CYBERCRIME AND COVID19 in Southeast Asia: an evolving picture

KEY JUDGMENTS

1. **There is no uniform method of gathering data, nor reporting of, cybercrime and, in particular, online child sexual abuse and exploitation in Southeast Asia.** Consequently, building an accurate picture of threat remains challenging.

2. **Cybercriminals in Southeast Asia seek to profit from the accelerated digitisation of society.** It is essential that public awareness of cybercrime countermeasures continues to grow.

3. **Online child sexual exploitation, compounded by the covid-19 pandemic, continues to rise.** Victim-centric responses should be prioritised.

4. **The COVID-19 pandemic, and subsequent responses, created a wealth of opportunities for cybercriminals.** Government, the private sector, civil society, and the public must work together to counter these evolving threats.

Context

1. This briefing provides a Southeast Asia-focussed update to our snapshot cybercrime analysis of April 2020. It intends to bolster ongoing collaboration and suggests new avenues for addressing cyber threats, taking the UN Crime Congress Kyoto Declaration into account. This briefing should be read in conjunction with our 2020 "UNODC Darknet Cybercrime Threats to Southeast Asia" report.

Regional Picture-of-Threat

2. In most instances in Southeast Asia, governments apply different data metrics and standards, thus making it difficult to accurately measure the relative scale of cybercrime activity and the effectiveness of enforcement and prevention measures. Specifically, on the issue of online child sexual exploitation, policy and investigative gaps create opportunities for criminals and obstacles for law enforcement.

3. With increased connectivity, mobile device penetration, COVID lockdown and online schooling, more children have been online, more often, than ever before. This, coupled with the increased use of social media and online gaming platforms[1], combined with a lack of risk awareness, has resulted in a significant increase in potential victims for online child sexual exploitation.[2] Live streaming of child sexual abuse also continues to grow[3], enabled by encryption technologies (including the darknet), and the proliferation of anonymous payment methods, including cryptocurrencies.

4. Cybercrimes, including the spread of malware, ransomware[4], DDoS attacks, data breaches and phishing, continues to rise in Southeast Asia[5]. Financial data fraud, credit card fraud and romance scams also continue to grow as cybercriminals ultimately seek to make profit. With the increased digitisation of society, we also see an increase in the targeting of critical national infrastructure[6]. These trends are driven by the increasing number of available targets and the perception of cybercrime as highly profitable with a relatively low risk of detection.

5. Websites that have a coronavirus-related name are more likely to be malicious[7], with those that claim to track viral spread on maps often exploiting browser permissions to covertly install malware. The production and dissemination of contact tracing applications has also presented opportunities for cybercriminals[8]. By adapting network intrusion tools, criminals may be able to access, steal, exploit and profit from the personal information of individuals, businesses and government whilst also undermining trust in these institutions.

Analysis and Recommendations:

A. **ENHANCE COORDINATOIN AND INTERNATIONAL COOPERATION BETWEEN AND WITHIN STATES**
There is an urgent need, recognised in the UN Crime Congress Kyoto Declaration, to enhance coordination and international cooperation to effectively prevent and combat the growing threat of cybercrime[9]. The lack of uniformity of data collection methodology in Southeast Asia hinders a unified response, obfuscating the true scale of the phenomenon.

B. COUNTERING ONLINE CHILD SEXUAL EXPLOITATION AND HIGH IMPACT CYBERCRIME SHOULD BE PRIORITISED
With an accurate picture-of-threat and reporting mechanisms, the true scale of the phenomenon can be gauged, thus enabling authorities to triage and direct resources towards the crimes that cause the most serious harms. These crimes pose the greatest threats to children, livelihoods, wellbeing, and societal development. Government officials, the private sector, civil society, and the general population must be routinely sensitized to the cybercrime threats that impact the region. With a better understanding of the threat, everyone can respond more effectively to the challenges we face.

[1] https://www.interpol.int/en/content/download/15611/file/COVID19%20-%20Child%20Sexual%20Exploitation%20and%20Abuse%20threats%20and%20trends.pdf
[2] https://www.iwf.org.uk/report/iwf-2020-annual-report-face-facts
[3] https://www.state.gov/reports/2020-trafficking-in-persons-report/philippines/
[4] https://www.trendmicro.com/vinfo/us/security/research-and-analysis/threat-reports/roundup/a-constant-state-of-flux-trend-micro-2020-annual-cybersecurity-report
[5] https://www.interpol.int/en/content/download/16106/file/ASEAN%20Cyberthreat%20Assessment%202021%20-%20final.pdf
[6] http://techandlifestylejournal.com/cybersecurity-trends-southeast-asia-2021/
[7] https://blog.checkpoint.com/2020/03/05/update-coronavirus-themed-domains-50-more-likely-to-be-malicious-than-other-domains/
[8] https://www.securityweek.com/covid-19-contact-tracing-apps-effective-virus-risk-management-tools-or-privacy-nightmare
[9] A/CONF.234/L.6 - E - A/CONF.234/L.6 -Desktop (undocs.org) at para 93

C. INCREASE CAPACITY-BUILDING EFFORTS TO COUNTER CYBERCRIME

Well-trained and equipped counter-cybercrime and cybersecurity professionals are an essential resource in the fight against cybercrime. Regular training, mentoring and equipment upgrades will improve capacity across government and industry in this constantly evolving digital space. This will further ensure the integration of capacity-building into pre-established mechanisms such as the ASEAN SOMTC, its Working Group on Cybercrime, the ASEAN Declaration to Combat Cybercrime and the Plan of Action to Implement the Joint Declaration between ASEAN and the United Nations (2021-2025).[10]

D. STRENGTHEN COOPERATION MECHANISMS AND PUBLIC-PRIVATE PARTNERSHIPS BETWEEN SEA COUNTRIES

Southeast Asian States, taking the UN Crime Congress Kyoto Declaration[11] *into account, should promote, at the national, regional and international levels, with due respect for domestic legal frameworks and the principles of international law, public-private partnerships with the digital industry, the financial sector and communication service providers in order to enhance international cooperation to combat cybercrime*[12]*. Increasing and improving mechanisms for effective cooperation, trust and coordination can create a powerful collaborative environment, delivering an effective, robust, and lawful response to the cybersecurity threats of the future by fostering open dialogue, consensus, and the participation of all relevant stakeholders.*

ENDS

[10] https://asean.org/storage/2020/10/ASEAN-UN-POA-2021-2025-final.pdf
[11] https://www.unodc.org/unodc/en/crimecongress/documents.html
[12] A/CONF.234/L.6 - E - A/CONF.234/L.6 -Desktop (undocs.org) at para 96