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)** reports 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, room has been made for paedophiles to sexually abuse children through virtual means such as grooming and accessing child pornography.

As reported by the police's Sexual, Women and Children Crime Investigation Division (D11) principal assistant director Siti Kamsiah Hassan, data shared by Interpol, the FBI, and the National Centre for Missing and Exploited Children shows that from 2017, there were only 46 IP addresses identified.

By the year after, ie, 2018, however, the number had spiked to 2,660 IP addresses. This continued to increase dramatically, 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.

But it is not surprising that the number of IP addresses accessing child sexual content online could continue to rise.

This alone should encourage us to think about how we could do more to suppress cyber-paedophilia, which represents a present and continuing danger to children not only outside the country but in Malaysia also.

The discovery of two notorious paedophiles, Richard Huckle and Blake Johnston, 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.

<u>Why is the number of Malaysian IPs addresses still high?</u>

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

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 are not obligated to block, delete or report inappropriate information concerning child sexual abuse.

Moreover, directives by the Malaysian Communications and Multimedia Commission can only go so far since any blocking of access is limited to the domain name system or IP address which can be easily circumvented.

Secondly, the police force is under-staffed and not well equipped to effectively combat and deter child pornography online.

Siti Kamsiah said the reason why the number of arrests is very low is due to a shortage of manpower and staff trained in digital forensics, including to filter and track IP addresses, despite the police force having the technical apparatus to do so.

In reality, the police rely heavily on information and data shared by its 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 police's Malaysian Internet Crime Against Children (MICAC) D11 investigation unit which at the moment only comprises three investigating officers (IOs) who are all ranked as inspectors.

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

According to the police, 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, ie the technical apparatus or software deployed to detect the IP addresses.

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 a lack of awareness among some minors which in turn increases their susceptibility/vulnerability to sexual exploitation.

There is also a sub-culture whereby the perverted fascination with child and pre-pubescent sexuality is considered a trivial and minor issue.

<u>Ensuring a proactive role for 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 and block child porn.

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 lacking in sufficient technical capacity (in their own right) to penetrate the dark web.

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

And if the 2010 Act presents one obstacle to the police's efforts to investigate and suppress cyber-paedophilia, it is vital for the legislation to be amended with specific reference to Section 40 (1) – wherein the reference is 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, ie with respect to the right and authority of law enforcement agencies to access and investigate personal data for child pornography purposes.

If need be, we should 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 this evil is compounded by the difficulty in tracking down the practice of illegal/illicit transactions that are made in cryptocurrency for child pornography content.

Child pornography also includes the 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 child pornography activities is through 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.

We can build on these successes in the fight against cyber-paedophilia through strengthened regional and international cooperation, not only by exchanging information but also by 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 of combating the evil of child pornography.

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

In addition to technical and technological sophistication to "outwit" 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.

As part of the reinforced policing of cyber-paedophilia and, by inclusion, the wider field of paedophilic activities, there is also a critical need to penetrate the domestic paedophile community 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 as well, has made it all the more imperative for the police and the government to intensify efforts and measures to achieve greater success in the suppression of this evil.

https://www.malaysianow.com/opinion/2022/08/22/the-rising-danger-of-cyber-paedophilia-in-malaysia