[COLUMNIST] The rising danger of cyber-paedophilia in Malaysia

THE ICT Use and Access by Households Survey Report 2021 released by the **Department of Statistics (Dosm)** has reported that Internet usage in Malaysia last year increased by up to 95.5% compared to 91.7% in 2020.

However, as Internet access has become more widely available, this has made room for paedophiles to sexually abuse children through virtual means such as grooming and accessing child pornography.

As reported by PDRM's Sexual, Women and Children Crime Investigation Division (D11) Principal Assistant Director ACP Siti Kamsiah Hassan, data shared by Interpol, FBI, and National Centre for Missing and Exploited Children showed that from 2017, there were only 46 IP addresses identified.

By the year after, i.e., 2018, however, the number has spiked to 2,660 IP addresses and it kept increasing dramatically afterwards – escalating to 48,752 IP addresses in 2021.

In total, there were 93,368 IP addresses detected engaging in cyber-paedophilia activities from 2017 until the first quarter of 2022 (see "Police receive thousands of IP addresses suspected of sharing child pornography", New Straits Times, May 15, 2022).

Nevertheless, it is not surprising that the number of IP addresses accessing child sexual contents online could continue to rise.

This by itself should incite us to think as to how we could do more to suppress cyber-paedophilia that represents a real and present and continuing danger to children not only outside but in Malaysia also. The discovery of two notoriously well-known paedophiles – one based in the country and the other via cyberspace, namely Richard Huckle and Blake Johnston, respectively – finally led to the introduction of the Sexual Offences Against Children Act (Soca) in 2017.

However, even after the Act was passed, it was discovered in 2018 that Malaysia had the largest concentration of IP addresses used to upload and download child pornographic content in Southeast Asia (see "Malaysia tops in South-east Asia for online child pornography", The Straits Times, January 30, 2018).

<u>Why does the number of Malaysian IPs addresses continue to be high?</u>

Firstly, the current legislative provisions in Malaysia pertaining to online child sexual exploitation have some limitations.

The Soca (2017) is a comprehensive legislation that seeks to safeguard children from both online and offline sexual abuse compared to the older Child Act (2001) that does not criminalise child pornography.

In spite of that, Ecpat International (a global network of civil society organisations that works to end the sexual exploitation of children) has scored Malaysia 0/100 in the Out of the Shadows indicator for Internet protection for children.

This is because ISPs (Internet service providers) in Malaysia were not obligated to block, delete or report inappropriate information concerning child sexual abuse.

Moreover, directives by the Malaysian Communications and Multimedia Commission (MCMC) can only go so far – since the any blocking of access is limited to the Domain Name System (DNS) or IP address which can be easily circumvented.

Secondly, the Royal Malaysian Police (PDRM) is under-staffed and not well-equipped to effectively combat and deter child pornography online.

ACP Siti Kamsiah Hassan stated that the reason why the number of arrests is very low is due to manpower shortage and not enough trained staff in digital forensic training, including to filter and track the IP addresses, despite having the technical apparatus to do so.

In reality, PDRM relies heavily on information and data shared by international counterparts and partners.

In early 2022, only 103 out of 14,385 IP addresses were tracked leading to the arrests of 50 individuals. These IP addresses come under the purview and review of the PDRM's Malaysian Internet Crime Against Children (MICAC) D11 investigation unit which at the moment only comprises of three investigating officers (IOs) who are all ranked inspector.

Additionally, despite having the technical apparatus, PDRM has said that the Data Protection Act (2010) has made it more difficult for them to have full access to the activities from the IP addresses. For example, whilst PDRM can track the IP addresses, at present they are unable to determine whether any sharing or exchanges of images and videos have taken place.

According to PDRM, this is because private activities carried out within the (public) Internet domain are protected under the 2010 Act – which hampers the effectiveness of the ICACCOPS, i.e., the technical apparatus or software deployed to detect the IP addresses (see "Monitoring Internet Child Pornography (ICP) in Malaysia", Pertanika Journal of Social Sciences and Humanities, May 17, 2021).

ICACCOPS stands for Internet Crime Against Children: Child Online Protective Services.

Thirdly, the social stigma built around the topic of sex has led to under-reporting.

The taboo and shame surrounding sexual abuse topics/issues contribute to the lack of awareness among some minors which in turn increases their susceptibility/vulnerability to sexual exploitation. There is also the sub-culture whereby the perverted fascination with child and pre-pubescent sexuality is considered as a trivial and minor issue.

<u>Ensuring a pro-active role for the ISPs</u>

As it is, Southeast Asia is notorious for being a sex tourism hotspot for paedophiles.

This includes the sexual, physical and mental abuse of children as subjects for pornographic content. However, the Philippines is the only country in the region that has mandated ISPs to report, block, and report child porn.

Rightfully, therefore, Malaysia which is among the countries with the highest rate of Internet penetration in the region must take the critical step to ensure a safer Internet environment.

Furthermore, due to the technical capacity of the ISPs, they are well-poised and better positioned than the law enforcement authorities to serve as the frontline investigators and co-regulatory agents when it comes to the identification and blocking of child pornography sites which are typically hosted on the dark web.

This is why we need to ensure that the ISPs play a more active role in monitoring, penetrating, accessing and regulating the dark web on behalf of law enforcement authorities.

However, even ISPs are said to be currently lacking in sufficient technical capacity (in their own right) to penetrate the dark web.

Perhaps, the PDRM should engage the consultancy and technical services of private dark web intelligence firms as well as contract an expert/specialist to be "seconded" to Malaysia for a period. The contractor would also be responsible for capacity-building and training and development (T&D) of the MICAC personnel.

And if the 2010 Act presents one obstacle to the PDRM's efforts in investigating and suppressing cyber-paedophilia, then it is vital for the legislation to be amended with specific reference to Section 40 (1) – wherein the reference has been made – which prohibits the accessing and processing of "any sensitive personal data". Sensitive personal data "includes information on physical health or any other information the relevant Minister deems to be personal, including an individual's private communications data".

A clause should be inserted which provides for an additional exception or derogation, i.e., with respect to the right and authority of law enforcement agencies to access and investigate personal data for child pornography purposes.
Hence, if need be, we need to further empower our law enforcement authorities with the necessary legal backstop.

<u>Enhancing regional cooperation with technology and reinforced policing</u>

The challenge in combating the evil is compounded by the difficulty in tracking down the practice of illegal/illicit transactions that are made in cryptocurrency for child pornography contents.

Child pornography also includes live-streaming of children being abused via webcams. This activity has been on the rise in the Southeast Asian region.

One way to break down and smash child pornography activities is by the cryptocurrency trail which leads right back to the users.

In 2017, a company known as Chainalysis became the world's first tech firm to focus solely on tracing cryptocurrency transactions.

The firm has been collaborating with government agencies, and its successes include busting of one of the biggest websites for child pornography (see "Inside the Bitcoin Bust That Took Down the Web's Biggest Child Abuse Site", Wired, April 7, 2022).

We can build on these successes in the fight against cyber-paedophilia through strengthened regional and international cooperation by not only exchanging information but also actively working together to suppress the dramatically increasing numbers of IP addresses suspected of accessing child porn with advanced technologies.

Again, procuring the technical expertise of foreign-based firms such as Chainalysis for use in the Southeast Asia region is one example, especially in the context of Aseanapol – as the embodiment of regional and cross-border cooperation on policing.

Aseanapol should establish a regional cybercrime centre with the specific purpose also of combatting the evil of child pornography.

The shortage of manpower and technical capacity could be partly alleviated by pooling and sharing of resources (including financial).

In addition to technical and technological sophistication to "outwit" the cyber-paedophiles, law enforcement authorities also need to step up the utilisation of other methods at their disposal including entrapment and dragnet and intelligence operations, including especially impersonation techniques and various guises as a user.

As part of the reinforced policing of cyber-paedophilia and, by inclusion, the wider paedophilic activities, there is also a critical need to penetrate the domestic paedophile community also – by informants – to become more familiar with the tactics and methods employed to evade detection.

The rising danger of cyber-paedophilia – which represents a menacing threat to society in general too – has made it all the more imperative and critical for PDRM and the government to intensify efforts and measures to achieve greater success in the suppression of this evil.

https://www.astroawani.com/berita-malaysia/columnist-rising-danger-cyberpaedophilia-malaysia-377313