UNODC
United Nations Office on Drugs and Crime

Regional Office for
Southeast Asia and the Pacific

5 August 2021

UNODC Southeast Asia Pacific Written Submission to the Parliament of Australia Joint Committee on Law Enforcement

Introduction:

Organized crime groups have the ability to manipulate and exploit the people and governments of Southeast Asia (SEA). Worldwide, cybercrime is one of the fastest-growing types of crimes with reported losses totalling over US$3 trillion in 2015 alone, with a forecast of US$6 trillion for 2021 and over US$10.5 trillion by 2025. SEA is victim to roughly 33 per cent of the world's cybercrime. As of 2019, businesses that operate in the Asian region are victims of six cyber threats every minute.

Cybercriminals will certainly exploit vulnerabilities wherever they find them (hardware, software, technological configuration, methods of operation, etc.). Cybercrime is an evolving threat – the capabilities and technology employed by these criminals is advancing all the time. The result is that efforts to combat cyberattacks and other online crimes are becoming more complicated and costly, and often more difficult to achieve at a national level.

Each year, cybercriminals steal terabytes of intellectual property and financial assets, as well as facilitating and benefiting from a wide range of online crimes, including the exploitation of children. Cybercriminals also pose a very real threat to crucial networks like local power grids, global financial systems, health care systems and telecommunication networks. It is highly probable that many governments and organizations are being attacked by cybercriminals right at this moment and are not even aware of it. Every government, company, and person possesses information and/or assets that are valuable to cybercriminals.

The establishment of a safe, secure national and international cyberspace in SEA requires a cybersecurity workforce that is technically and tactically competent to meet not only today's challenges but also the emerging threats of tomorrow. Governments need to work more closely with private industry, with a particular focus on education and cyber-defence tools. In short, Southeast Asian countries must make efforts to transcend national differences in cyber policy and law enforcement to be more effective in tackling cybercrime in the region. Success lies in capacity building and cross-border cooperation and development with countries working together to create a truly international force leaving these transnational cybercriminals no place to hide.

UNODC
United Nations Office on Drugs and Crime

Regional Office for
Southeast Asia and the Pacific

The challenges facing the region's law enforcement agencies are numerous and varied, and one of the most prevalent is ransomware. As illustrated by the high-profile attacks on hospitals in Indonesia and Thailand, the threat of ransomware is on the rise in Southeast Asia, and is in no way isolated to only these two countries. The problems posed by ransomware are growing in many Southeast Asian countries and should therefore be one of the top priorities with law enforcement agencies in the region. Unfortunately, as the number of victims continues to increase, so too does the advancement in encryption and anonymity-protecting technology (including the application of cryptocurrencies to obscure transactions), all of which make it more difficult to catch the perpetrators. Increased training and a greater understanding of these emerging technologies is vital in the fight against ransomware attacks and other cybercrimes.

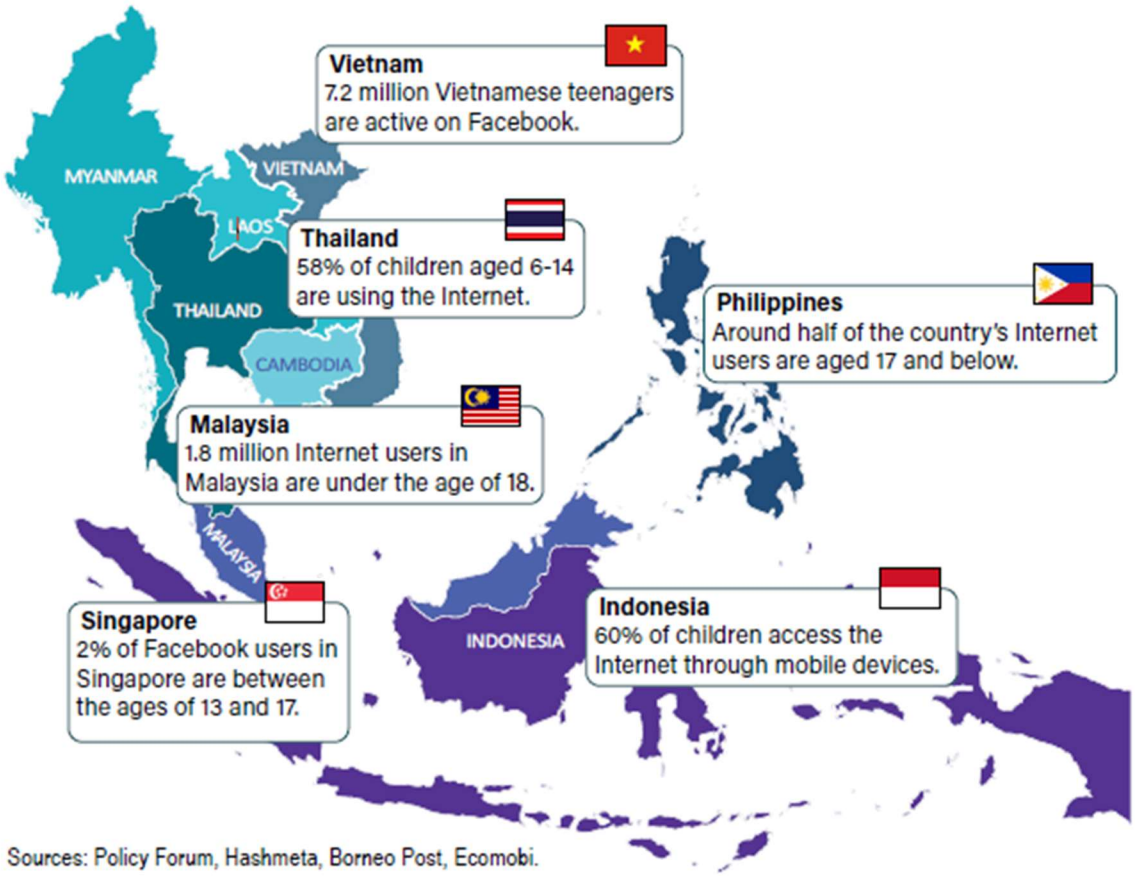
One of the region's most prevalent crimes is online child sexual abuse and exploitation (OCSAE). The fact that more and more child sexual exploitation material (CSEM) is appearing online is just one indicator that this most pernicious of crimes (that preys on the most innocent and vulnerable) is growing rapidly, and the trend looks likely to continue as more people access the Internet. Although much of this activity is conducted within the enhanced security afforded by the Darkweb, there is still a tremendous amount available on the Clearnet with criminals creating closed forums on social media platforms to add security for streaming actions and the dissemination of this material all around the world.

Online child sexual abuse and exploitation (OCSAE) involves the use of information and communication technology as a means to either sexually abuse or sexually exploit children, or both concurrently.

The proliferation of the Internet has transformed the distribution of child sexual abuse media into a crime without geographical boundaries. As the Internet and mobile broadband become more accessible and the use of smart technologies is expanding significantly in Southeast Asian countries – a trend that is expected to continue in the years to come – not only adults, but also children and adolescents, are becoming advanced Internet users, actively engaging in online gaming and social media. Estimations from Indonesia are that 60 per cent of the children have access to the Internet through mobile devices. Likewise, in the Philippines, roughly half of the 44 million Internet users are younger than 18 years old and, in Thailand, 58 percent of children between 6 and 14 years old are connected. Moreover, a recent study stated that, around the age of 10, Asian children start using the Internet not only for gaming but also for entertainment, communication, learning, and self-expression.

UNODC
United Nations Office on Drugs and Crime

Regional Office for
Southeast Asia and the Pacific

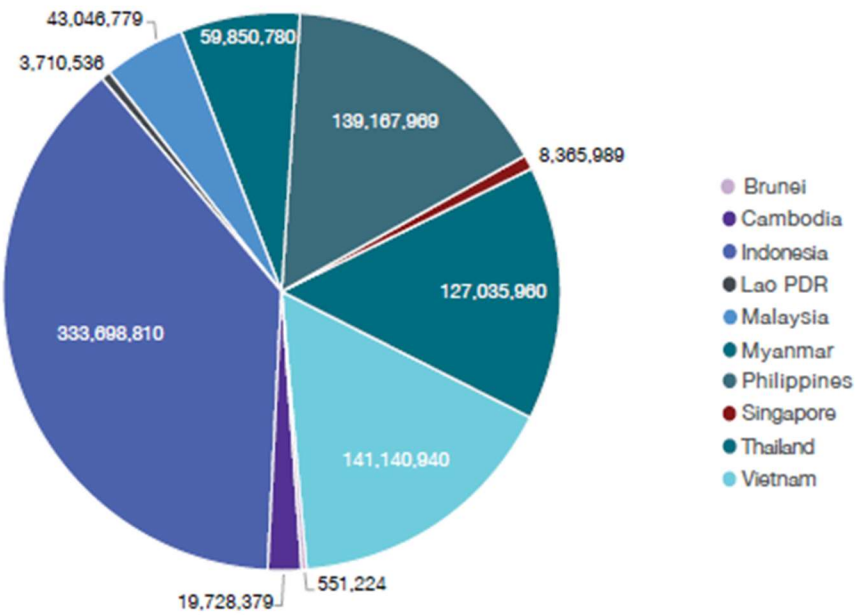


Sources: Policy Forum, Hashmeta, Borneo Post, Ecomobi.

One alarming trend illuminating the youth of victims is the substantial escalation in CSAM where the victims are infants or "pre-verbal" children. These children cannot self-report the abuse and are often abused by someone they know. The Internet Watch Foundation (IWF) reported that 94 percent of CSAM found online contains images of children aged 13 or under. IWF also found that 39 percent of the images were children aged 10 or under. Parents and law enforcement must find a way to give children the latitude to use online resources while protecting them from the dangerous traps emplaced by criminals hiding in the virtual world.

UNODC
United Nations Office on Drugs and Crime

Regional Office for
Southeast Asia and the Pacific



Increased fraud on mobile platforms

Cybercriminals are increasingly using mobile devices to ply their trade, as evidenced by a 680 percent increase in fraud transactions from mobile apps between 2015 and 2018.[i] The saturation of the mobile phone market does bring some benefits as well as complicating other issues which need to be addressed. This market is mostly Android, which is frequently the target of criminals and state sponsored attackers alike, traditionally through their software but recently involving their hardware as well.[ii] Criminals can exploit the numerous mobile applications to gain critical information about an individual, including, at a minimum, the potential victim's location and at the maximum, their whole pattern of life and personal information. This increased threat vector also brings potential benefits for law enforcement to track criminals and collect evidence. The only limitations for action are legal authority and support, as well as the technical acumen of law enforcement and cyber operators to monitor and access the criminals while collecting information.

Over 60% of online fraud is accomplished through mobile platforms. Additionally, 80% of mobile fraud is carried out through mobile apps instead of mobile web browsers.[iii]

UNODC
United Nations Office on Drugs and Crime
Regional Office for
Southeast Asia and the Pacific

Availability and Types of Online Child Sexual Exploitation

This section provides an overview of the different types of online child sexual abuse and exploitation present in the region and the statistics on OCSAE-related reports that have been made available by both law enforcement authorities and other partners.

Reporting accurate OCSAE statistics is challenging because law enforcement agencies are only able to investigate a fraction of the vast amount of offences that occur. Additionally, this type of offence does not yet have a definition that has been agreed upon by all Southeast Asian states, which increases the difficulty of obtaining figures on a regional scale.

Child sexual abuse material

Child sexual abuse material (CSAM) is defined 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."[iv]

In Chiang Mai in 2019, officers from the Thailand Internet Crimes against Children (TICAC) Unit arrested the administrator of a VK group distributing CSAM. VK (VKontakte) is a Russian social media platform with over 500 million accounts worldwide. The group was originally created in Russia and later purchased by Thais. More than 100 child sexual abuse (CSA) clips depicting sexual acts between Thai children and adult foreigners were posted in the group and perpetrators had to pay membership fees to view the uncensored versions. Upon apprehension, the suspect declared he had been running the group for a year.[v]

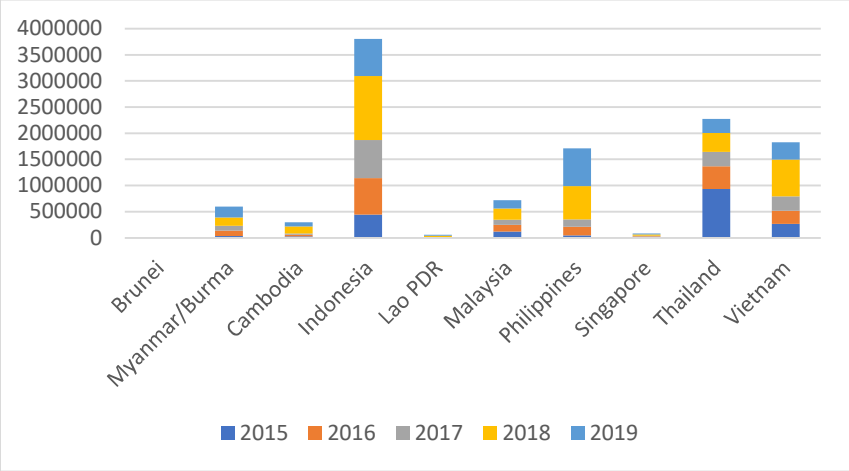
Thailand Internet Crimes against Children Task Force

The amount of CSAM uploaded and shared online in Southeast Asia has increased dramatically in recent years, as reported by both law enforcement agencies and industry partners. Out of the 10 ASEAN member

states participating in a UNODC research on the topic, only Cambodia, Indonesia, Thailand, the Philippines, and Malaysia were able to provide some statistics on CSAM-related reports, with the other countries having either very few records or none at all.

However, recent work by the IWF, ECPAT International, UNICEF, Terre des Hommes, and local child protection initiatives has demonstrated that the number of offences reported to law enforcement is likely to be only a fraction of the actual cyber-related dangers currently threatening Southeast Asian children and adolescents. For example, the International Centre for Missing and Exploited Children (ICMEC) reported that in Indonesia, over 18,000 children were sexually exploited via the Internet between 2011 and 2015.[vi] The sheer volume of reports submitted by US based electronic service providers to the National Centre for Missing and Exploited Children (NCMEC's) CyberTipline (TiP) from 2015 to 2019 (*Figure 15*) highlights over 11 million OCSEA reports including geographic indicators related to four Southeast Asian countries as the upload location of CSAM.[vii]

Figure 16: Breakdown of NCMEC's CyberTipLine reports sent to ASEAN law enforcement agencies for review between 2015 and 2019.[viii]



To illustrate this point, in Cambodia alone, the number of CSAM reports has been steadily increasing from 2013: the NCMEC[ix] together with APLE, and the Cambodia Child Helpline have processed over 200,000 OCSAE-related reports since 2015. However, 2018 saw a spike with over 120,000 CSAM reports – an increase of 490 per cent compared to the previous year – with 29 per cent of these reports containing new or previously unknown CSAM.[x] Likewise, the NCMEC conveyed over 1.2 million reports to the Philippine authorities between 2015 and 2019.

Table 4: A breakdown of NCMEC's CyberTipLine reports sent to ASEAN law enforcement agencies for review between 2015 and 2019.[xi]

Countries	2015	2016	2017	2018	2019	Total
Brunei	1,268	2,028	1,527	3,058	1,757	**9,638**
Myanmar	35,102	105,756	88,152	157,982	208,226	**595,218**
Cambodia	29,816	30,937	25,354	130,688	80,249	**297,044**
Indonesia	441,692	702,163	728,035	1,219,204	711,056	**3,802,150**
Lao PDR	6,076	5,876	5,773	23,103	17,936	**58,764**
Malaysia	117,982	130,960	96,760	217,512	156,046	**719,260**
Philippines	49,510	161,764	138,851	640,730	722,188	**1,713,043**
Singapore	12,049	15,004	14,920	25,379	15,980	**83,332**
Thailand	936,829	430,415	279,386	356,532	270,329	**2,273,491**
Vietnam	265,268	254,306	272,465	706,392	328,098	**1,826,529**
Total	**1,895,592**	**1,839,209**	**1,651,223**	**3,480,580**	**2,511,865**	**11,378,469**

As can be seen in *Figure 1* and *Table 1*, the year 2018 saw a spike with over 3.4 million reports originating in the region – an increase of about 120 percent compared to the previous year – and a drop to 2.5 million in 2019, although the latter figure might be influenced by the NCMEC's new reporting techniques. In addition to that, from April 2019 to April 2020, there was a further 106 per cent increase worldwide.[xii] This subsequent spike is mostly non-cyber and draws a correlation to the COVID-19 lockdown which means there is a relationship between people being locked down and child abuse.

Conversely, the reports from 2019 were mostly cyber and in SEA, they were traced back to Indonesia (33.4%), Thailand (20%), Vietnam (16.1%) and the Philippines (15.1%).

As seen above with the VK group, there is substantial organization in this industry and experience with the distribution and sale of material; however, efforts have been made at the national level (and some internationally) to address and disrupt this industry. Capacity building, training and education are essential in codifying a successful program in SEA.

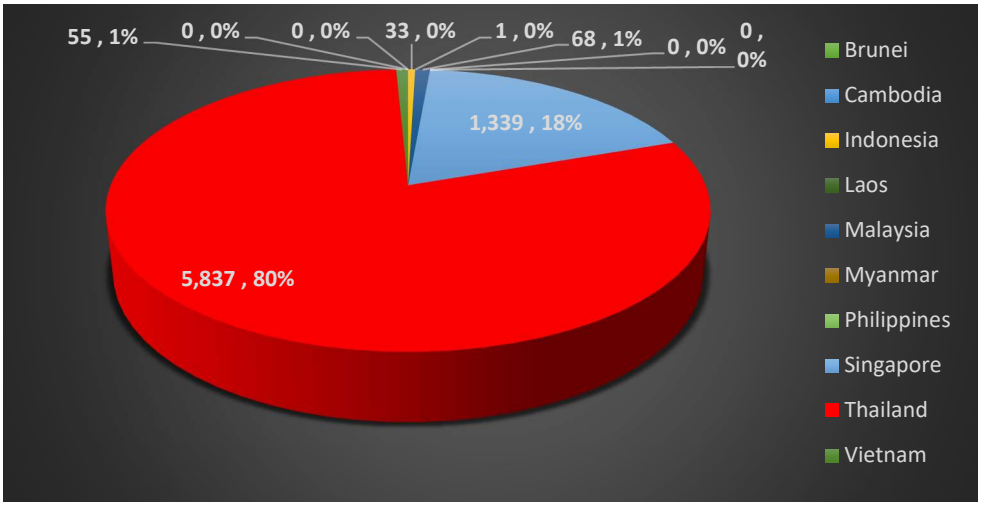
Online distribution of child sexual abuse material

The IWF reported that in Southeast Asia, the majority of child sexual abuse imagery was found on image hosting websites on the Clearnet (open Internet), with Thailand and Singapore as the main hosting countries in the Southeast Asian region (see *Figure 16* and *Table 5*)

UNODC
United Nations Office on Drugs and Crime

Regional Office for
Southeast Asia and the Pacific

Figure 17: Number of reports between 2014 and 2019 where action was taken by the IWF regarding CSAM in SEA.* [xiii]



* *Note: Each report can contain multiple images/videos.*

To avoid detection, online child sex offenders tend to use multilingual, specialised vocabulary and include spelling variations together with other linguistic noise in their filenames to avoid (automatic) detection of their shared files, while making them widely searchable for other offenders. Additionally, alterations to media files, such as cropping, scaling, colour adaptations, format transcoding or embedding them into other regular images or videos, are used to hide child sexual exploitation and abuse (CSEA) content.

UNODC
United Nations Office on Drugs and Crime
Regional Office for
Southeast Asia and the Pacific

Table 5: Number of reports between 2014 and 2019 where action was taken by the IWF regarding CSAM in SEA.*.[xiv]

Hosting country	2014	2015	2016	2017	2018	01/01/2019 - 16/08/2019	Total IWF reports
Brunei	0	0	0	0	0	0	**0**
Cambodia	0	0	0	0	0	0	**0**
Indonesia	0	19	4	3	7	0	**33**
Laos	0	0	0	0	0	1	**1**
Malaysia	0	0	5	7	12	44	**68**
Myanmar	0	0	0	0	0	0	**0**
Philippines	0	0	0	0	0	0	**0**
Singapore	23	13	211	428	50	614	**1,339**
Thailand	129	365	345	643	3,112	1,243	**5,837**
Vietnam	2	14	29	7	0	3	**55**
Totals	**154**	**411**	**594**	**1,088**	**3,181**	**1,905**	**7,333**

* *Note: Each report can contain multiple images/videos.*

Of the CSAM found in Southeast Asia, 20.1 per cent involved images of child abuse depicting penetrative sexual activity and/or sexual activity with an animal or sadism; 26.8 per cent contained images involving non-penetrative sexual activity, and 53.1 per cent showed other indecent images of children not falling within the previous categories. Furthermore, 96.6 per cent depicted girls as the subject matter and 96.9 per cent of the victims were 0-13 years old, with 6.6 per cent being younger than seven.[xv]

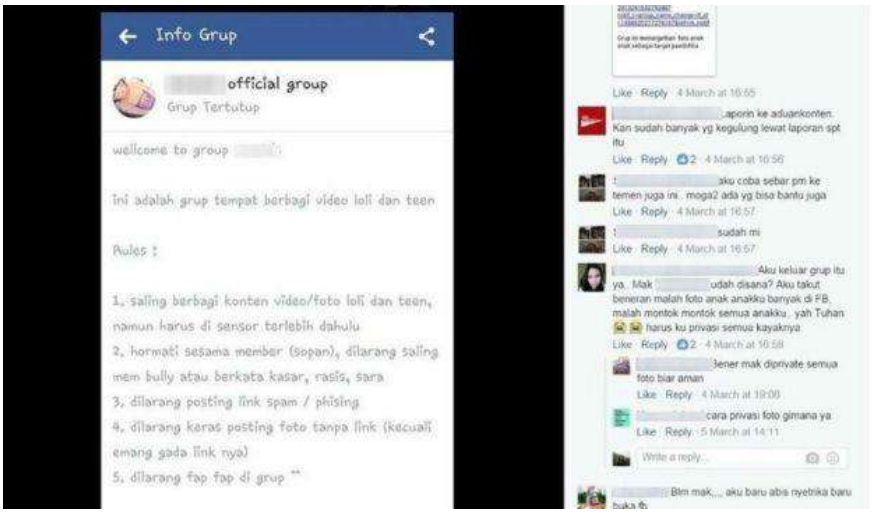
As mentioned, most online CSAM in SEA is found on image hosting websites on the Clearnet. Dissemination happens on various online platforms; however, peer-to-peer (P2P) sharing is one of the most frequently attested means, both globally and in Southeast Asia.

Furthermore, sharing CSAM on social media platforms has increased due to the self-destruct function and encryption some of these applications offer. Additionally, false user profiles are easily created, taken down, and recreated, enabling the set-up of hidden social media offender groups distributing such illicit media.

In 2017, a group of Indonesian mothers sharing images of their children in an online parenting community accidentally discovered a Facebook group with over 7,000 members sharing at least 100 pictures and 400 videos depicting child sexual abuse and talking about how to approach and seduce children while avoiding detection from supervising adults. Police arrested five suspects. One of the suspects was reported to have joined 11 WhatsApp groups linked to 11 different countries.[xvi]

UNODC
United Nations Office on Drugs and Crime

Regional Office for
Southeast Asia and the Pacific



Paedophile Facebook Group discovered by Indonesian mother

Online solicitation or "grooming"

In the context of child sexual abuse and exploitation, *grooming* refers to a process by which an offender prepares a child, significant others, and the environment for the abuse of this child. Specific goals include gaining access to the child, gaining the child's compliance, and maintaining the child's secrecy to avoid disclosure. This process strengthens the offender's abusive pattern, as it may be used as a means of justifying or denying his or her actions.[xvii] *Online grooming* refers to the process of establishing a sexual relationship with a child either through the use of the Internet or other digital technologies to facilitate either online or offline sexual contact with the victim. For the offender, this type of grooming can save money, time, and risk of detection by law enforcement compared to the more "traditional" approach of searching for children in brothels, bars, massage parlours or other venues.

The general modus operandi for grooming is similar for most perpetrators in that they tend to use social media platforms on the Clearnet because these provide easy access to potential victims. Some of them create false online (child) identities to gain their victims' trust.[xviii] However, the actual grooming tactics may differ according to the type of offender in question. Research has shown that some child sex offenders believe that their contact with the victim(s) is like a relationship.[xix] In contrast, others mainly act upon their own sexual needs and regard the victim(s) as mature and capable participants. A third type tends to dehumanise their victims completely, considering them nothing more than objects. These perpetrators usually have an extensive collection of images and videos displaying CSAM and they often communicate with other online predators.[xx, xxi]

Additionally, research[xxii] has found that skilled groomers adjust their grooming methods to fit the targeted child. These grooming methods range from (or include combinations of) attention, compliments, affection, kindness, recognition, gifts (digital or even alcohol, drugs or money) to *sextortion*, i.e.,

threatening to disseminate existing images of the victim to lower their inhibitions and gain their "consent". The process can also involve offenders sharing CSAM with children, which, in turn, is considered as a form of sexual exploitation.[xxiii]

Online grooming is also reported as a technique used by traffickers operating in SEA. In some cases they will even pay for internet access to their potential victims. Such criminals attempt to arrange offline meetings, often taking their victims shopping in a big city, and later trafficking them across borders.

The United Nations Convention on the Rights of the Child (CRC) is the international treaty that legally obligates nations to protect children's rights.[xxiv] Articles 34 and 35 require states to protect children from all forms of sexual exploitation and abuse.[xxv] Additionally, these articles outlaw the coercion of a child to perform sexual activity, engage in prostitution and prohibits exploitation of children in creating pornography.[xxvi] Despite this, only 4 out of the 10 Southeast Asian nations (Brunei Darussalam, Singapore, Malaysia and the Philippines) have an anti-grooming law in place. The Sexual Offences Against Children Act (SOAC) came into effect in Malaysia making child sexual grooming a criminal offence on July 10, 2017,[xxvii] highlighting how new these anti-grooming laws are in the region. In Cambodia, Lao PDR, Thailand, and Vietnam there is still no legislation criminalising online grooming.[xxviii] Lack of national legislation empowers criminals to use jurisdiction to their advantage. Their presence on the internet may be in a location with no laws that protect children, meaning they cannot be extradited to a country with these laws. Conversely, police in countries with these laws can use them to their advantage. For example, a cybercriminal may be grooming a child in a country with no laws that protect children but may have an internet connection that goes through a country that does have such laws on their books. In this case, law enforcement officials would be able to arrest the criminal if international extradition agreements existed between the countries.

On-line groomer who used Facebook[xxix]

UNODC
United Nations Office on Drugs and Crime
Regional Office for
Southeast Asia and the Pacific

In 2016, Vietnam's Cyber Security and High-tech Crime Prevention Department together with the CID and FBI investigated a group of cybercriminals who ran an online forum focusing on CSAM involving boys aged under 13, in which members were able to upload and share their material. At the time of arrest, the Vietnamese forum had 1,328 videos and 690 photo albums available. Membership could only be established through an invitation from an existing member and perpetrators not only had to pay a membership fee, but also had to upload at least one video or image to maintain their membership. One of the members apprehended by the police had groomed and threatened (online) over 200 boys from eight different countries into producing videos while pretending to be a 10 to 12-year-old girl.[xxx]

Moreover, a recent study[xxxi] found that most adults in SEA do not consider grooming as child sexual abuse. Parents often lack awareness regarding OCSAE and the risks of online grooming, leaving children without proper guidance or supervision in a fast-developing virtual world. Many young people in SEA, especially girls, experience online grooming and usually do not have the skills or knowledge required to address the problem, e.g., by reporting, blocking or using the privacy settings on the social media platforms they use.

As a result, there is an increase in the number of cases documented each year involving Internet perpetrators soliciting children via social media and chat rooms in SEA. A research team from Terre Des Hommes that posed as a 10-year-old girl from the Philippines in online chat rooms (i.e., "the Sweetie project")[xxxii] reported that over 50,000 potential child sex offenders had crossed their path in only ten weeks in 2013. When comparing the few statistics available to the results of the Terre Des Hommes team, it is most likely that the figures shown are a significant underestimate of the situation. Data from Brunei law enforcement included 55 CSEA cases between 2015 and 2017, in which 11 victims met their abuser online.[xxxiii] Data from Malaysia showed that, between January and May 2017, 117 cases were reported in which a child was sexually assaulted by an offender they met through the Internet.[xxxiv] These examples highlight the need for more in-depth research into the scale of this type of OCSAE in the region.

UNODC
United Nations Office on Drugs and Crime

Regional Office for
Southeast Asia and the Pacific

UNICEF Cambodia providing resources for children[xxxv]

A 2013 survey by UNICEF in Cambodia reported that almost 1 in 10 females in the group aged between 13 and 17 had already been upset by someone speaking or writing sexual things to them. Just under half of the males aged 13 to 17 reported being forced by someone to watch explicit photos or videos against their will.[xxxvi] A more recent survey by APLE among 117 children in Cambodia found that 1 in 4 children had experienced grooming or sexual advances by adults online. High-risk platforms cited by children and teachers for being exposed to harmful content, such as adult pornography, CSAM and grooming, were Facebook, Instagram, Messenger, Line, Skype, gaming platforms (e.g., Rules of Survival), TikTok, and Bigo Live.

Production of self-generated explicit material

User-generated content is content that is self-created and self-published online by Internet users. Typical forms of user-generated content include blogs, videos, podcasts, comments on articles, forum commentaries, social media postings, and contributions to wiki sites.[xxxvii] In the context of child sex abuse and exploitation, user- or self-generated explicit material (SGEM) entails images and videos that not only feature children but are also (coercively) produced by children. It is a relatively new phenomenon that has grown significantly on a global scale in recent years[xxxviii] and the trend is likely to continue due to children's increasing access to smart devices and their lack of awareness of the risks of producing and sharing SGEM.[xxxix]

> "When I started using Facebook, one person added me as a friend, he said he is from Dee Maw So. So, I thought he is a good guy since we are from the same ethnicity. He said later he is actually from another place, he threatened to use my pics on Facebook for other use. I was so scared and begged him." – *Girl, Kayan Christian, Loikaw, Myanmar.*[xl]

Once children or adolescents start to manage their Internet usage, self-generated material is often shared with peers. However, law enforcement agencies have reported that *sexting*[xli] is becoming more popular among youth. In many of these cases, the self-generated material is sexually explicit in nature and shared without the sender's consent. It can then end up in an online child sex offender's collection and subsequently be used to convince or coerce the child or adolescent into producing new CSAM. In cases where coercive techniques are used, an emerging trend can be identified towards more extreme, violent, sadistic, or degrading demands by perpetrators.[xlii]

A commonly reported outcome of producing SGEM is *sextortion*, in which the victim is blackmailed with their SGEM to extort sexual favours, money or other benefits under the threat of the material being shared online (e.g., on social media, with the victim's family, etc.). Cases involving sextortion are increasing rapidly and it is fast becoming one of the most significant worldwide online threats towards children and adolescents. Child victims of sextortion are typically between 10-17 years old, but victims as young as 9 have been reported. Moreover, sextortion cases are increasingly being documented in which the perpetrator manipulates or coerces their victims into abusing younger family members or friends.[xliii, xliv]

Operation Strikeback[xlv]

"In 2014, INTERPOL launched an operation specifically targeting organised online sextortion rings in the Philippines. The operation included coordinated information sharing between the Interpol Digital Crime Centre, the Philippines National Police and law enforcement agencies in Hong Kong and Singapore. The two-day raid led to the arrest of 58 individuals, the seizure of over 250 pieces of electronic equipment, and the identification of over 190 individuals associated with organised crime in the Philippines. Three of the men arrested had harassed and sextorted a Scottish teenager, who later committed suicide." [xlvi, xlvii]

INTERPOL and Philippine National Police

Offenders are typically male adults or young people, who may or may not know their victims. However, online sextortion is also committed by organised cybercriminal networks that operate out of locations similar to call centres.[xlviii] Offenders utilise a range of online environments to gain access to potential child victims, such as social networking sites, messaging and photo apps, video calling apps, dating apps, and gaming platforms. Their tactics can include online grooming or hacking their victims' social media profiles. Additionally, across Asia, Remote Access Trojan (RAT) software tools are widely used by hackers who disseminate them via popular video games, with victims documented in, for example, Malaysia and Singapore.[xlix] The increased use of camera-enabled smart devices has also led to a rise in (distant) live-streaming child sexual abuse and exploitation online (see below). Video calls enable "sextorters" to engage in virtual face-to-face interaction, which strengthens their influence and control over their victims.[l]

Being coerced into producing sexually explicit material is considered highly traumatising for the victims. They tend to withdraw from family members and friends in self-blame, which in some cases even leads to suicide – 28 per cent of US FBI cases in 2015 had at least one victim who committed or attempted suicide.[li] Hence, it is essential to educate children and adolescents on the risks of user-generated content and sextortion, as well as making best practices in care accessible for victims and their families.

Live-streaming and the production of other-generated explicit material

Studies dating back to the 1990's identified the negative impact of tourism on child protection, leading to a series of campaigns against child prostitution in Asian tourism and the establishment of a global network to end child prostitution, child sexual abuse and the trafficking of children for sexual purposes (e.g., ECPAT). However, as the Internet expanded to more parts of the world, foreign child sex offenders no longer needed to travel to gain access to Southeast Asian children. They can now easily contact local traffickers, select children, view and even direct long-distance video calls in real-time from any location while maintaining their anonymity. Such live-streaming of child sexual abuse is described as an increasing challenge in OCSAE by both regional and international law enforcement agencies.

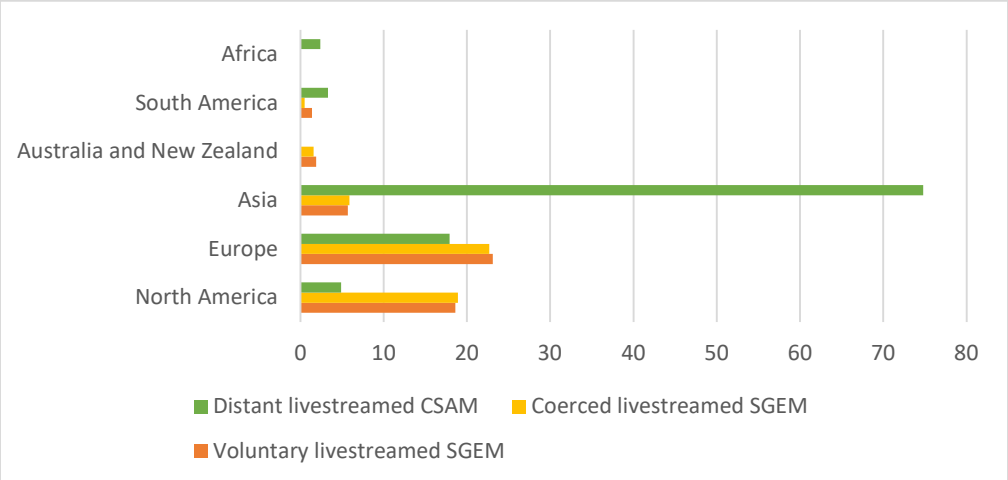
The volume of live-streamed CSAM available online at any given time is unknown and is constantly changing. Due to this limitation, reports are based primarily on law enforcement experts' experiences and

findings made available by industry partners and NGOs. For this study, the following types are distinguished:

- Live-streaming of voluntary SGEM, which features children or adolescents engaging voluntarily in live-streaming of nudity or sexual behaviour and is typically initially shared with a peer.
- Live-streaming of SGEM that is the result of grooming or sextortion, in which case the victims are coerced into live-streaming while they are undressed or performing sexual acts.
- Distant live-streamed child sexual abuse, which entails webcam "shows" often pre-ordered by child sex offenders, in which an adult is either physically involved in the abuse or is coercing the victim into performing sexual acts.

UNICEF reported in 2016 that the Philippines has become the "global epicentre of the live-stream sexual abuse trade" resulting in tens of thousands of Filipino children being victimised via chatrooms and other social media offering online child sex performances. This abuse is not only due to the population's high level of Internet penetration and entrenched poverty, but also widespread knowledge of the English language. These results are confirmed by a recent survey among 450 law enforcement specialists from 41 different countries and multinational organizations such as INTERPOL and Europol. As shown in *Figure 17*, when asked to specify the origin of victims of live-streamed child sexual abuse based on the three types described above, more than 40 per cent of the respondents mentioned Asia and, more particularly, the Philippines (20%) as primary source countries for distant live-streamed CSA. Other Southeast Asian countries that were mentioned were Thailand, Cambodia, Vietnam, and Malaysia.[lii]

Figure 18: Percentages per region of CSA live-streaming according to the NetClean 2019 survey.[liii]



Offenders of distant live-streamed child abuse were found to be primarily located in Europe (25%) and the United States (22%). However, as can be seen in *Table 6*, Asian countries/regions (16%), such as the

Philippines, India, Pakistan, China, Thailand, Malaysia, Indonesia, and the Middle East, were also cited by police officers.

Table 6: Locations of offenders consuming CSA live-streaming according to the NetClean 2019 survey.[liv]

Country/Region	Voluntary livestreamed SGEM	Coerced live streamed SGEM	Distant live streamed CSAM
North America	41.0	38.7	22.4
Europe	32.4	34.2	24.8
Russia	5.3	4.5	5.6
Asia	7.0	6.8	16.1
Australia & New Zealand	2.9	2.3	5.6
South America	1.6	1.8	1.9
Africa	-	0.5	-
unknown	3.6	5.3	19.9

Contact with local perpetrators is often established through adult pornographic websites and, subsequently, communications are moved to encrypted online messaging environments.[lv] In addition to offenders paying to view real-time distant child sexual abuse, offenders travel to Southeast Asian countries to engage in hands-on abuse and remain in contact with adults after their return, paying them to continue the abuse via live-streaming services.

An increasing amount of child sexual abuse in SEA is being live-streamed from people's homes and is mostly operated by the victims' families rather than by organised crime syndicates online. Child victims are reported to "work" throughout the day, having to cater to offenders located in different time-zones. As the abuse is carried out by their family or parents, children are often oblivious to the exploitation and they experience the abuse as normal or accept it so they can better provide for themselves and their family. Hence, they are often unwilling to incriminate their relatives in court. With such "shows" costing between US$5 and US$200, the United Nations has estimated that the child abuse industry in the Philippines is already worth over US$1 billion.

UNODC
United Nations Office on Drugs and Crime

Regional Office for
Southeast Asia and the Pacific

UNICEF interview of rescued child (identity hidden) forced to perform sex shows at the age of 7.

In 2011, police in the Philippines arrested a Filipino mother who was organising a live webcam feed of her two daughters aged 7 and 11 and her 13-year-old niece. Similar cases have also been reported in subsequent years – 57 in 2013, 89 in 2014 and 167 in 2015. In some cases, children and adolescents even suggest the practice themselves in an attempt to provide a better life for their families.[lvi]

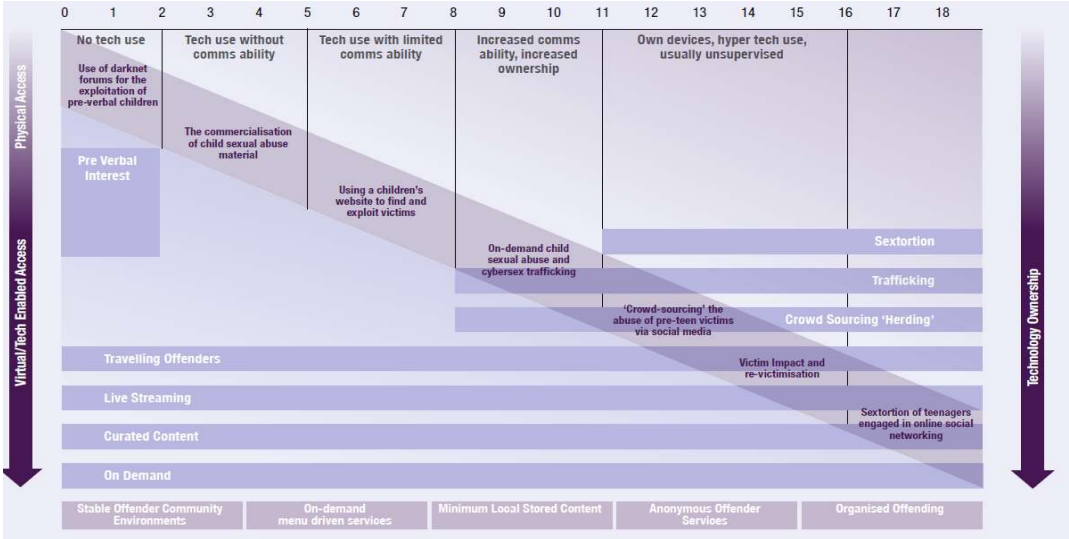
The role of the Darkweb

The Darkweb and other encrypted software techniques have become increasingly popular among Internet child sex offenders because it enables its users to disseminate child sexual abuse material anonymously. For example, Tor can be used to hide a user's location and identity. Cryptocurrencies allow criminals to easily pay for services and create obstacles for police to decipher which hinders them from using this data for prosecution of crimes. Although recent analyses[lvii] of the Darkweb indicated that only 2 per cent of hidden web services on Tor hosted CSAM, these 2 per cent accounted for 80 per cent of the Darkweb traffic. A complete accounting of Darknet activities is covered in the UNODC report named *Darknet Cybercrime Threats to Southeast Asia*.

Other concerns

Sexualised cartoons, video games and deepfake images represent areas where the ability to enforce law is difficult in part because the victim of the crime is also the consumer of the criminal content. Although there is some precedent for conducting criminal prosecution, and legislation has been enacted to make some of this activity criminal, this is not yet widespread practice.[lviii] Given the growth of these technologies and their viral nature, these areas should be key focus areas for research especially as the advancement of deepfake technology will increase the ability of criminals to adversely influence, manipulate and exploit vulnerable children.

Figure 19: The intersection between victim, child sex offender and technology at different stages of childhood.[lix]



[i] "2019 Current State of Cybercrime - RSA.com." RSA, Dell Technologies, www.rsa.com/content/dam/en/white-paper/2018-current-state-of-cybercrime.pdf.

[ii] Goodin, D. (2020, August 10). Over a Billion Android Devices Are at Risk of Data Theft. Retrieved from https://www.wired.com/story/over-a-billion-android-devices-are-at-risk-of-data-theft/

[iii] "2018 Current State of Cybercrime - RSA.com." RSA, Dell Technologies, www.rsa.com/content/dam/en/white-paper/2018-current-state-of-cybercrime.pdf.

[iv] Optional Protocol to the Convention on the Rights of the Child on the sale of children, child prostitution and child pornography, 2000.

[v] Pattaya One News (2019). *Operator of child porn site arrested in Chiang Mai*. https://pattayaone.news/operator-of-child-porn-site-arrested-in-chiang-mai/

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

[vii] It is important to note that country-specific numbers may be impacted by the use of proxies and anonymizers.

[viii] https://www.missingkids.org/
[ix] Reporting from NCMEC comes largely from US-based Service Providers that are legally required to report any child sexual abuse content on their platforms or servers.

[x] APLE (2020). *"They had pictures of me"*. National Study on the Nature & Extend of Online Child Sexual Exploitation in Cambodia.

[xi] https://www.missingkids.org/
[xii] https://www.forbes.com/sites/thomasbrewster/2020/04/24/child-exploitation-complaints-rise-106-to-hit-2-million-in-just-one-month-is-covid-19-to-blame/?sh=1ed7c5ef4c9c
[xiii] Source: IWF (2014 – 2019).
[xiv] Source: IWF (2014 – 2019).
[xv] Source: IWF (2014 – 2019).

[xvi] BBC News (2017). *The mothers who infiltrated an online paedophile group*. https://www.bbc.com/news/world-asia-39300320

[xvii] Craven, S., Brown, S., and Gilchrist, E. *Sexual grooming of children: Review of literature and theoretical considerations.* Journal of Sexual Aggression 12, 3 (2006), 287–299.

[xviii] UNODC. *Study on the effects of new information technologies on the abuse and exploitation of children*, 2015.

[xix] Gottschalk, P. A. *Dark side of computing and information sciences: characteristics of online groomers*. Journal of Emerging Trends in Computing and Information Sciences 2, 9 (2011), 447–455.
[xx] Gottschalk, P. A. *Dark side of computing and information sciences: characteristics of online groomers*. Journal of Emerging Trends in Computing and Information Sciences 2, 9 (2011), 447–455.

[xxi] Webster, S., Davidson, J., Bifulco, A., Gottschalk, P., Caretti, V., Pham, T., Grove-Hills, J., Turley, C., Tomp-kins, C., Ciulla, S., et al. *European online grooming project (final report)*. European Commission Safer Internet Plus Programme, Tech. Rep., 2012.

[xxii] Lanning, K. *Child molesters: A behavioral analysis for professionals investigating the sexual exploitation of children.* National Center for Missing & Exploited Children with the Office of Juvenile Justice and Delinquency Prevention, 2010.

[xxiii] ECPAT International. *Regional overview: sexual exploitation of children in Southeast Asia*, 2017.

[xxiv] https://www.ohchr.org/EN/pages/home.aspx
[xxv] https://www.ohchr.org/EN/pages/home.aspx
[xxvi] https://www.ohchr.org/EN/pages/home.aspx

[xxvii] Chu, M., Zainal, F., Tang, A., Zolkepli, F., & Aqilah, I. (2018, November 8). Predator roaming in plain sight. Retrieved May 26, 2020, from https://www.thestar.com.my/news/nation/2018/11/08/predator-roaming-in-plain-sight-man-exposed-online-targeted-underage-girls-in-ngos-churches-and-scho; The Star Newspaper

[xxviii] Online grooming of children for sexual purposes: Model legislation & global review (1st ed., Rep.). (2017). International Centre for Missing and Exploited Children

[xxix] Fun, P. (2018, November 7). M'sian who preyed on young girls in churches & NGOs for past 15 years exposed as pedophile. Retrieved May 28, 2020, from https://worldofbuzz.com/msian-who-preyed-on-young-girls-in-churches-ngos-for-past-15-years-exposed-as-pedophile/

[xxx] Le Trung, K., & Thi, T. N. T. (2019). Child Sexual Exploitation Investigation in Vietnam and Recommendations. *American Scientific Research Journal for Engineering, Technology, and Sciences (ASRJETS)*, *51*(1), 66-77.

[xxxi] Vorng, S. *Sex, Abuse and Childhood. A study about knowledge, attitudes and practices relating to child sexual abuse, including in travel and tourism, in Cambodia, Lao PDR, Thailand and Vietnam.* World Vision International, 2014.

[xxxii] Terre des Hommes (2013). *Sweetie 2.0: stop webcam child sex*. https://www.terredeshommes.nl/en/programmes/sweetie-20-stop-webcam-child-sex

[xxxiii] Nur Judy binti Abdullah (2018). *The overview on Access to Justice of Girl-Children who are Victims of Sexual Violence in Brunei Darussalam*. Presentation held at the national dialogue on 'Access to Justice of Girl-Children who are Victims of Sexual Violence in Brunei Darussalam', Bandar Seri Begawan. https://www.reddit.com/r/Brunei/comments/9ut8dt/32_of_reported_rape_cases_in_brunei_last_year/

[xxxiv] UN Human Rights Council (2019). *Visit to Malaysia - Report of the Special Rapporteur on the sale and sexual exploitation of children, including child prostitution, child pornography and other child sexual abuse*. 13. A/HRC/40/51/Add/3.

[xxxv] UNICEF Cambodia. (2020, August 03). Retrieved from https://www.unicef.org/cambodia/

[xxxvi] UNICEF (2013), "Findings from Cambodia's Violence Against Children Survey 2013", https://www.unicef.org/cambodia/UNICEF_VAC_Full_Report_English.pdf

[xxxvii] UNODC (2015). *Study on the effects of new information technologies on the abuse and exploitation of children*.

[xxxviii] VGT (2019). *Virtual Global Taskforce Online Child Sexual Exploitation: Environmental Scan*.

[xxxix] Europol (2019). *IOCTA*.

[xl] Ridout, B., McKay, M., Amon, K., Campbell, A. (2019). *Mobile Myanmar: the impact of social media on young people in conflict-affected regions of Myanmar.*

[xli] *Sexting* can be defined as sending, receiving or forwarding sexually explicit messages, pictures or videos. In most cases, mobile phones are used, but sexting can include any smart device.

[xlii] CEOP/NCA (2013), *Threat Assessment of Sexual Exploitation and Abuse*.

[xliii] ICMEC (2018). *Studies in Child Protection: Sexual Extortion and Nonconsensual Pornography*.

[xliv] VGT (2019). *Virtual Global Taskforce Online Child Sexual Exploitation: Environmental Scan*.

[xlv] https://www.news.com.au/world/breaking-news/cyber-extortion-ring-busted-in-philippines/news-story/4bcde9c3b7eb5d96cd495fb9a7a2e8ed
[xlvi] ICMEC (2018). *Studies in Child Protection: Sexual Extortion and Nonconsensual Pornography.*

[xlvii] Aljazeera America (2014). *Philippines bust global online 'sextortion' ring*. http://america.aljazeera.com/articles/2014/5/2/global-online-sextortionringbustmanila.html

[xlviii] ICMEC (2018). *Studies in Child Protection: Sexual Extortion and Nonconsensual Pornography.*

[xlix] Asia Digital Alliance (2016). *RAT Infestation: Your Family Privacy at Risk*. http://www.asiadigitalalliance.com/wpcontent/uploads/2016/05/ADA-_RAT-infestation-Your-family-privacy-at-risk_.pdf

[l] ICMEC (2018). *Studies in Child Protection: Sexual Extortion and Nonconsensual Pornography.*

[li] ICMEC (2018). *Studies in Child Protection: Sexual Extortion and Nonconsensual Pornography.*

[lii] NetClean (2019). *NetClean Report 2019. A report about child sexual abuse crime*.

[liii] NetClean (2019). NetClean Report 2019. A report about child sexual abuse crime.
[liv] NetClean (2019). NetClean Report 2019. A report about child sexual abuse crime.
[lv] Europol (2019). *IOCTA*.

[lvi] The Guardian (2016). *How child sexual abuse became a family business in the Philippines.* https://www.theguardian.com/world/2016/may/31/live-streaming-child-sex-abuse-family-business-philippines

[lvii] G. Owen (2015). *TOR: Hidden Services and Deanonymisation*, presentation. https://www.youtube.com/watch?v=-oTEoLB-ses

[lviii] "House wants to ban pornographic cartoon". House of Representatives of the Philippines. Retrieved 2009-04-16.

[lix] Global Threat Assessment 2018 (Publication). (2018). London: WeProtect Global Alliance. https://static1.squarespace.com/static/5630f48de4b00a75476ecf0a/t/5e4ed6110f2fa76663e58a83/1582224937659/Global Threat Assessment 2018 - English