropriateness for a particular age group, and inform parents or legal guardians on any payments related to the product;
- Article 26 "restricts the provision of Internet games to juveniles under the age of 16 between 12 midnight and 6am; and
- Article 27 details the support given for juveniles afflicted with addiction to Internet games by the, Ministry of Gender Equality and Family.

Other countries in the region, such as China, have begun to address Internet addiction through measures like rehabilitation programmes and by limiting permissible hours for children in Internet cafes.

An important international legal instrument that addresses child safety and protection online is the Convention on the Rights of the Child, which all selected economies have signed and ratified. Specific provisions, such as Article 19, requires countries to take appropriate legislative, administrative, social and educational measures to protect the child from all forms of physical or mental violence, injury or abuse, neglect or negligent treatment, maltreatment or exploitation, including sexual abuse.

The Committee on the Rights of the Child has affirmed that Article 19 applies to violence through information communication technologies (ICTs), including sexual abuse for the production and dissemination child abuse images; exposure to harmful material; bullying; harassment; or being groomed for sexual activities.[42] In addition, Article 16 recognises children's right to privacy, and Articles 13, 15 and 17 make governments responsible for ensuring children's freedom of expression, freedom to seek information and freedom of association, all which are relevant to the benefits that the Internet provide.

Online Consent

More recently in Vietnam, a new regulation to take effect this year requires Internet users to obtain permission from children or their legal guardians prior to posting the information of anyone below 16 years of age online. This includes the child's name, age, images, address, distinguishing features and health conditions. The policy also entitles children and their parents to demand authorities and online service providers to remove private information about them on the Internet.[43]

[41] Republic of Korea Juvenile Protection Act 2014, http://elaw.klri.re.kr/eng_service/lawView.do?hseq=32537&lang=ENG.

[42] UNICEF, *Child Safety Online: Global Challenges and Strategies - Technical Report* (Florence, 2012), https://www.unicef-irc.org/publications/pdf/ict_techreport3_eng.pdf.

[43] "Vietnam steps up child protection with new Internet law", Vietnam Breaking News, 16 May 2017,

https://www.vietnambreakingnews.com/2017/05/vietnam-steps-up-child-protection-with-new-internet-law/

Child Online Safety Implementation: Policies and Plans

It must be emphasised that drafting and implementing legislation are only among the many steps that can be taken by governments: legal measures alone are insufficient to address child online safety issues. Other approaches that include education, awareness-raising and cooperation with stakeholders - including young people and children themselves- are key.

Economies with High Internet Penetration	Economies with Moderate Internet Penetration	Economies with Low Internet Penetration
• Australia -The National Safe Schools Framework • Japan -Responses to Online Bullying -Information Moral Education	• Malaysia -National Child Protection Policy -Plan of Action on Child Online Protection • Philippines -Child Protection Against Online Sexual Abuse and Exploitation Program • Viet Nam -Joint Circular on Management of Online Games	• India -National Policy on Information and Communication Technology -National Advisory on Preventing and Combating Cyber Crime against Children, 2012

Table 4. List of policies and plans related to online child safety in selected economies

Australia and Japan have education policies for online child empowerment. In Japan, it is mandatory for elementary school students to take an "Information Moral Education" course. In Australia, the National Safe Schools Framework provides Australian schools with a set of guiding principles to develop student safety.[44]

Malaysia's National Child Protection Policy and Plan of Action on Child Online Protection is consistent with the Convention on the Rights of the Child and the country's Child Act 2001. The policy does not explicitly address the protection of children online, but it can be applied to both the offline and online environment.[45] Drafted in 2015, the Plan of Action on Child Online Protection has four focus areas: (1) advocacy and awareness-raising; (2) prevention of online child abuse; (3) interventions in identified cases, and (4) support for victims and their families.[46] These will be carried out by the assigned lead agencies: the Women, Family and Community Development Ministry; the Science, Technology and Innovation Ministry; the Education Ministry; the Home Ministry, the Malaysian Communication and Multimedia Commission (MCMC) and Malaysian Royal Police.

In the Philippines, the Department of Social Welfare and Development, the Department of Justice and the Asia Foundation launched a three-year programme with support from the Australian Government and

[44] Australian Government Department of Education and Training, "The National Safe Schools Framework," http://education.gov.au/national-safe-schools-framework-0.

[45] Ministry of Women and Family Development, "National Child Protection Policy," http://www.jkm.simple.my/content.php?pagename=dasar_perlindungan_kanak-kanak_negara&lang=en.

[46] Ministry of Women and Family Development, "Child Online Protection in Malaysia," http://www.childhelplineinternational.org/media/154436/1-ministry-ptcop.pdf; and Open Gov, "Malaysia online child protection plan ready for action, says Minister," 27 March 2015, http://www.opengovasia.com/articles/6357-malaysian-online-child-protection-plan-ready-for-action-says-minister.

UNESCO. The Philippines Child Protection Against Online Sexual Abuse and Exploitation Programme aims to develop the capacity of the court system, police, social services and the education sector on issues related to child online sexual abuse and exploitation. Its components include:[47]

- Drafting a Sex Offender Registration and Notification Act;
- Advocating for child-friendly rules in family courts;
- Establishing community-based, multi-sector and local task forces in selected pilot areas to serve as Child Protection Quick Reaction Teams;
- Legal audit of online child sexual abuse cases in courts; and
- Public information and education campaigns on the rights of children against online sexual abuse and exploitation, and multi-sector training of those involved in the justice system.

In 2015, the Viet Nam Ministry of Information and Communication (MIC) issued a circular to govern the production, provision and use of online gaming services. It limits the time that children under the age of 18 can spend playing an online game to no more than 180 minutes per day.[48]

India's National Policy for Children was adopted in 2013 to guide all laws, policies, plans and programmes affecting children. It includes the protection of children, and calls for measures to:[49]

- Provide access to ICT tools for equitable, inclusive and affordable education for all children especially in remote, tribal and hard to reach areas; and
- Promote safe and enjoyable engagement of children with new technology in accordance with their age and level of maturity, taking into consideration respect for their own culture and roots.

The Indian Government's National Advisory on Preventing and Combating Cyber Crime against Children, prepared in 2012, provides a set of guidelines to help state agencies minimise cases of cybercrime against young Internet users. The government is also planning to establish a National Cyber Crime Coordination Centre with a dedicated unit for cyber offenses against women and children.

Regional and International Policies, Plans and Initiatives

There is a growing number of agreements to help promote coordination and cooperation among APAC economies in tackling child online safety issues. Those with high Internet penetration and increasingly, those with moderate Internet penetration, are joining global networks that can support their domestic initiatives to tackle child online safety issues.

In 2013, ASEAN leaders adopted the Declaration on the Elimination of Violence against Women and the Elimination of Violence against Children. The **ASEAN Regional Plan of Action on the Elimination of Violence**

[47] Australian Minister of Foreign Affairs, "Philippines Child Protection Against Online Sexual Abuse and Exploitation Program Launch," Speech on 17 November 2015, http://foreignminister.gov.au/speeches/Pages/2015/jb_sp_151117a.aspx?w=tb1CaGpkPX%2FlS0K%2Bg9ZKEg%3D%3D; and D. J. Yah, "Aussie-funded project needs sex offenders' registry in PH, *Philippine Daily Inquirer*, 21 November 2015, http://globalnation.inquirer.net/132529/aussie-funded-project-needs-sex-offenders-registry-in-ph.

[48] http://en.nhandan.com.vn/society/item/3057302-vietnam-introduces-measures-to-regulate-online-games.html

[49] Government of India, Ministry of Women and Child Development, National Policy for Children, 2013, http://www.childlineindia.org.in/pdf/The-National-Policy-for-Children-2013.pdf.

against Children, approved in 2015, includes the development of preventive measures against online violence as a priority action.[50]

The **Asia-Pacific Financial Coalition Against Child Pornography** (APAC-FCACP), an initiative of ICMEC, was launched in 2009 to fight against the online sale and dissemination of child sexual exploitation materials. APAC-FCACP members include banks, credit card companies, online third-party payment systems, technology companies, social networking platforms, industry associations and law enforcement agencies.[51]

The Child Online Protection (COP) Initiative of the International Telecommunication Union (ITU) has emerged as an international platform for dialogue, engaging with multiple stakeholders[52] to develop child online protection guidelines for: (1) children; (2) parent, guardians and educations; (3) industry; and (4) policymakers. ITU has also come up with comparable indicators to measure various aspects of child online safety.[53]

The **Dynamic Coalition for Child Online Safety** at the Internet Governance Forum (IGF) aims to create an open avenue for the discussion of fundamental and practical issues related to child online safety among representatives from children's organisations, government, industry, academia and other civil society groups.[54]

The **International Association of Internet Hotlines** (INHOPE)[55] collects reports of illegal online activities using 51 hotlines in 45 countries. Its members include Australia, Japan, Republic of Korea and New Zealand INHOPE Foundation likewise supports hotlines in Cambodia and Thailand. The network allows countries to coordinate and exchange information among themselves, and with law enforcement and ISPs, particularly in reporting and removing illegal content that is hosted abroad..

Insafe, a European network of awareness centres for child online protection, organises the annual Safer Internet Day every February, and involves numerous countries outside Europe.[56]

The **Virtual Global Taskforce for Combating Online Child Sexual Abuse**[57] is an international alliance of law enforcement agencies, non-governmental organisations (NGOs) and industry players. Members include the Australian Federal Police, Indonesian National Police, Korean National Police Agency Cyber Bureau, Philippine National Police Anti Cybercrime Group and the New Zealand Police.

INTERPOL, the world's largest international police organisation, counts all of the selected economies in this report as its members. INTERPOL's International Child Sexual Exploitation database has identified more than 8,200 victims around the world, with an average of seven child victims found every day in 2015. Its Baseline project works with private entities to encourage industry and network administrators to recognise, report and remove child abuse material from their networks. It provides support to member countries in locating and arresting travelling sex offenders. The INTERPOL Specialists Group on Crimes Against Children brings together experts to share best practices and information on the apprehension of child sex offenders and

[50] Ibid.

[51] ICMEC, "Asia-Pacific Financial Coalition Against Child Pornography," http://www.icmec.org/apac-fcacp/.

[52] For a list of organisations involved in the ITU COP initiative, see http://www.itu.int/en/cop/Pages/partners.aspx.

[53] See ITU, "Child Online Protection," http://www.itu.int/en/cop/Pages/default.aspx.

[54] Internet Governance Forum, "Dynamic Coalition on Child Online Safety," http://igf.wgig.org/dynamic_coalitions.php?listy=13.

[55] INHOPE, http://www.inhope.org/gns/home.aspx.

[56] Wikipedia, "Insafe," https://en.wikipedia.org/wiki/Insafe.

[57] Virtual Global Taskforce for Combating Online Child Sexual Abuse, http://virtualglobaltaskforce.com/.

their treatment and management within the community. It is also a member of the Virtual Global Taskforce for Combating Online Child Sexual Abuse.[58]

The **WePROTECT Global Alliance to End Child Sexual Exploitation Online** combines the Global Alliance, led by the US Department of Justice and the EU Commission, and WePROTECT, convened by the UK. It involves 70 member countries, along with major international organisations, 20 global technology corporations including Google, Facebook, Microsoft and Tencent, and 17 civil society organisations. Australia, Japan, the Republic of Korea, New Zealand, the Philippines and Thailand are members. These countries commit to four policy targets that aim to: (1) identify, support and protect victims; (2) identify and prosecute offenders; (3) raise awareness; and (4) reduce the availability of child pornography online.[59] Soon after the merger in June 2016, WeProtect Global Alliance launched the Global Partnership and Fund to End Violence Against Children, in partnership with UNICEF and World Health Organization, and supported by a multi-donor fund.[60]

ECPAT International is a global network of 90 civil society organisation in 82 countries, including most of the economies in this study (Singapore is not a member). It focuses on eliminating child prostitution, pornography and trafficking for sexual purposes. ECPAT runs a programme to combat the sexual exploitation of children online, and aims to:

- Develop and implement stronger legal frameworks;
- Widely deploy technical tools to reduce the availability of child sexual abuse material online;
- Provide capacity building for law enforcement to identify and care for victims; and
- Drive public information and awareness-raising to support behavioural change.

B. Actor Analysis

Child online safety requires the involvement and cooperation of various stakeholders at local, national, regional and international levels. This section gives a snapshot of the different actors involved in child online safety in the selected economies.

Economies with High Internet Penetration

Australia

Australia's Enhancing Online Safety for Children Act in 2015 established the Office of the Children's e-Safety Commissioner. The Office provides online safety education for Australian children and resources for parents, as well as a complaints service for cyberbullying victims. It also addresses illegal online content. Specifically, it runs the Budd:E Cybersecurity Education[61] platform, an interactive tool for young people, and

[58] Virtual Global Taskforce for Combating Online Child Sexual Abuse, "Member Countries," http://virtualglobaltaskforce.com/who-we-are/member-countries/.

[59] WeProtect Global Alliance to End Child Sexual Exploitation Online, http://www.weprotect.org/; and European Commission, "A Global Alliance against Child Sexual Abuse Online," http://ec.europa.eu/dgs/home-affairs/what-we-do/policies/organized-crime-and-human-trafficking/global-alliance-against-child-abuse/index_en.htm.

[60] Baroness Joanna Shields, "When My Time is Up, Have I Done Enough? - Global Mission to Eradicate Child Sexual Exploitation," *Huffington Post,* 24 July 2016, http://www.huffingtonpost.co.uk/baroness-joanna-shields/child-sexual-exploitation_b_11140074.html.

[61] https://budd-e.cybersmart.gov.au/

a free mobile app, Cybersafety Help Button[62], that provides Internet users, particularly children, with easy access to online safety information and assistance. The service likewise offers counselling, reporting and materials to help young people deal with online risks.

The Department of Education works closely with the Department of Communications, which along with the Australian Communications and Media Authority is primarily responsible for cybersafety matters,.[63] It makes available online safety education to children, parents, guardians and teachers, and operates the "Safe Schools Hub", a one-stop shop for relevant information and resources. Another website for schools is "Bullying No Way!" which has an online curriculum and other resources related to bullying online and offline.[64]

Platforms such as Digital Licence,[65] offer certification programmes on digital reputation, well-being and safety for different age groups. Global organisations, such as UK-based Think You Know, and Cyber Safe Kids are also involved in empowering young people in Australia through guidance, workshops and training. More locally, Telstra, along with the Queensland Government, has launched a game, "Creep Quiz: Are U Safe Online"[66], to help children safely navigate social media sites.

Japan

In Japan, the Ministry of Education, Culture, Sports, Science and Technology trains teachers, and encourages students to "acquire the basic attitude for behaving appropriately in the information society" through its model curriculum for information morals education.[67]

Likewise, the National Information Security Center emphasises education on cyberethics.[68] The Content Evaluation and Monitoring Association, established upon the recommendation of the Ministry of Internal Affairs and Communications, is a third-party organisation that certifies and tracks the operation of mobile Internet service providers. It is involved in the filtering of harmful content and in educational activities to improve digital literacy.[69]

[62] https://www.esafety.gov.au/complaints-and-reporting/cybersafety-help-button

[63] Other organisations or initiatives working on online child safety in Australia are: the Australian Cybercrime Online Reporting Network (http://www.acorn.gov.au); Bully Zero Australia Foundation (http://bzaf.org.au); Daniel Morcombe Foundation (http://www.danielmorcombe.com.au); Education Services Australia (http://www.esa.edu.au); Kids Helpline (http://www.kidshelpline.com.au); Lawstuff (http://www.lawstuff.org.au); National Association for Prevention of Child Abuse and Neglect (http://www.napcan.org.au); National Center Against Bullying (https://www.amf.org.au); Reachout.com (http://www.au.reachout.com); Stay Smart Online (http://www.staysmartonline.gov.au); The Line (http://www.theline.org.au); ThinkUKnow (http://www.thinkuknow.org.au)

[64] Australian Government Department of Education and Training, "Cybersafety in schools," https://www.education.gov.au/cybersafety-schools.

[65] https://www.digitallicence.com.au/--Digital Licence is now available in New Zealand.

[66] http://www.creepquiz.eq.edu.au/index.html

[67] Ministry of Education, Culture, Sports, Science and Technology, "Promotion of information morals education at school to acquire the basic attitude for behaving appropriately in information society," http://www.mext.go.jp/b_menu/hakusho/html/hpac200701/1283225_004.pdf.

[68] Cyberethics is the use of appropriate and ethical behaviours and acknowledging moral duties and obligations pertaining to online environments and digital media, although what is and is not cyberethical behaviour varies from country to country. iKeepSafe, "Cyber-ethics," http://ikeepsafe.org/educators_old/more/c3-matrix/cyber-ethics/.

[69] Content Evaluation and Monitoring Association, "An Introduction to the Content Evaluation and Monitoring Association," https://www.ema.or.jp/en/dl/introduction.pdf.

The not-for-profit Japan Internet Safety Promotion Association has a multi-stakeholder approach to child online safety—the Anti-Child Pornography Working Group deals with information on relevant international responses as well as legal and technical measures in Japan; while the Social Game Working Group tackles problems related to gaming among children and young people.[70] Meanwhile, the Safer Internet Association, whose members include Yahoo Japan and local ISP Sakura Internet, receives reports from the public on potentially harmful online content, and also trains instructors to provide Internet safety courses for both children and adults[71]

Republic of Korea

In the Republic of Korea, the Ministry of Gender Equality and Family screens harmful content on the Internet by reporting it to the Korea Communications Standards Commission (KCSC), through its Illegal and Harmful Information Report Center and the Game Rating and Administration Committee, which subsequently send blocking requests to online portals. The harmful content is listed with the Parents' Union on Net.[72] KCSC also SafeNet, which has a website rating system and provides information on content filters.

The National Information Society Agency (NIA) works with various government agencies, including the Ministry of Science, ICT and Future Planning (MISP) to raise awareness on cyber ethics and cyberbullying issues among children, parents, guardians and educators. NIA and MISP aim to prevent smartphone addiction through their Smartmedia Clean School Programme.

New Zealand

In New Zealand, the Department of Internal Affairs provides information on censorship and Internet child safety, including guidelines for parents and interactive sites for children. Its website has an online safety agreement template to help parents establish some rules for children's Internet use.[73]

The Office of the Privacy Commissioner[74], which administers the country's Privacy Act, has partnered with NetSafe and the New Zealand National Commission for UNESCO to launch OWLS[75], a resource that teachers can use to orient students on concepts like online privacy. Its Youth Privacy Kit,[76] co-developed by young people, has guidance notes and ideas for presenters, and includes a variety of youth-oriented activities.

Netsafe,[77] a not-for-profit organisation funded by the Ministry of Education[78], InternetNZ and other partners, produces a range of materials on online safety for children of different age groups, as well as for

[70] Japan Internet Safety Promotion Association, "Outline of JISPA," http://www.good-net.jp/english/.

[71] https://www.saferinternet.or.jp/edu/

[72] Researcher's interview with Google staff.

[73] New Zealand Department of Internal Affairs, "Child Safety Online," https://www.dia.govt.nz/Censorship-Child-Safety-Online.

[74] New Zealand Privacy Commissioner, "Introduction," https://privacy.org.nz/about-us/introduction/.

[75] Netsafe, "OWLS. Wise Words on Privacy," https://www.netsafe.org.nz/owls-wise-words-on-privacy/.

[76] Privacy Commissioner, "Youth Privacy," https://www.privacy.org.nz/your-rights/young-people/youth-privacy/.

[77] Netsafe, "About Netsafe," https://www.netsafe.org.nz/aboutnetsafe/.

[78] The Ministry of Education also makes available content filters on its website: www.education.govt.nz/school/running-aschool/technology-in-schools/safe-and-secureinternet/

teachers, parents and businesses. It has played a key role in drawing up a framework for digital citizenship for the country's educational system. Such efforts are complemented by resources offered by other institutions like the National Library of New Zealand, which provides guidance to school libraries to cultivate digital literacy among students.[79]

As an "approved agency" under the Harmful Digital Communications Act, Netsafe can receive, assess and investigate complaints about harm caused to individuals by digital communications via its Online Operating Button (ORB) website[80]. It is a member of INHOPE, and partners with public, private and civil society groups, including Microsoft and Google, to promote online safety issues.

The 'Online Child Exploitation Across New Zealand' (OCEANZ), a specialist unit of the New Zealand Police, is part of the Virtual Global Taskforce. It identifies child sexual offenders and child exploitation sites; works with district-based child exploitation squads and the Department of Internal Affairs and Customs; and coordinates international investigations.[81]

The website Connect Smart, a multi-stakeholder initiative led by the National Cyber Policy Office,[82] provides resources on online safety for children, parents, schools and businesses.

Singapore

In Singapore, the government-backed Media Literacy Council[83] develops public awareness and education programmes on cyberwellness. This includes cyberbullying, making virtual friends, sharing personal information, cybersecurity, inappropriate content and Internet addiction. It also takes charge of organising the annual Safer Internet Day.

The Ministry of Communications and Information's Cyber Security Agency (CSA) manages the website "GOsafeonline" which contains tips on how to safely use social networks, as well as resources for parents.[84] Recently, CSA has collaborated with the Singapore Personal Data Protection Commission to develop a series of Student Activity Books to raise awareness on cybersecurity and personal data protection.[85]

The examples above indicate that economies with high Internet penetration are actively working to address a variety of child online safety issues, both through top-down approaches to limit and respond to children's exposure to online harm, and increasingly, through initiatives to enable children, parents and educators to take charge of minimising the dangers that young people face online. Most are led by the public sector, but many involve public-private-civil society partnerships.

It must be noted that no single actor takes charge of all digital skills training for young people—programmes have been initiated by different government agencies, as well as non-government organisations, but always with the involvement of other stakeholders.[86]

[79] https://natlib.govt.nz/schools/digital-literacy/connections-to-digital-citizenship

[80] http://www.theorb.org.nz/

[81] New Zealand Police, "Online Child Safety," http://www.police.govt.nz/advice/email-and-internet-safety/online-child-safety.

[82] Connect Smart, "About," http://www.connectsmart.govt.nz/about/.

[83] Singapore Media Literacy Council, http://www.medialiteracycouncil.sg.

[84] GOsafeonline, https://www.csa.gov.sg/gosafeonline.

[85] GOsafeonline, "Cyber Security Activity Book," 15 November 2016, https://www.csa.gov.sg/gosafeonline/resources/activity-book.

[86] In Taiwan, where some 84% of the population are online, a not-for-profit group, iWin, receives complaints about content that may

As economies with high Internet penetration are generally high-income economies, the public sector tends to be better resourced to lead and coordinate child online safety measures.

Economies with Moderate Internet Penetration

Malaysia

In Malaysia, the Ministry of Women, Family and Community Development's Child Online Protection Taskforce, comprised of relevant ministries and agencies, helps to mitigate online threats and crimes such as cyberbullying, pornography, sexting and cybergrooming. It also led the development of the Plan of Action on Child Online Protection, in coordination with other government agencies.

The Malaysian Communications and Multimedia Commission (MCMC) is tasked with prohibiting offensive content as well as promoting public education on content-related issues. MCMC has since 2012 been collaborating with different stakeholders to carry out the Klik Dengan Bijak (Click Wisely Programme),[87] which aims to raise online safety awareness among children and young people, as well as parents, guardians and other caregivers.[88]

The Ministry of Education, along with Cybersecurity Malaysia--an agency of the Ministry of Science, Technology and Innovation--and mobile service provider DiGi Telecommunications implements the CyberSAFE Programme to raise awareness of online safety issues among children, parents and educators. It conducts the annual CyberSAFE in Schools National Survey to investigate the extent to which children are exposed to online risks and harm,[89] and more recently has partnered with UNICEF to organise a Digital Citizen Camp for schoolchildren to help nurture peer-to-peer learning on positive conduct on the Internet. Locally, Digi carries out Telenor's global 'Be a Cyberhero' campaign, which aims to engage four million children by 2020 in online safety practices. Along with Digi, the Malaysia Digital Economy Corporation (MDEC) is developing a digital citizenship module for schools, as well as for the #mydigitalmaker Mobile Learning Unit that will make its way to rural areas across the country.

Philippines

The Inter-Agency Council Against Child Pornography (IACACP),[90] comprised of 12 governmental and three non-governmental organisations, was established in 2010 to coordinate, monitor and oversee the implementation of the Anti-Child Pornography Act of 2009. The Philippine Department of Social Welfare and Development leads the #StopChildPornPH initiative, launched in 2016, to provide online safety

be inappropriate for children, as well as those that might violate a child's online privacy. It liaises with the sector's regulatory body, the National Communications Commission, as well as other government agencies to rectify or remove harmful content on the Internet. It has, in the past in the past partnered with content providers like Facebook to conduct online safety workshops fur students and parents.

[87] Klik Dengan Bijak, http://www.klikdenganbijak.my/?lang=en-GB.

[88] Partners include the Ministry of Communications and Multimedia; Ministry of Education; Ministry of Science, Technology and Innovation; Ministry of Women, Family and Community Development; Ministry of Youth and Sports; Royal Malaysian Police; National Service Training Department; Communications and Multimedia Content Forum; Scouts Association; Kidzania.

[89] CyberSAFE, http://www.cybersafe.my/en/.

[90] IACACP, http://www.iacacp.gov.ph/.

education for children, parents, guardians and service providers. The government also works with UNICEF and various NGOs on child online safety issues (see section on UNICEF below).

Earlier this year, the National Telecommunications Commission ordered ISPs to block adult pornographic sites, pursuant to the country's Anti-Child Pornography Law[91]—the move has been criticised for restricting freedom of expression online. The regulator had previously issued a memorandum, back in 2014, for Internet service providers to prohibit access to websites with child pornography content.

The Department of Education has partnered with local not-for-profit Stairway Foundation to launch a series of CyberSafe Project Manuals, which contain lesson plans for educators; and with mobile operator Globe Telecom to roll out the latter's Digital Thumbprint Programme to help nurture responsible behaviour in public schools across the country.

Thailand

In Thailand, the Department of Children and Youth of the Ministry of Social Development and Human Security leads the development of a Strategy for Child and Youth Online Protection and Enhancement.[92]

Mobile operator DTAC, owned by Telenor, has launched a number of initiatives to drive online empowerment among young people in the country. Under its Safe Internet project, supported by the National Broadcasting and Telecommunications Commission (NBTC) and the Ministry of ICT, it has organised talk show pilots in several cities, anti-cyberbullying campaigns, summer camps, and has created the Thai Digital Citizen Hub for children to share their concerns and coping strategies online.

Meanwhile, the not-for-profit Internet Foundation for Development of Thailand conducts training and develops resources on online safety for children, parents and teachers[93]. It also operates the Thai Hotline[94] with support from INHOPE Foundation, and in partnership with the Ministry of ICT, law-enforcement agencies, ISPs, web hosting services and child protection organisations.[95] The hotline allows anyone to report cases of online child sexual abuse and exploitation, privacy violations, and any content that is illegal under Thai legislation, and works with partners to process legal actions.

The Ministry of Justice and the Ministry of ICT launched a Cyber Scout Programme in 2010, recruiting students and young volunteers to monitor online content that deemed potentially offensive.[96]

[91] The Philippines' Anti-Child Pornography Act has been criticised for having a mandatory filtering provision, to be implemented by ISPs with instructions from the NTC, which in turn acts upon the recommendations of the IACACP. The clause has likewise drawn flak from civil society organisations as an ineffective measure in stemming both the local production of and the foreign consumption of child porn originating from the country, one of the top sources of child pornography worldwide.

[92] Rattana Jaroonsaksit, "Kingdom of Thailand: Child Online Protection Initiatives," presentation made on 13 September 2016, http://www.itu.int/en/ITU-D/Regional-Presence/AsiaPacific/Documents/Events/2016/Sept-COP/Presentation/Thailand_COP_Initiative.pdf.

[93] http://www.inetfoundation.or.th/

[94] Thai Hotline, http://report.thaihotline.org/en.

[95] Thai Hotline, "Partners," http://newreport.thaihotline.org/en/partner.

[96] Cyber Scout, http://www.cyberscout.in.th/home.php.

Vietnam

SecDev Foundation, a cyber-research think tank based in Canada, is helping to spur discussions around digital citizenship in Vietnam. It's Chong Hack[97] campaign encourages young people to secure their accounts on social media. More recently, it marked Safer Internet Day with a multi-stakeholder symposium to promote digital literacy and online child protection in the country.

Overall, the public sector in economies with moderate Internet penetration has begun to address safety issues for children in cyberspace, albeit less rigorously than those with high Internet penetration. In the former, other actors - from the private sector to NGOs and international organisations - are becoming more and more involved in projects to promote online child protection. It is worth noting that many of the initiatives are public-private-civil society partnerships.

UNICEF

UNICEF has been supporting research that will guide policymaking and help raise public and stakeholder awareness with regards to online child protection

At the regional level, the UNICEF East Asia Pacific Regional Office and Child Rights Coalition Asia jointly launched an awareness-raising programme that develops and distributes child-friendly materials with the involvement of children. Children from Cambodia, Hong Kong, Indonesia, Malaysia, Myanmar, Philippines, Thailand and Viet Nam came up with a campaign called #SafeWeb4Kids, which emphasised that children can protect themselves and their peers from violence in cyberspace.[98]

In the Philippines, it conducted a National Baseline Survey on Violence Against Children in 2015. The following year, UNICEF signed a Memorandum of Understanding (MoU) with Globe Telecom and the Ateneo Human Rights Center to combat and prevent online child sexual exploitation and cyberbullying. A study will be conducted to determine how Globe, a major carrier, could integrate child rights into its business principles. The partnership aims to help further develop the Digital Thumbprint Programme, a school-based workshop adopted by Globe from Optus of Australia.[99] To better understand Filipino children's online behaviour, UNICEF has commissioned the University of the Philippines Manila – National Institute of Health to localise and implement the EU Kids Online Survey, which should provide an overview of children's online access, use, risk, coping strategies and safety awareness in pilot areas. UNICEF is also supporting the Philippines in undertaking a comprehensive study on the scope and trends of online child abuse and exploitation.[100]

In Viet Nam, UNICEF partnered with Yahoo! in 2011 to launch Yahoo! Safety Viet Nam. The initiative promotes children's responsible use of the Internet, and aims to curb cyberbullying and other forms of abuse and exploitation. It aims to help parents and educators identify online risks that may impact families,

[97] https://chonghack.com/

[98] Child Rights Coalition Asia, "CRC Asia and UNICEF Launch Online Child Safety Campaign #SafeWeb4Kids," http://childrightscoalitionasia.org/crc-asia-and-unicef-launch-online-child-safety-campaign-safeweb4kids/.

[99] UNICEF, "Globe, UNICEF Philippines, Ateneo sign MoU on online child protection," https://www.unicef.org/philippines/media_25571.html#.WDsg91zvccQ.

[100] UNICEF, *Child Protection in the Digital Age: National Responses to Online Child Sexual Abuse and Exploitation in ASEAN Member States* (Bangkok, 2016), https://www.unicef.org/eapro/Child_Protection_in_the_Digital_Age.pdf.

students and communities.[101] More recently in Malaysia, it partnered with Digi Communications to launch a parental guidebook to promote safe Internet experience for children on social media.

Economies with Low Internet Penetration

Bangladesh

In 2011, Ministry of Social Welfare' Department of Social Services, in partnership with a local NGO and with support from UNICEF, piloted a Child Helpline which in 2015 was extended to other areas in the country.[102]

A recent survey by Telenor, a mobile service provider, found that almost half of the 1,896 urban students[103] , polled experienced cyberbullying.[104]

India[105]

In India, child pornography is reported to the Police Cybercrime Cell, which seeks clearance from the Department of Telecommunications, and from the Ministry of Electronics and Information Technology (MeitY) to block sites containing illegal content.

Google has worked with MeitY and the Computer Emergency Response Team-India to organise Internet safety campaigns, including its Web Rangers initiative to foster peer-to-peer learning on digital footprint management among teenagers. The Internet and Mobile Association of India has likewise partnered with Opera Software for its 'Safe Surfing' initiative, and with Facebook to train young students, teachers and parents on community awareness and Internet safety practices.

Local not-for-profit Aarambh collaborated with the UK-based Internet Watch Foundation to establish a national hotline for reporting, removing and blocking CSAM. NGOs like Aarambh, the Tulir Centre for the Prevention and Healing of Child Sexual Abuse, and the Centre for Cyber Victim Counselling are among the organisations providing recovery and care for victims of child online abuse and exploitation.

Standalone programmes exist, although many have limited reach: The Data Security Council of India, an industry association, has conducted awareness raising campaigns for children and adults on cybersecurity and cybercrimes. Private sector organisations like Intel Security, Microsoft and Telenor target children and/or parents in their online safety programmes, and tackle issues related to abuse, bullying and malware.

Information on the country was drawn largely from the UNICEF study. India, when compared with those of moderate and high Internet penetration has weaker legislation and actors are less coordinated in tackling child online safety issues.

[101] UNICEF, ""Yahoo! Safely" Launched To Help Create a Safer Internet Environment For Users In Viet Nam," 31 May 2011, https://www.unicef.org/vietnam/media_16185.

[102] UNICEF, "Child Help Line offers protection against cyber crime," http://www.unicef.org/bangladesh/media_9966.htm.

[103] Respondents were between 12-18 years old

[104] Daily Sun, "49pc school students in Bangladesh have encountered cyberbullying," 10 February 2016, http://www.daily-sun.com/printversion/details/113098/49pc-school-students-in-Bangladesh-have-Encountered-Cyber-bullying-.

[105] The reference for this sub-section is UNICEF, *Child Online Protection in India* (New Delhi, 2016), http://unicef.in/Uploads/Publications/Resources/pub_doc115.pdf.

Emerging Priority Issues

This study finds that all selected economies with high Internet penetration have relatively stronger legislation and policies to address a variety of child online safety issues. These are also high-income economies where the public sector is more likely to have greater capacity and is better resourced to lead such measures. Notably, these economies have begun to prioritise online child empowerment alongside online sexual abuse and other concerns related to online child protection.

Countries with moderate and low Internet penetration are starting to more actively support digital skills training initiatives for children, but overall continue to focus on online sexual abuse and exploitation through a range of measures—legal, policy, technical, social and educational. However, regional and international studies have reported that these are less effective and less well-coordinated.

There is an urgent need to harmonise relevant laws, and bring them in line with the **Optional Protocol to the Convention on the Rights of the Child on the Sale of Children, Child Prostitution and Child Pornography** (OPSC). Countries have highlighted difficulties in extraditing and prosecuting transborder crimes, due to the "dual criminality"[106] clause--extraterritorial legislation that requires an act to be a crime in both the country where it took place and the country where the suspect resides.[107]

Online grooming, a relatively new phenomenon, has yet to be universally criminalised. In the selected economies in this study, only Australia, the Philippines and Singapore have introduced legal measures to prohibit it. Preventing online grooming is important[108] as it often precedes the creation or distribution of child pornography, in that by the time intent to meet the child has been expressed, s/he is likely to already have been exploited online. Targeted legislation may help to prevent latent or previously undetected sex offenders from targeting children.

Another priority issue in many of the selected economies is cyberbullying, and various studies and surveys have been conducted to try and understand it. Australia, New Zealand, Philippines and Singapore have passed laws against it, but because children are often the perpetrators of cyberbullying, these laws also face criticism for criminalising children and being inconsistent with the right to freedom of expression.

Addiction has likewise emerged as a significant concern in some countries. The Republic of Korea is addressing game addiction as well as smartphone and Internet addiction problems through its Smartmedia Clean School Programme.[109] Similarly, in China and India, there are camps or centres to rehabilitate and counsel children suffering from Internet addiction.

Such concerns are complex as they involve children's behaviour, as well as their social interactions online. It is in addressing these challenges that education and awareness-raising among children, parents, guardians and educators become critical. Additionally, peer support initiatives, wherein older children mentor

[106] Dual criminality is a requirement in the extradition law of many countries. It states that a suspect can be extradited from one country to stand trial for breaking a second country's laws only when a similar law exists in the extraditing country. Wikipedia, "Double criminality," https://en.wikipedia.org/wiki/Double_criminality.

[107] UNICEF, *Child Safety Online: Global Challenges and Strategies - Technical Report* (Florence, 2012), https://www.unicef-irc.org/publications/pdf/ict_techreport3_eng.pdf.

[108] ICMEC, *Child Pornography: Model Legislation & Global Review*, Eighth Edition (2016), http://www.icmec.org/wp-content/uploads/2016/02/Child-Pornography-Model-Law-8th-Ed-Final-linked.pdf.

[109] http://www.gdes.es.kr/board/view.do?boardId=BBS_0000001&menuCd=MCD_000000000000080173&dataSid=12331778 (in Korean).

younger ones on appropriate behaviour in cyberspace, can be useful in expanding an understanding of online risks among young Internet users.

The building blocks for fostering digital citizenship are already built into a number of legislation around child protection. In Japan, for instance, the policy that mandates harmful content filtering also pushes for education on appropriate Internet use for children. Meanwhile, Malaysia's National Child Protection Policy includes the provision of basic knowledge to children to enable them to protect themselves from harm. At the global level the ITU's Child Online Protection programme and the Internet Governance Forum's Dynamic Coalition for Child Online Safety both encourage the development of online protection tools and guidelines for young people.

Initiatives to protect children online, as the study demonstrates, are not always government-driven, with a significant number being led by the private sector or civil society organisations, but all tend to involve government support.

More broadly, all the economies covered by the study have carried out initiatives to promote digital citizenship among young Internet users, albeit with varying degrees of impact. Economies with high Internet penetration in the region tend to have programmes managed by a wider range of stakeholders, making them more sustainable, and specifically involve the education sector in promoting awareness on responsible behaviour online among students. With a few exceptions, initiatives in moderate and low penetration economies tend to be standalone campaigns. Yet this study also finds a growing number of resources—toolkits, modules, platforms and training materials—developed by different stakeholders in the Asia-Pacific region, many of them targeting specific age groups, and focusing on social media use. These can be used as a take off point or as references in developing more scalable programmes and tools to empower young Internet users.

Economies with High Internet Penetration	Economies with Moderate Internet Penetration	Economies with Low Internet Penetration
• Online sexual abuse and exploitation • Safe and secure Internet use • Cyberbullying • Cyberethics education • Digital citizenship • Addiction (game, Internet and smartphone) • Privacy	• Online sexual abuse and exploitation • Cyberethics education • Digital citizenship • Cyberbullying • Addiction (online games) • Online consent	• Online sexual abuse and exploitation • Digital citizenship • Cyberbullying

Table 5. List of emerging priority issues in the selected economies

Policy Recommendations

I. In domestic law, clearly define terms based on international legal standards and include offenses facilitated by all Internet-enabled platforms

Terms such as “child”, “child pornography” and “online grooming” should be clearly defined where relevant based on the OPSC and guidelines from ICMEC, ITU COP, UNICEF, #WePROTECT and other international bodies. It is also important to explicitly include offenses facilitated by all Internet-enabled platforms in national law.

II. Ensure that policies to protect children online are consistent with other important policy objectives, such as the preservation of fundamental rights

Measures that prevent and mitigate risks should not reduce the benefits of the Internet for children, and should be consistent with the UN Convention on the Rights of the Child, which were signed and ratified by all countries in Asia-Pacific. These fundamental values include the right of children to freedom of expression and privacy.

III. Collaborate, adopt a multi-stakeholder approach, and ensure international cooperation

Partnerships are essential for addressing child online safety issues. Relevant actors include (a) Government and law enforcement agencies; (b) Social services organisations; (c) ISPs and mobile service providers; (d) Teacher and parent associations; (e) Children and young people; (f) Child protection and welfare NGOs; (g) Academic and research institutions; (h) Owners of public access points, e.g. Internet cafés, telecentres, online gaming centres; (i) Private sector; and (j) International alliances and networks

IV. Make digital citizenship a priority in online child protection policies

Policymakers need to acknowledge children’s capacity to protect themselves, and to combat the risks that they encounter on the Internet. Legislation to minimise harm should be balanced with measures that make available knowledge and tools, and that develop habits and attitudes to build children’s resilience, while also enabling them to engage constructively online.

Digital literacy training should thus not only equip children with technical skills, but also seek to instil responsible behaviour. This includes exercising care in the content they create, the information they share with others, and their interaction with other children and with adults, especially strangers in cyberspace.

That children as young as 10 years old can become active consumers and producers of online content underlines the importance of empowering children to use the Internet safely and confidently at a younger age.

Efforts to promote digital citizenship should be undertaken alongside measures to encourage parents, guardians, caregivers and teachers to guide and assist young Internet users in safely navigating the open Internet. Parents and guardians should also be aware of what their children are doing online, and they should be able to discuss any issues or concerns in a manner which encourages care and understanding rather than being perceived as parental control.

V. Develop a coordinated strategy for awareness-raising and education on child online safety for different actors

Many countries have implemented activities to raise awareness on child online safety issues among children, parents, educators and even industry, but they are often ad hoc activities. A coordinated approach and strategy would enable stakeholders to pool resources and expertise for greater impact.

There are diverse groups of children of different ages, ethnicity, ability, socio-economic positions living in urban or rural settings. Public awareness and education materials on child online safety need to be tailored to suit the different groups of children.

Empowering older children to act as mentors and guides to younger users could be effective as a peer support mechanism. Children may find it easier to discuss some issues with those of a similar age (e.g. senior/older students) rather than adults. This could be implemented in schools along with digital literacy programmes.

VI. Strengthen the child protection and technological capacity of law enforcement agencies

Law enforcement agencies do not always view online sexual abuse and exploitation as a child protection issue. In many countries it is regarded as a "cybercrime" and officers may therefore have little or no expertise, or professional interest in child protection. It is therefore important for law enforcement agencies to be aware and sensitive to aspects of online child safety and have the will and capacity to work with other stakeholders. An understanding of the fast-changing Internet ecosystem is needed, as well as expertise in areas such as digital forensics.

VII. Engage with children to develop robust research on child online safety and integrate findings in child protection systems

Children are a vital stakeholder in addressing issues of online safety. Countries in the region are starting to gather data on children's online conduct and usage patterns, including their coping strategies and safety awareness, but many are one-off studies. Information from such initiatives need to be consolidated, promoted and updated through further research to bring online child protection issues to the attention of relevant stakeholders, and to better inform policymaking in the region. Effective interventions require developing a good understanding of children's behaviour on the Internet, and the online risks they face. Keeping current with evolving technology will enable stakeholders to develop and carry out more timely interventions.

VIII. Develop consistent indicators to assess and monitor child online safety

There is limited statistical data on children's use of the Internet and the risks that they face online. Findings from various studies are rarely comparable. International cooperation would benefit from consistent indicators to measure child online safety. Countries may refer to existing guidelines, such as the ITU's Child Online Protection Statistical Framework and Indicators.[110]

[110] ITU, *Child Online Protection Statistical Framework and Indicators* (Geneva, 2010), http://www.itu.int/dms_pub/itu-d/opb/ind/D-IND-COP.01-11-2010-PDF-E.pdf.