Octopus Project

to support implementation of the Budapest Convention on Cybercrime and its Protocols

Report version 29 June 2022

COVID-19 related cybercrime in Asia: Regional Study

With examples from
India, Indonesia, Japan, Laos, Malaysia,
Philippines, Singapore, Sri Lanka, Vietnam

Prepared within the framework of the Octopus Project

COUNCIL OF EUROPE

CONSEIL DE L'EUROPE

www.coe.int/cybercrime

Contents

Contact
Cybercrime Programme Office of the Council of Europe (C-PROC)
Tel +33-3-9021-4506
Email alexander.seger@coe.int

1 Introduction

1.1 Background and purpose

The COVID-19 pandemic from early 2020 onwards demonstrated how the reliance of individuals and societies is exploited for criminal purposes. During this crisis, the need to rely more than ever on computer systems, mobile devices and the Internet to work, communicate, shop, share and receive information and otherwise mitigate the impact of social distancing, was accompanied by phishing campaigns and malware distribution, ransomware attacks, attacks against critical infrastructure, offenders targeting public and private sector organisations through the devices of teleworking employees, fraud schemes or disinformation. At the same time, COVID-related restrictions adversely affected the ability to criminal justice authorities to investigate prosecute such offences.

The COVID-19 pandemic and the related crimes have affected all regions of the world. This is also true for Asia. It was agreed, therefore, that the Council of Europe – through the Octopus Project – would support a series of activities, including the preparation of the present report, in order to strengthen the criminal justice response to COVID-19 related cybercrime in Asia.

The present study is an attempt to assess and understand this response using the examples of nine Asian countries, that is, India, Indonesia, Japan, Laos, Malaysia, Philippines, Singapore, Sri Lanka and Vietnam.

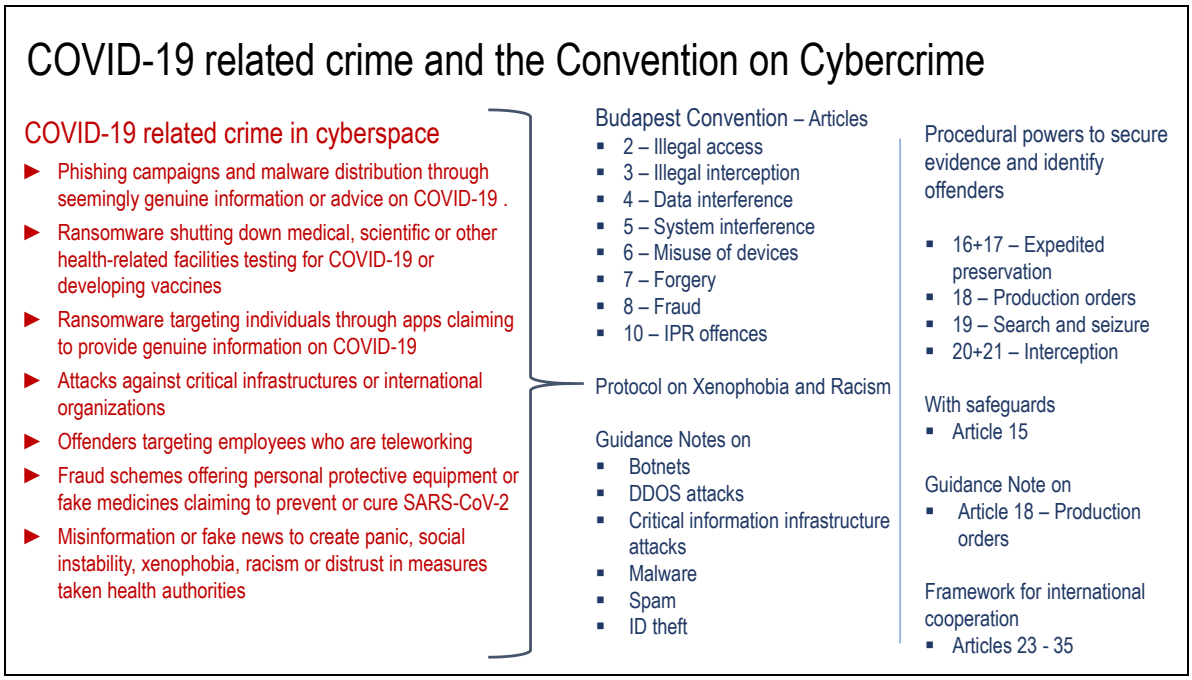
This study is based on information obtained from different resources and several studies listed in the bibliography, on country Wiki Profile as published in the Octopus Cybercrime Community (Council of Europe website) but also on information provided by representatives of these countries either through answers to a questionnaire or during the three virtual workshops dedicated to this activity in October, November and December 2021, followed by a physical regional workshop held on March 7-9 in Colombo, Sri Lanka.

1.2 COVID-19 related cybercrime and the Convention on Cybercrime

Following the onset of the COVID-19 pandemic, the Council of Europe – like other organisations prepared a number of tools and recommendations addressing different aspects, ranging from questions related to data protection or artificial intelligence, to falsified medical productions or the constitutionality of emergency powers. Similarly, specific resources were made available to facilitate the criminal justice response to COVID-19 related cybercrime.[1]

Within this context, the mechanism of the Convention on Cybercrime ("Budapest Convention ") is considered to provide a framework also for a rule of law-based criminal justice response to COVID-19-related cybercrime through its provisions on criminalising conduct, its procedural powers to investigate and secure electronic evidence and its tools for international cooperation:

[1] Links to these resources are available at https://www.coe.int/en/web/cybercrime/cybercrime-and-covid-19



The Convention on Cybercrime is backed up by capacity building projects to assist States in the implementation of its provisions.[2] A number of countries in Asia have benefitted from such support in recent years.

Between September 2017 and May 2021 – that is also under COVID-19 conditions – the Parties to the Convention on Cybercrime negotiated a new 2nd Additional Protocol on enhanced cooperation and disclosure of electronic evidence.[3] This Protocol provides for expedited forms of cooperation, including direct cooperation with service providers in other Parties for the disclosure of subscriber information. It also includes two articles on cooperation in emergency situations.

This Protocol was opened for signature in May 2022. Once ratified by sufficient number of States, it will offer additional solutions in future pandemics or other global crises that require expedited access to electronic evidence across borders.

[2] https://www.coe.int/en/web/cybercrime/capacity-building-programmes

[3] https://www.coe.int/en/web/conventions/full-list?module=treaty-detail&treatynum=224

2 Regional overview of the criminality landscape during COVID-19

The COVID-19 pandemic, while accelerating digital transformation with increased connectivity and changes in the way people work, shop, socialize, and learn, also amplified vulnerabilities and exposures of individuals and society to cybercrimes.

The number of businesses that moved their activities online, the increased number of individuals working remotely from home coupled with longer time spent by people in cyberspace offered more avenues and opportunities to the criminals for exploitation by using the COVID-19 narrative with high likelihood to click on a malicious link.[4]

Although many of these threats existed even before the pandemic, some became more common or pronounced in the last two years as cyber threats continue to evolve. New business models of cybercrime have emerged such as Phishing-as-a-service (PhaaS), Malware-as-a-Service (MaaS), Ransomware-as-a-Service (RaaS). These forms of Crimes-as-a-Service (CaaS) lower the threshold for criminals to enter cyberspace and commit cybercrime since the tools and services are readily, widely, and cheaply available and usable without much technical knowledge.

Regardless of old and new threats or crimes, illicit financial gain and fraud continue to be the main motivation for cybercriminals even during the COVID-19. What follows is an overview of the developments on cybercrime in the region with mini case studies, trends, and figures in select countries.

2.1 COVID-19 and cybercrime in Asia

This section summarises some of the important recent threats and the trends[5] of cybercrime in Asia. With countries in the region amongst the fastest-growing digital economies in the world, they have become primary targets for cyberattacks.

Asia covers a huge expanse of territory that spans a diverse range of people, political systems, social ethnographies, besides various cultural and economic levels of maturity, size, growth, and digital readiness. In fact, all governments, organizations, and individuals experience similar disruptions with the rise of cyber threats and cybercrimes. The pandemic had both positive and negative impact on crime numbers. Indeed, due to the lockdown measures that include checkpoints, quarantine, and isolation, besides the increased awareness and practice of social distancing, certain crimes declined. The study explores some of the emerging trends and more common cybercrimes during the pandemic.

Online scams and phishing

Phishing attacks in the region show no signs of slowing down or decreasing. From January to June 2020, Kaspersky alone blocked more than 1.6 million attempts to transfer users to phishing pages via malicious links. Kaspersky foiled the most phishing attempts in the region against small and medium businesses

[4]In April 2020, Zoom announced that it had surpassed 300 million meeting participants daily. Apart from work, individuals in ASEAN also spent more leisure time online during the pandemic. The Global Web Index's special coronavirus study revealed that the Philippines had seen the greatest number of people reporting an increase in the amount of time spent on social media platforms. Around 64% of the Filipinos who participated in the survey reported an increase in their "social time", compared with the global average of 47%.

[5] Interpol ASEAN Desk on ASEAN Cyber Threat Assessment for 2021. Available at: https://www.interpol.int/content/download/16106/file/ASEAN%20Cyberthreat%20Assessment%202021%20-%20final.pdf

in Indonesia, Malaysia, and Vietnam. Singapore experienced the lowest toll of phishing emails but still witnessed an increase of 60.5% compared with the same period in 2019.[6]

Kaspersky's data show that Indonesia accounted for 749,915 incidents, Vietnam 737,152, Thailand 478,795, Malaysia 442,439, Philippines 200,312, and Singapore 145,004.

Cybercriminals are deploying COVID-19 themed phishing emails and social media messages, often impersonating government, health authorities, and even charities, to trick victims into clicking on malicious links or opening suspicious attachments to reveal their credentials.

An example is a series of fake and fraudulent emails pretending to have originated from the World Health Organization (WHO) with malicious attachments. Another variant is to send emails or phone messages from scammers pretending to be charitable organizations.[7]

According to Trend Micro's endpoint detections, the Association of Southeast Asian Nations (ASEAN) accounted for 3.7% of global malicious URL in relation to the COVID-19 pandemic equivalent to 80,000 phishing attacks during the first nine months of 2020. Singapore was among the top seven countries globally with such incidents.

Fraud

Online and telecom fraud also increased. This form includes fraudulent websites, e-commerce platforms, social media accounts, and emails claiming to sell and deliver medical products.

To illustrate, scammers fraudulently solicited donations from individuals, groups, and areas affected by COVID-19 taking advantage of their vulnerabilities. Calls impersonating hospital officials requesting payments to help relatives and donations, calls were from health authorities, utility or telco companies asking about personal information and account details became more prevalent.

A particular form of fraud, Business Email Compromise (BEC), was committed frequently. Cybercriminals would, for example, build a narrative that puts pressure on accounting or finance employees by sending messages allegedly from their superiors directing them to immediately transfer funds to another bank account. This has resulted in huge monetary losses for businesses.

Misinformation or "fake news"

Another trend is the rise of fake media account and trolls with the negative effects on communities and social stability, the manipulation of opinions, and disinformation and distrust in governments and health measures. These also facilitated the execution of cyberattacks. Some reports of misinformation were linked to the illegal trade of fraudulent medical commodities while others pertained to conspiracy theories around origin, propagation, prevention, treatment, preparedness, and prevalence of COVID-19. Similar trends accompanied vaccine development, their use and effectiveness, and potential side-effects.

---

[6] ASEAN Cyber Threat Assessment 2021. Available at: https://www.interpol.int/content/download/16106/file/ASEAN%20Cyberthreat%20Assessment%202021%20-%20final.pdf

[7] Webinar on the evolution of cyber-threats during the covid-19 pandemic by CEPOL, October 2020. Available at: https://www.cepol.europa.eu/education-training/what-we-teach/webinars/covid-19-webinar-no4-evolution-cyber-threats-during-covid

Malicious or fraudulent websites

Fraudulent websites grew in number and exploited the recent surge in demand for surgical masks, personal protective equipment; coronavirus test kits, and medical ventilators to sell fake, non-existent or defective supplies. The tactics copied legitimate sites to receive payments without any deliveries. When transacted overseas, the money trail becomes very difficult to trace and the identities almost impossible to attribute leading to financial loss.

Cybercriminals increasingly resorted to register seemingly genuine domain names containing coronavirus related keywords such as "coronavirus", "COVID", "Corona", or "COVID-19". Such fraudulent websites were often used for malicious purposes even as they masqueraded with unsubstantiated claims to provide updated information or advice on COVID-19.

Compared to February 2020, number of new domain names registered with a nexus to COVID-19 grew up by 569% to 116,357, with 2,022 identified as malicious and 40,261 classified as high-risk.[8]

Ransomware and malware

Incidents of ransomware attacks targeting the health sector like hospitals, research centers, laboratories, and other health-related facilities increased exponentially being overwhelmed by the health crisis and highly susceptible to pay up the ransom rather than risking to be locked out of their systems.

The RaaS market attracted a lot of potential cybercriminals into hacking as a means of making money quickly. In 2020, RaaS operators succeeded in compromising more than 800 victim organizations with most targeted industries being the government, education, healthcare, critical manufacturing, information technology, and financial services.

Some ransomware attacks targeted mobile phones of individuals using apps like contact tracing applications, applications that claim to provide genuine updated information on COVID-19 and in the process steal money or data, or both.

Kaspersky noted that there were about 2.7 million ransomware detections in ASEAN during the first three quarters of 2020. Indonesia had the most with 1.3 million counts accounting for almost half of the total.

A study conducted by the Identity Theft Resource Center (ITRC) found that the average ransomware payouts for all businesses grew from less than USD 10,000 in the third quarter of 2018 to more than USD 178,000 per event by the end of the second quarter of 2020[9].

According to Group-IB's estimates, the total financial damage from ransomware operations amounted to over USD 1 billion, admittedly highly underestimated since only 2.5% of ransomware incidents were made public. No wonder, ransomware continues to accrue substantial profit for cybercriminals.

Meanwhile, INTERPOL's ASEAN Desk coordinated a cyber-operation against a strain of malware targeting e-commerce websites. It identified hundreds of compromised websites in affected countries, reported the threats to member countries' attention and offered support with national investigations. In particular, the intelligence detected Command-and-Control (C2) servers and located infected websites in six countries in the ASEAN region. Cybercriminals were deploying data harvesting malware such as Remote Access Trojans (RAT) including banking trojans, key loggers, information stealers, and spyware.

[8] https://unit42.paloaltonetworks.com/how-cybercriminals-prey-on-the-covid-19-pandemic/

[9]Identity Theft Resource Center. Available at: https://www.idtheftcenter.org/2021-predictions-government-support-for-identity-crime-victims-is-out-and-stealing-passwords-is-in/

Cryptojacking

Threat actors were taking advantage of the wider user of Internet of Things (IOT) devices and the greater acceptability of electronic money and the rise of cryptocurrency offerings and relatively lower prices to launch cryptojacking campaigns. They exploited several vulnerabilities with evolved tactics and advanced mining malware to achieve maximum gains. One example is the coin miner malware that runs on victims' computers without their knowledge. Cybercriminals consider the attack as a less disruptive way of making money compared with other types of cyber threats.

Distributed Denial of Service (DDoS) attacks

DDoS attacks remained a big concern during the pandemic but became increasingly more targeted, automated, and adaptive. Targets were mainly large organizations with online presence even as efforts to take down botnets infrastructure were underway.

The duration of these attacks became shorter with enhanced bandwidths and growing amounts of information. Service providers are severely challenged to maintain the quality of service with increased traffic and bandwidth constraints. This resulted in success rate of DDoS attacks in 2020 by 17%.[10]

Child sexual exploitation online

There was a significant increase in the amount and demand of online child sexual abuse material. The commercial aspects were increased with offenders often using encryption and other anonymous communication networks (like TOR) to hide their identities and activities making it very difficult for law enforcement to investigate and uncover these crimes.

There was consequently significant increase in the reported cases of online child sexual exploitation. The National Center for Missing and Exploited Children (NCMEC) had received 4.2 million reports in April 2020, up 2 million from March 2020 and nearly up 3 million from April 2019.

2.2 COVID-19 and organised crime

There is as yet no comprehensive study on the role of organised crime taking advantage of the pandemic. However, the nature of some forms of cyberattacks point to their perpetration as an orchestrated and organized criminal activity by one or more groups.

The pandemic constitutes an opportunity for organized criminal groups around the world to expand their territories and markets. Cybercriminals are fine-tuning their attacks by relying on social media platforms like Facebook, WhatsApp, Instagram, and Snapchat to collect more information about their victims and to access their targets.

Many were targeting legitimate businesses that were struggling. In what follows, we highlight some of the major organized crimes in the last two years.

Recruitment of online money mules

The pandemic caused an increase in unemployment which was exploited by criminals to recruit online money mules, i.e., those that help knowingly or unknowingly to commit crimes.

[10] The impact of COVID-19 on Financial Crimes Webinar – GLACY+ Project and Interpol webinar, May 2020. https://www.coe.int/en/web/cybercrime/glacyplusactivities/-/asset_publisher/DD9qKA5QlKhC/content/joint-c-proc-interpol-webinar-impact-of-covid-19-on-financial-crimes?inheritRedirect=false

"Sextortion"

There was a significant increase in the number of "sextortion" cases amongst adolescents during the time of stay at home during but also beyond the lockdowns and other restrictions.

Trafficking in human beings

Illegal migration continued to be a hook for human traffickers to victimize desperate people. These crimes rely on complex logistics and are extremely difficult to prevent, detect or investigate.

Falsified Products

Organized crime groups took advantage of the high market demand in the health sector like medical devices, pharmaceutical products, personal protection, hygiene products, sanitary masks, breathing devices and medicines and engaged in their fake or substandard goods or non-existent deliveries.

In March 2020, there was an increase in fake or counterfeited medical items available on the market including: disposable surgical masks (Fake N95 masks, hand sanitizers, antiviral and antimalarial medication, vaccines, and COVID-19 test kits).

An international operation coordinated by INTERPOL led to the seizure of more than four million potentially dangerous pharmaceuticals, worth more than USD 14 million, and interrupted the activities of 37 organized crime groups. More than 34,000 unlicensed or fake products were being sold across some 2,000 websites. They included falsified masks, substandard hand sanitizers, "corona spray," "coronavirus packages," and unauthorized antivirals[11].

In the rush to secure vaccine supplies, several governments were tricked by fraudulent tactics of scamsters, leading to an alert issued by INTERPOL in August 2021[12].

Illegal wildlife trade

The illegal wildlife trade was also implicated in coronavirus related trends. Traders based in China and Laos marketed rhino horn products as "cures" for coronavirus. On September 22, 2021, the state government of Assam in India, with the largest population of the great one-horned rhino, burned 2,479 rhino horns across six giant furnaces to bust such myths in a much-publicized move[13].

Other business sectors suffering from financial distress caused by the COVID-19 crisis were also targets. These include retail and marketplaces, transportation, tourism, recreation and hospitality, arts, and entertainment. The organized criminal groups have controlled some of them by either exchanging of money for buying shares or by directly taking over operations. This would generate more opportunities for criminal activity, including money laundering and trafficking activities, allowing criminal groups to further control and use power over the illicit economy[14].

---

[11] Mapenzauswa, S., "Interpol Cracks down on the Illicit Trade of Medical Supplies", African News Agency, 20 March 2020. Available at http://www.africannewsagency.com/23972792

[12]https://www.interpol.int/en/News-and-Events/News/2021/INTERPOL-issues-global-alert-as-fraudsters-target-governments-with-COVID-19-vaccine-scams

[13]https://www.livemint.com/news/india/assam-govt-burns-around-2-500-rhino-horns-today-here-s-why-11632280986291.html

[14]The impact of COVID-19 on Organized crime, UNODC https://www.unodc.org/documents/data-and-analysis/covid/RB_COVID_organized_crime_july13_web.pdf

2.3 Examples from the region

2.3.1 India

In 2020, a total of 50,035 cases of cybercrime were reported in India thereby recording a jump of 11.8% over 44,546 in 2019. Both in 2020 and 2019, fraud related cases made up almost 60%. In 2020 sexual exploitation was the second leading reason followed by extortion while in 2019, 'causing disrepute' was the second leading cause followed by extortion.

All the same, trends across different states and cities may be at variance from the country-level macro trends. For example, the capital city of Delhi saw a significant jump in fraud cases while the crimes against women were slightly down. Telangana led in reporting of OTP (One Time Password) related crimes whereas Uttar Pradesh and Telangana topped in fake news.

Incidentally, while ransomware attacks continued to ravage computer systems around the world, most Indian states did not record a single case. Its most populous state Uttar Pradesh recorded 618 cases, Jharkhand recorded 49 and the leading IT state Karnataka recorded just 23 cases.

Movement in the public space was extremely limited during complete nation-wide lockdown from March 25, 2020 to May 31, 2020 and remained less than usual during the subsequent multi-phase process of unlocking. Hence, it is not surprising to see that the cases registered under crimes against women, children and senior citizens, theft, burglary, robbery and dacoity declined during 2020.

All the same, lockdown related enforcement resulted in a huge number of cases registered under 'Disobedience to Order Duly Promulgated by Public Servant' under the section 188 of the Indian Penal Code, 1860 as well as under similar provisions of certain state legislations.

As law enforcement agencies became preoccupied with enforcing COVID-19 rules, certain types of crimes declined even as fraud, hate speech and misinformation increased significantly. The vacuum created by inadequate and inconclusive scientific evidence was quickly filled by conspiracy theories churned out by the rumor mills and propagated through social media, at times leading to serious injuries and even life-threatening risks whether through propagation of dangerous prescriptions or utter defiance.

On the other hand, reliance on digital devices and services went up as people used it for work, entertainment, information and to keep in touch with families and friends amidst all the challenges of restrictions on travel besides social distancing in the public spaces. This reinforced ideological bubbles and amplified polarization, at times led to hate speech and defamation predicated on falsehoods or manipulated media often taken out of context.

In a survey done by Deloitte of more than 200 companies in India, 80% of respondents said that corporate fraud would rise, much higher than the 50 – 55% figure in the previous years. Also, 70% of the respondents point out that even the quantum of the fraud losses would go up and these could be as high as 1-5% of the companies' turnover. About 45% of the participants said that the fraud risk management frameworks 45% of the participants said that the fraud risk management frameworks are not adequate to tackle this future fraud and that the fraud is emanating from risks such as working from home and from new business models[15].

[15] https://economictimes.indiatimes.com/markets/expert-view/post-covid-corporates-see-huge-increase-in-cyber-crimes/articleshow/79530142.cms?from=mdr

All the same, the Indian Computer Emergency Response Team observed 11,58,208 cyber security incidents in 2020, almost three times the number (3,94,499) in 2019. It is likely that the victims grossly under-reported the cybercrime cases even as it is noteworthy that not every cyber security incident pertains to a cybercrime *per se*.

2.3.2 Indonesia

Certain crimes in Indonesia (theft covering robbery and vehicle theft) significantly increased. The crime of rape surged during the pandemic. The National Commission on Violence against Women found that reported sexual harassment and abuse, particularly online, increased. From January to October of 2020, there were a total of 659 cases of online sexual harassment and abuse and already more than doubled from the 281 cases in the previous year.

Relatedly, cases of domestic violence also rose. The Legal Aid Foundation of the Indonesian Women's Association for Justice (LBH APIK) received 1,178 reports of violence against women and children in 2020, a spike from 794 reported cases in 2019 and 837 in 2018.

Gender-based violence cases increased by 12% according to the recent online survey conducted by the National Commission for Violence against Women (NCVAW) even if it believes that cases are vastly underreported mainly due to lack of access to services as they are confined with the perpetrators at homes.

Indonesia is vulnerable to cyberattacks. These are mostly hacking cases targeting the government and corporate websites. Some government institutions like the General Elections Commission, Defense Ministry, and Indonesian Child Protection Commission were targets alongside some corporate companies like Telkomsel.

In 2019, the Indonesian National Cyber and Crypto Agency (BSSN) reported 290 million cases of cyberattacks which was 25% more than the previous year, when cybercrimes had caused losses of USD 34.2 billion for Indonesia. COVID-19 triggered a significant increase in phishing attacks, malspams and ransomware attacks, adding to the urgency of establishing a well-functioning infrastructure for cybersecurity in Indonesia.

In May 2020, the online mall Tokopedia suffered Indonesia's biggest data breach with the theft of personal data. This included emails and passwords for 91 million accounts, which was then put on sale on the dark web. Days after the Tokopedia heist, smaller rival Bhinneka, which specializes in business supplies, revealed that it too was a victim of a hack which gained access to 1.2 million accounts. In the same month, the country's election commission investigated the release of 2.3 million voters' private information on a hacker's website who threatened to release of the data of about 200 million people.

In 2021, Indonesia suffered its second massive data breach in a year involving the alleged sale of personal information belonging to 279 million people on an online forum. On May 12, an online hacking forum user started offering data allegedly belonging to national health insurance (JKN) policyholders both dead and alive in exchange for two Bitcoins, or roughly equal to Rp1 billion (USD 69,661) causing outrage about a lack of data security and privacy. Three times more data was leaked when compared with the 2019 hacking of local e-commerce platform Tokopedia, although the Communications and Information Ministry insisted in an ongoing investigation that only 100,000 entries out of 1 million checked were valid so far.

A reported data breach of the now-defunct electronic Health Alert Card (eHAC) system raised serious concerns about the security of the PeduliLindungi application, a key part of the government's "living with COVID-19" strategy. The authorities said that they had investigated a suspected data breach of

the old eHAC system, which had jeopardized the data of around 1.3 million users. The system was primarily used by the Health Ministry to help with COVID-19 contact tracing.

An Interpol-coordinated cyber operation against a strain of malware targeting e-commerce websites identified hundreds of compromised websites and led to the arrest of three individuals who were allegedly running the malicious campaign from Indonesia. The malware, known as a JavaScript-sniffer, is the online equivalent of a traditional card skimmer that targeted online shopping websites.

2.3.3 Japan

National Police Agency (NPA) data shows that in 2020, the crime rate hit the lowest since World War II with a sharp decline in street crimes. Although many different factors can cause an increase or decrease in the number of crimes, one factor in the decrease is believed to be the decrease in the number of people out of doors due to those self-restraints on going out to prevent infection from the spread of COVID-19. Overall, in 2020, the total number of known cases of penal code offences was 614,231 with a 17.9% decrease rate from the previous year. In 2019, the rate of decrease was 8.4% from preceding year.

Heinous crimes, including murder, dropped by 5.5%. Street crimes, including vending-machine vandalism and snatch-and-run cases, fell 27.0%. The decline was more prominent after the first declaration of the State of Emergency in April 2020. However, the number of consultations on domestic violence and cybercrime reached record-high levels. COVID-19-related crimes such as the burglary of closed stores and fraudulent collection of subsidies associated with measures to counter the spread of the coronavirus occurred more.

According to the same agency, the number of cleared cybercrime cases continues to increase and in 2020 increased 3.7% from the previous year. And the number of suspicious internet connection attempts detected by police rising more than 55% to a daily average of 6,506 per IP address. One of the reasons for this rise is believed to be the increase in people working remotely amid the pandemic and the increased use of home appliances and other devices connected to the internet.

The number of cases and amounts of damage in relation to online banking fraud, which had been trending lower since 2016 due to enhanced security measures at financial institutions, increased dramatically in 2019.

The number of child victims of crimes arising from social networking services had also been trending higher since 2013 but decreased from the previous year. However, the trend stayed at a high level due to cases of people who fell victim to crime when they became acquainted with others in cyberspace and so forth.

2.3.4 Laos

Laos has harnessed the internet for society’s use, for example, in the distribution of learning needs of the youth through online platforms. In January 2021, social media penetration on Laos was around 49.1% of its population. With the current restriction implemented by the government, buyers and sellers went online to communicate and to transact. The government wanted to regulate the new channels to avoid fraud, scams, and unjust enrichment in the exchanges. It established a task force to monitor social media by focusing on fake news and posts that criticize government.

In December 2020, a crime report was presented to the Minister of Public Security that there are out of the 6,200 crimes reported, 3,519 were drug-related offence, 311 finance-related crimes and the rest, theft, and other forms of crime.

The illegal wildlife trade was implicated in coronavirus related trends. Traders based in China and Laos have been marketing rhino horn products as "cures" for coronavirus. Conversation groups responded by campaigning that the demand for rhino horn in traditional medicine drives poaching has no medical value.

Organized crime took advantage of low medical supplies to sell counterfeit medical products.
Based on the report of UNDOC Darknet Cybercrime threats to Southeast Asia, users from Laos is approximately 250 user average but slightly increased to 500 user average in early 2020. There was no reported activity from Laos that uses I2P darknet from January 2019 to January 2020.

According to the Asia Pacific Computer Response Team (APCERT) Annual Report 2020, the government encountered cyber-attacks in different forms - 72.34% IP Attacks, 21.28% vulnerability, 4.3% web defacement with the rest, fraud, and phishing incidents.

2.3.5 Malaysia

In Malaysia, a total of 7,765 incidents were reported to Cybersecurity Malaysia in the first eight months of 2020 with fraud topping the list at 5,697 cases compared with 4,671 incidents for the same period in 2019. There were 11,511 (33.2%) complaints on online transactions representing 33% of all cases which is an increase compared to the 5,416 or 24.7% of total complaints received in 2019.

Malaysians suffered losses amounting to about RM2.23 billion from cyber-crime frauds since 2017. A total 67,552 cybercrime cases were reported between 2017 until June of 2021. E-commerce scams topped the chart with 23,011 cases, followed by illegal loans (21,008) and investment scams (6,273). Complaints steadily rose and as of June 2021, it was one of the most frequent complaints reported at 45% of total complaints.

Meanwhile, more than 15,000 people were arrested for contravening the movement control orders put in place since March 18, 2020. Initially, authorities sent alleged violators to jail but later shifted to on-the-spot fines after concerns on prison overcrowding that made social distancing impossible to observe or enforce.

In April 2020, the government announced that those violating control orders will be criminally prosecuted and detained at police academies. Since then, police have arrested hundreds of more people in police lockups. Courts sentenced some with fines or requirements to perform community service. Many others received jail sentences ranging from two days to several months. Those who could not pay the fines were also imprisoned.

2.3.6 Philippines

In the Philippines, the total crime volume dropped by 49.43% from 5,104 cases in January 2020 to 2,581 cases in January 2021 this year. The significant decline in eight focus crimes (murder, homicide, physical injury, robbery, theft, vehicle theft, motorcycle theft, and rape) was attributed to implementing the community quarantine across the country amid the COVID-19 pandemic.

A huge increase in online scams was recorded. There were 869 cases reported within a six-month period which is an increase of 37.3% compared to the same period for 2019. Identity theft increased by 21.47% with 362 cases. Other cases reported pertained to hoarding, price gouging, overpricing, corruption, fake tests, tampering of test results, and fake vaccination cards.

According to the National Bureau of Investigation's Cyber Crimes Division, phishing is the top cybercrime committed during the pandemic, followed by online selling scams, the spreading of misinformation that tends to cause panic among the public, online sexual exploitation, and abuse of children.

The Department of Justice (citing data from the US-based National Centre for Missing and Exploited Children) reported that cases on online sexual exploitation and abuse of children increased by 264.6% or 202,605 more reports during the imposition of the enhanced community quarantine from March to May 2020, compared to the 76,561 cases during the same period in 2019.

Philippine National Police Anti-Cybercrime group reported 869 online scams cases recorded from March to September 2020. This is higher by 37% compared to 633 incidents recorded in the same period in 2019. Filipino internet users also encountered an increase of 20% in online credit card skimmers in 2020.

The police identified the top five cybercrimes from March to September 2020 were online scams, online libel, computer-related identity thefts, anti-photo and video voyeurism, and illegal access to another's online account. These crimes were related to each other being different forms of computer-related identity theft.

The Central Bank reported on the Philippine banking system that "the disruption caused by the lockdown offered cybercriminals a unique opportunity to exploit the vulnerabilities in systems, networks, and applications used in remote working arrangements." Based on the Reports on Crimes and Losses filed by banks during the lockdown period March 15 to May 18, 2020, 98.4% of all criminal incidents reported were classified as cyber or online in nature.

2.3.7 Singapore

The latest Singapore Landscape Report noted that a significant portion of cyber activities "fed off and took advantage of the coronavirus outbreak". There is an increase in crimes relating to cyber threats such as ransomware incidents, online scams, and COVID-19 related phishing activities.

As for scams, from January to June 2020, the Singapore Police Force handled 4,226 scam cases, and 82 million Singapore dollars (SGD) were lost by victims through the top ten scam categories compared to 2019. These top four categories of scams were e-commerce scams and social media impersonation ruses, followed by loan and banking-related phishing scams. Cybercrime involving social media impersonation was also an area of concern, as the number of such scams increased from 83 in the first half of 2019 to 1,175 for the same period in 2020.

Eighty-nine (89) ransomware cases were reported to Cyber Security Agency in 2020, a sharp rise of 154% from the 35 cases reported in 2019. The cases affected mostly Small-and-Medium Enterprises (SMEs) and hailed from sectors such as manufacturing, retail, and healthcare. The significant increase in local ransomware cases was likely influenced by the global ransomware outbreak. Three distinct characteristics were observed as ransomware operators deployed increasingly sophisticated tactics. They include (a) shifting from indiscriminate, opportunistic attacks to more targeted "Big Game Hunting (BGH)"; (b) the adoption of "leak and shame" tactics; and (c) rise in "Ransomware-as-a-Service" (RaaS) models.

In 2020, the agency observed 1,026 malicious servers hosted in Singapore, a 94% increase from the 530 servers observed in 2019. The rise was in part attributed to the increase in servers distributing the highly pervasive Emotet and Cobalt Strike malware which accounted for one-third of the malware servers observed.

It also detected about 6,600 botnet drones daily with Singapore IP addresses an increase from 2019's daily average of 2,300. Variants of the Mirai and Gamarue malware were prevalent among infected botnet IP addresses in 2020, with Mirai malware, which primarily targets IoT devices, staying strong due to the continuing growth of such devices.

About 47,000 unique Singapore-hosted phishing URLs ('.sg' domain) were observed in 2020 a slight decrease of 1% compared to 47,500 URLs seen in 2019.

The overall volume of malicious phishing URLs remained comparable to the figures seen in 2019. COVID-19-related sites very likely accounted for over 4,700 of malicious URLs which spoofed local entities and services that were in greater demand during lockdown.

Four hundred ninety-five (495) '.sg' websites were defaced in 2020, a decrease of 43% from 873 in 2019. Most of the victims were SMEs, and no government websites were affected. The significant fall in 2020 is consistent with global trends and suggests that activist groups could have chosen other platforms with potentially wider reach (e.g., social media) to embarrass their victims and attract visibility for their causes. Finally, the Singapore Police Force reported that cybercrime remained a key concern, with 16,117 cases reported in 2020, up from 9,349 cases in 2019. It accounted for 43% of overall crimes reported in 2020.

Online cheating cases made up the top cybercrime category in Singapore, recording a rise of almost 62% from 7,580 cases in 2019, to 12,251 cases in 2020. This trend is attributed to the rapid growth of e-commerce, the proliferation of community marketplace platforms and social media platforms as Singaporeans carried out more online transactions due to COVID-19.

2.3.8 Sri Lanka

The Sri Lanka Computer Emergency Readiness Team (CERT) has reported an increase in the number of cybercrimes in Sri Lanka of 8,255 counts from December to 2019 to July 2020, which was a large surge from last year's cybercrime count of 3,562. Among them, 97.4% were social media cybercrimes such as impersonating other people through fake profiles, 0.07% were financial or email frauds, 0.025% were abuse, hate and privacy violation through phone hacking, and 2.5% were caused by ransomware and phishing. The most cybercrime increase was in social media privacy violation and impersonation through fake profiles as the percentage of social media cybercrime increased from 74.7% to 97.4% in 2020.

On April 2, 2020, the police announced the arrest of several persons for allegedly spreading disinformation on the COVID-19 virus. Among them was a university student who allegedly spread a rumor that a special quarantine center had been built for VIPs.

In another incident, a woman was arrested under Section 6 of Sri Lanka's Computer Crimes Act for allegedly spreading a false rumor that the country's president had contracted the virus. Section 6 refers to using a computer in a manner that poses a danger to national security, the national economy, or public order. The police have interpreted the provision to apply to false rumors regarding the head of state. In general, increased cases of violence against women and children have been reported in Sri Lanka during the COVID-19 lockdown, a trend also seen in several other countries.

2.3.9 Vietnam

In 2020, there were 5,168 cyber-attacks on information systems with a year-on-year decline of 0.15%. In the first three months of 2021, the Information Security Department under the Ministry of Information and Communications recorded 1,271 cyberattacks compared with nearly 1,600 for the first quarter of 2020 including cases of malicious code installation or malware attacks at 623 incidents.

A total number of 449 incidents of phishing attack were reported. Some of these used old techniques but took advantage of content and information presented in new ways especially information related to the COVID-19 pandemic. Separately, a total 199 incidents of 'deface attacks' took place where messages can convey a political or religious message, profanity, or other inappropriate content to embarrass website owners, or a notice that the website has been hacked by a specific hacker group.

Organized crime targeted critical information infrastructures using new cyberattack methods by exploiting security holes of online meeting applications. Cybercriminals likewise impersonated law enforcement agencies to commit fraud online by phone or though multi-level business methods beyond its borders.

3 Criminal justice challenges and responses to COVID-19 related cybercrime and electronic evidence

With the shifting criminal landscape, criminal justice authorities, faced with their own cyber limitations and challenges to institutional capacities, are pressed to rises, respond, and overcome the new cyber challenges. A quick review is presented below.

3.1 Regional criminal justice challenges and responses

Cybercrimes have always had an international dimension especially about the location of the crime, the criminals and the victims and the effect on the legal jurisdiction and practical challenges of international cooperation.

These include the disparate legislative frameworks and the different requirements for mutual legal assistance (MLA) treaties. In fact, not only definitions of certain dimensions, types of aspects of cybercrimes vary across countries, at times even the very notion of what connotes or denotes a cybercrime in one country may not even qualify as a crime in another one.

Practical, technical issues often revolve around the location of the data that is increasingly stored in the cloud; use of encryption and anonymization tools like proxies and virtual private networks (VPN); the dark web and cryptocurrencies. The proliferation of IoT devices and ever-increasing reliance on information technology further compound the challenge of the criminal justice authorities.

Some countries do not have adequate representation in regional or international organizations or are limited in their participation in bodies like INTERPOL, Europol and Eurojust, among others. Given the nature of cybercrimes and the hurdles for their successful interdiction, regional or international coordinated investigations by law enforcement authorities to target large scale operations or criminal organized groups will require a simplified and expedited process built upon the trust and interdependence of concerned agencies.

Furthermore, all these efforts are underpinned by the collection of electronic evidence. This is an arduous task even in the best of times but became even more challenging during the pandemic. Countries covered in this study were no exceptions to this phenomenon.

However, several initiatives are underway to address this challenge. For example, in ASEAN, there is a collective effort to enhance sharing of intelligence and to do joint work with the establishment of the ASEAN Cyber Capability Desk in 2018, and since renamed to the ASEAN Cybercrime Operations Desk in March 2020 in the early part of the onset of COVID-19.

3.2 Examples from the region

3.2.1 India

When India enacted the Information Technology Act, 2000[16], the Indian Evidence Act, 1872[17] was also amended simultaneously thereby paving the way for admissibility of electronic evidence in the courts of law.

The government has been issuing several guidelines[18] on strengthening the procedure for electronic evidence and its admissibility including chain of custody and other safeguards. In. addition, significant investments have been made to both develop and deploy tools for cyber forensics. Select forensic laboratories have the requisite tools – both developed indigenously by government agencies and commercial ones.

To deal with all types of cybercrimes in a comprehensive and coordinated manner, Indian Cyber Crime Coordination Centre (I4C) has been set up. It comprises seven components - National Cyber Crime Threat Analytics Unit, National Cyber Crime Reporting Portal, National Cyber Crime Training Centre, Cyber Crime Ecosystem Management Unit, National Cyber Crime Research and Innovation Centre, National Cyber Crime Forensic Laboratory Ecosystem and Platform for Joint Cyber Crime Investigation Team.

In addition, it is pertinent to mention that electronic evidence is becoming almost a feature of criminal case as there is always some evidence pertaining to mobile phones, computer devices, smart devices like CCTV and social media. Accordingly, considering the increasing case load and technological complexity both the infrastructure and manpower need commensurate investment.

Legislative process in a democratic setup like India tends to be iterative and deliberative by design, resulting in rather slower development. Also, situations keep changing and may need a faster response. Accordingly, legislations often vest certain powers with the governments for subordinate legislations. Using such powers, the Government of India notified the Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Rules in February 2021.[19]

While none of the provisions thereunder pertain specifically to COVID-19 *per se*, certain rules require significant social media companies[20] and digital news media to comply with government asks and directions in a time-bound manner or face criminal liability even as some of these rules or parts thereof are facing legal challenge across the Supreme Court of India and several High Courts. In some cases, injunctions have been granted against certain provisions[21].

Individuals should be encouraged to report cybercrimes and governments must make it easy to do so. For example, anybody can register a complaint on any type of cybercrime in India via the National Cybercrime Reporting Portal operated by the Ministry of Home Affairs.[22] It even allows registering complaints anonymously. The latter comes in handy especially in relation to cases pertaining to sexual

[16] https://www.meity.gov.in/content/information-technology-act-2000

[17] https://www.indiacode.nic.in/handle/123456789/2188?view_type=search&sam_handle=123456789/1362

[18] https://www.mha.gov.in/sites/default/files/Advisory_20052021_0.pdf

[19]https://www.meity.gov.in/writereaddata/files/Gazette%20Significant%20social%20media%20threshold.pdf

[20] Having more than 5 million users in India

[21] https://economictimes.indiatimes.com/tech/technology/madras-high-court-stays-certain-sub-clauses-of-new-it-rules/articleshow/86265232.cms?from=mdr

[22] https://cybercrime.gov.in

exploitation. Moreover, this centralized system enables authorities to monitor broad trends in real-time rather than having to wait for the annual compendia.

More worryingly, as per the report Crimes in India 2020[23] published by India's National Crime Records Bureau (NCRB)[24] the number of cybercrime cases pending at various stages of trial actually grew during 2020.

3.2.2 Indonesia

In 2019, the government of Indonesia launched a website called "Patrolisiber" for citizens to report cybercrimes. These include online scam, provocative content spread, pornography, illegal access, gambling, extortion, data/identity theft, electronic system hack, illegal interception, site appearance change, system crash and data manipulation. For the period of 2018 to 2020, most of the incidents were online scam and provocative content spread.

Previously in 2008, Indonesia passed an Electronic Information and Transaction Law that was revised in 2016. Regulations were issued in 2019 against the misuse of electronic information and transactions and for the development of a national cybersecurity strategy. To specifically cover cyber threats to national security, the Ministry of Defense implemented a regulation on cyber defense guidelines in 2014. Its Directorate of Cyber Crime (Dittipidsiber) serves as the focal unit for digital evidence and with various institutions local and internationally.

During the pandemic, the country created an application called "Pedulilindungi" to strengthen health protocols by utilizing information and communication technology integrated with contact-tracing and to employees and visitors entering offices. This app also allowed those vaccinated abroad to access public facilities by registering their vaccination status.

The challenge was that despite willingness the development and protection of ICT, cyberattacks continued with personal information illegally accessed.

3.2.3 Japan

During the pandemic, there was a shift from physical to digital offices with increased ICT reliance. Local governments and businesses introduced telework, implemented online learning, and relaxed regulations related to online medical care. In industries with work onsite, production was carried out through remote control of machine operations.

The laws are the Act on the Prohibition of Unauthorized Computer Access (1999, amended in 2013) and Penal Code (amended in 2018) for cybercrimes and the Basic Act on Cybersecurity (2018) and Telecommunication Business Act (amended in 2018) on cybersecurity. The latter law was amended to enable sharing on transmission sources of cyber-attacks through an association accredited by the government, among telecommunications carriers with its specific members.

Various governmental agencies and bodies were formed to enforce these legislations. These include the IT Strategic Headquarters, Cybersecurity Strategic Headquarters, Cyber Incident Mobile Assistant Team, Cyber Attack Analysis Council and National Center for Incident Readiness and Strategy for Cybersecurity with the Government Security Operation Coordination team to monitor and respond to cyberattacks against government ministries and agencies.

[23] https://ncrb.gov.in/en/Crime-in-India-2020

[24] https://ncrb.gov.in

A unique challenge was the scheduled Tokyo Olympics in 2021. Preparation for it spurred the creation of a Cybersecurity Council. Its purpose was to strengthen cooperation and information sharing between national government agencies, local governments, critical information infrastructure operators, information security companies, and educational and research institutions.

There is a task force consisting of several trusted security vendors and other specialized research organizations to analyse threat information and design countermeasures. The Japan CERT first organized in 1996, serving as the coordinator with businesses and organizations also implemented measures to combat cybercrime and enhance cybersecurity.

The National Operation towards IoT Clean Environment has been implemented starting in February 2019 to also secure the Olympics. This project is a nation-wide awareness campaign on securing IoT devices with alert to users of IoT devices with ID/password settings easily guessed.

3.2.4 Laos

Overall, Laos set in place a country e-government development plan in three stages of Presence, Interaction and Transaction spanning 2013 to 2020. It passed its Law on Prevention and Combating Cyber Crime in 2015 which was preceded by Law on Electronic Transaction in 2012.

During the pandemic, its government also took the initiative to utilize the internet for various purposes. A task force was created to fight misinformation or fake news related to COVID-19. It regulated the increased online transactions to avoid fraud, scams and unjust enrichment between parties in a decree on e-commerce on 12 April 2021.

The government of Laos established the Lao Computer Emergency Response Team (LaoCERT) in 2012 to undertake research and draft the cybersecurity policy, cybercrime law, data protection law and incident handling as well as the international cooperation on cybersecurity. LaoCERT was eventually elevated as the Department of Cybersecurity.

Since then, it conducted drills and exercises to test capability to counter cyber-attacks. It continues to provide training, pursues collaboration and advocacy on awareness amidst the pandemic. There is a plan to establish a Cyber Security Operations Center, Government Threats and Network Monitoring Systems. It also considering the use of honeypot and honeynet.

In addition, Laos representatives clarified during the second regional workshop that the country encountered important challenges on reporting and for the law enforcement to understand and to have an adequate response. They further stated that there is no specific unit for dealing with cybercrime. However, cybercrime issues are mostly handled by the police.

3.2.5 Malaysia

There are several cyber-related laws in Malaysia. These include the Communications and Multimedia Act 1998, Computer Crimes Act 1997, and the Penal Code. There is also the National Cybersecurity framework to guide industries and provides support for digitalization across government services, energy, healthcare, finance, and defence.

Among the challenges was the lack of cyber security professionals. A proposal was made to set up a committee consisting of the relevant government agencies of law enforcement and banking, and telecommunication companies to discuss, monitor and identify effective actions to address cyber issues.

During the pandemic, a COVID-19 Act was legislated that amended several laws including the extension of the applicable period and credit transactions, relaxing insolvency and relief from distress, the right to possess after default. An Anti-Fake News (Repeal) Act of 2020 also took effect.

In addition, Malaysian representatives clarified during the regional workshops that public awareness campaigns were implemented in view of preventing individuals from being victims of online fraud and also actions for prevention of commercial crime have been taken. They also stated that Cooperation with private sector is also active, and a platform is available for exchange of practical information. The National Cybercrime Cooperation Committee ensures inter institutional cooperation and comprises also the private sector. The activity of the Cybercrime Unit is being overseen by the Transnational Crime Unit while all evidence needs to be presented in court upon formal request, therefore, informal cooperation would be needed in order to accelerate the process.

3.2.6 Philippines

During the last two years, criminal justice authorities activated social media accounts for easier reach and for reporting. There was a noticeable shift to cybercrimes with financial impact like phishing and other types of online fraud including the peddling of facemasks and vaccines. A particular *modus operandi* similar to those in Indonesia was the proliferation of online lending platforms that gathered personal information or by requiring the download of their app that then accessed personal details for exploitation.

The police launched two IT projects to prevent the proliferation of fake news that endangers people's health. One is Project E-*Sumbong* an online platform to file complaints and seek police assistance. Second is Project E-Access that provides a channel for cybercrime prevention awareness with information on online accounts or mobile phone numbers used in committing cybercrime particularly financial fraud.

There was a deliberate effort to strengthen interagency collaboration. Cybercrime units were actively communicating with each other on intelligence sharing via regular online consultations to exchange legal advice and procedures particularly in the collection of electronic evidence. It was recognized that operations of service providers were limited during the period but international cooperation continued with foreign and industry partners to follow the threat landscape. Best practices on successful cases were adopted and integrated into multi-agency training activities.

Law enforcement agencies prioritized the raising of public awareness through online platforms on how to apply cyber hygiene. Public advisories on how to protect from cybercrime and provide tips on how to be victimized by cybercriminals were regularly issued. The government launched an online portal on COVID-19[25] or the public to access reliable news and information on the current situation and another on working from home[26] for government employees to adjust to new work arrangements.

Special purpose laws were legislated to address the pandemic including the penalizing of false information. There is currently pending legislation on increasing protection against online sexual abuse and exploitation of children, focused anti-phishing with the rise in these types of cases during the pandemic.

[25] www.covid19.gov.ph

[26] wfh.gov.ph

3.2.7 Singapore

Singapore passed a Cybersecurity Act in 2018 headed by a Commissioner of Cybersecurity. This complements its Computer Misuse Act that was legislated way back in 1993 to cover several cyber offences.

Given its push towards adoption of technologies, the government progressively built up its digital infrastructure that enabled responses to the pandemic. A menu of digital tools were made available – 1) Ask Jamie chatbot as a virtual assistant designed to answer queries within specific domains on government websites with enhancement for COVID-19 questions; 2) COVID-19 Chat for Biz addresses questions from businesses including information on measures to help businesses; 3) COVID-19 GoBusiness Portal to support businesses applying for work permits and monitoring by police; 4) COVID-19 Situation Report is a dashboard presenting key statistics and figures on the current situation; 5) FluGoWhere is a website to search through a list of subsidized clinics for those with respiratory illnesses; 6) Gov.sg WhatsApp provides multi-lingual updates on the COVID-19 situation; 7) MaskGoWhere is another website to find the designated location, day and time to collect their allocation of masks; 8) Leave of Absence/Stay-Home Notice Tracking Solution is an SMS and mobile web-based solution that allows people serving out their Leave of Absence or Stay-Home Notice to report their locations; 9) Self-help Temperature Scanner to implement temperature checks prior to entry to buildings/offices; 10) SafeEntry is a national digital check-in system that logs the name, national identity number and mobile number of individuals visiting hotspots and venues providing essential services and workers thereat; and 11) TraceTogether is a mobile app for community-driven contact tracing.

Concurrently and with the increase of cyber-attacks, systems to prevent or reduce them were put in places. These include allowing the defensive use of cyber tools like beacons, honeypots, and sinkholes with safeguards on data protection.

Singapore joined the Interpol-led Global Financial Crime Task Force with the mandate to investigate COVID-19 vaccine scams. With the roll out of vaccination programs globally, criminal syndicates were conducting their schemes with links to financial hubs. The task force will also look into business email compromise scams and identify criminals who exploit government schemes that support businesses during the pandemic.

3.2.8 Sri Lanka

Sri Lanka is the third country in the study that is a member of the Budapest Convention of Cybercrime. At present, it is implementing an Information and Cyber Security Strategy (2019-2023). In 2003, it passed the Information and Communication Technology Act, followed by the Electronic Transaction Act of 2006 and Computer Crime Act of 2007. It also established the Information and Communication Technology Agency (ICTA) and the Cyber Crime Unit (CC).

In January 2020, the country established a Presidential National Task Force on COVID-19 with guidelines in managing patients introduced in the healthcare sector on the same day. During the pandemic, there were no specific pandemic-related laws.

The Sri Lanka Computer Emergency Readiness Team (CERT) continued to function. In April 2020, the police announced the arrest of several persons for allegedly spreading disinformation on the COVID-19 virus.

As response to the rise of cryptocurrency, the country organized a special committee tasked to formulate the country's policy on digital banking and crypto-related activities. Other initiatives include the National

Digital Policy for Sri Lanka (2020-2025), National Payment Platform, HealthTech (Digital Health), digital transport and digitalization of key government services including the courts and police.

3.2.9 Vietnam

Vietnam also passed its Law on Cybersecurity in 2018. The existing penal code was amended to punish cybercrimes. Previous laws in 2006 regulated e-transactions, in 2007 covered information technologies, in 2016 on cyber information security.

A number of cybersecurity teams were formed under the Ministry of Public Security. These include the Department of Cyber Security and Hi-tech Crime Prevention and Vietnam Cybersecurity Emergency Response Team/Coordination Centre (VNCERT/CC). These two agencies are instrumental to the country's cyber responses.

To illustrate, in 2020, it cracked down on an illegal ring of online gamblers in the form of online football betting. In 2018, it successfully investigated 27 specialized criminal cases and coordinated with other investigation agencies at all levels to prosecute 15 criminal cases and 121 arrestees as well as extradite 555 foreign criminals.

By end of 2020, the government adopted a multi-layered model of security measures by the end of 2020. A cybersecurity plan was implemented.

4 Preparing criminal justice systems for future crises: assessment and recommendations

The COVID-19 pandemic is not the first global crisis to severely challenge criminal justice systems, and it will not be the last. Offenders are and always will be opportunistic in times of crisis, with their activities spanning geographical systems and political and legal systems. Criminal justice authorities, in contrast, remain bound by geographical limitations, legal frameworks and procedural rules.

While presenting serious challenges, crises none the less provide important opportunities to assess the preparedness and responses of countries worldwide to combat cybercrime. Such a comparative assessment can be based on questions such as:

- How prepared are countries to respond to crises?
- Do they have the legal framework and basis with rule of law safeguards for an effective criminal justice response?
- Do they have cooperation mechanisms with the private sector in general and the service providers in particular?
- Do they have the tools needed for international cooperation like bilateral and multilateral treaties and conventions?

This section draws on the information collected in preparation of this report as well as the results of other studies conducted over the last two years to assess how criminal justice authorities in the Asian region are responding to COVID-19-related cybercrime and present recommendations on how they can strengthen their legal, policy and institutional frameworks to increase their preparedness for future crises.

4.1 Legal and policy frameworks and safeguards

Without comprehensive substantive legal provisions penalising cybercrimes and related crimes, and well-defined procedural codes with necessary safeguards and enforcement powers for the collection of electronic evidence, a country cannot have an appropriate criminal justice response to mitigate the effects of cybercrimes. This is particularly the cases in crisis situations.

In terms of substantive law, some national legislation does not criminalise the publication or circulation of "fake news" related to COVID-19. Such disinformation would also not fall under computer-related forgery provisions, because inauthentic data with the intent that it be considered or acted upon for legal purposes as if it were authentic do not fall under forgery offences. This prompted several countries to undertake or consider amendments to their laws to overcome this growing menace. Any such reforms would, however, need to be carefully devised to reflect freedom of expression guarantees. On the procedural side, countries' criminal justice responses will remain ineffective – even if they have the necessary substantive provisions in place – if law enforcement authorities do not have the procedural powers required to issue enforceable orders for the preservation, production, search and seizure, and disclosure of computer data, and if such data is not admissible in court.

A review of the cybercrime legislation in the selected Southeast Asian countries, using the Country Wiki profiles published as part of the Council of Europe Octopus Platform,[27] shows that the domestic legal situation varies significantly. Most countries' legal frameworks include provisions incorporating the substantive offences set out in the Budapest Convention:

- Illegal access, illegal interception, data interference and system interference (Articles 2, 3, 4 and 5 BC) are criminalised in all the countries.
- Misuse of devices (Article 6) and infringements to copyright (Article 10) are criminalised in all countries except Singapore.
- Computer-related forgery is not criminalised in Singapore, Sri Lanka and Vietnam. It is criminalised in Laos and India, but the criminalisation does not cover inauthentic data.
- Computer-related fraud is criminalised in all countries except Laos.
- The criminalised of offences related to child pornography differs significantly across the selected countries. It is not criminalised in the Philippines and Singapore. It is criminalised in Malaysia, Laos and Vietnam, but not in a manner fully compliant with Convention.

Frameworks for procedural powers pertaining to electronic evidence are even more varied:

- Of the countries covered, only laws in India, Laos, Sri Lanka and Japan contain procedures for the preservation of data and partial disclosure of traffic data (Articles 16 and 17 BC) in their legal frameworks.
- Production order powers are present in the legislation of all the countries except Indonesia and Singapore.
- Search and seizure provisions are present in the legislation of all the countries except Laos.
- Articles 29 and 30 of the Convention related to expedited preservation of stored computer data and Expedited disclosure of preserved traffic data are codified only in Sri Lankan and Japanese legislation.
- Article 32 related to trans-border access to data is codified only in Singaporean legislation. In India, the law enforcement agencies often use the Section 91 of the Criminal Procedure Code, 1974 even as some obligations have been imposed even under the Information Technology Act, 2000 albeit under subordinate legislations.

[27] https://www.coe.int/en/web/octopus/home

Notably, several of these issues were also identified in a study of cybercrime laws in the Asia-Pacific region prepared in 2007-8.[28]

From a policy perspective, national cybercrime strategies can underpin a better response to cybercrimes related to the COVID-19 pandemic by building the resilience of national infrastructure and services, which can help countries counter cyber threats effectively and protect communities from data breaches. For example, defining a certification for ICT products, processes and services in strategies is an important step in limiting the misuse of devices and crime as a service (CaaS).[29] INTERPOL's recent survey identified the absence of a such strategies in response to the COVID-19 pandemic in 30 member countries, however, highlighting a persistent gap in the policy response.[30]

Mechanisms for data preservation

Articles 16 and 17 of the BC require all parties to adopt the necessary measures to enable their competent authorities to order or similarly obtain the expeditious preservation of specified computer data, including traffic data that has been stored by means of a computer system. Parties are given flexibility in determining how to implement preservation, though the Convention requires that it be done as quickly as possible.

This power is very important given the volatility of computer data and the ease with which it may be deleted, modified, or altered, and because many service providers and persons do not retain computer data for long periods of time. Notably, there are no mandatory data retention rules in the United States, or at European Union level, since the Data Retention Directive was declared invalid by the Court of Justice of the European Union in 2014.

Among the countries covered by this report, it seems that only Laos, Sri Lanka and Japan have procedures for preservation of data and partial disclosure of traffic data in their legal systems.

Mechanism for production order

Article 18 of the BC empowers competent authorities to order a service provider offering its services in the territory of the Party to submit subscriber information relating to such services in that service provider's possession or control. This article is currently mainly used at the national level: competent authorities use this power to order service providers located within their territories to submit subscriber information.

However, Article 18 can also be used to order service providers located in another jurisdiction, but offering services within the territory of the Party, to produce subscriber information without requesting formal mutual legal assistance. This includes situations where a service provider enables persons to subscribe to its services in a territory, even if they have no physical presence there, or if the service provider has established real and substantial connection to the Party, for example through local advertising, or using local subscriber information or associated traffic data in the course of its activities.

Countries that have implemented Article 18.1.b of the BC in an enforceable manner in their national legislation are in a stronger position to develop effective public-private cooperation, including with the

[28] In 2007-08, Microsoft had published: 'Current and Pending Online Safety and Cybercrime Laws' by benchmarking then prevailing or proposed legislations across 14 Asia—Pacific countries, including 12 in Asia against the Cybercrime Convention https://www.itu.int/ITU-D/cyb/cybersecurity/docs/microsoft_asia_pacific_legislative_analysis.pdf

[29] Interpol, COVID-19 Cybercrime Analysis Report- August 2020

[30] Interpol, COVID-19 Cybercrime Analysis Report - August 2020. Available at: https://www.interpol.int/content/download/15526/file/COVID-19%20Cybercrime%20Analysis%20Report-%20August%202020.pdf

main international service providers such as Meta (Facebook and Instagram), Microsoft, Google, Twitter and Apple.

Recommendations: address gaps in national legal and frameworks

- Countries in the region need to improve their legislation by filling the gaps in substantive and procedural law on the national. Such amendments will ensure a strong legal basis and allow a swift and solid criminal justice response to cybercrime, including in crisis situations.
- Countries which are already parties to the Budapest Convention should rapidly sign and implement the Second Additional Protocol to the Budapest Convention. Domestic reform processes to align national legislation with the Protocol's provisions can be started immediately.
- Countries should develop comprehensive national cybercrime strategies to provide a clear policy and institutional framework to responding to cybercrime in crisis situations.

4.2 International cooperation between criminal justice authorities

Cybercrimes typically cross borders, spanning both different jurisdictions and legal systems. This presents significant challenges to criminal justice authorities, who need to cooperate with countries with different legal and institutional frameworks to ensure they collect the evidence they require. The role of the police and prosecutors may be different in common law and civil law countries, for example. International cooperation is therefore an essential component of an effective criminal justice response. Without it, countries are likely to face significant challenges in collecting the electronic evidence necessary to successfully investigate and prosecute cybercrimes and related offences.

The INTERPOL COVID-19 Cybercrime Analysis Report of 2020 highlighted the importance of collaboration among national law enforcement authorities and timely responses to the requests for information that they receive from other countries. Cooperation and information exchange is particularly critical to address threats of ransomware attacks against critical infrastructure, indicator of compromise, bitcoin addresses; cases related to Advance Payment Fraud (APF) and Business Email Compromise (BEC); malware spreading via non-governmental contact tracing applications; and details around campaigns leveraging high volume of malicious domains.

The Budapest Convention on Cybercrime is the only global treaty providing comprehensive and legally binding procedures for international criminal justice cooperation on cybercrime and cross-border access to electronic evidence. While some of the international cooperation tools are common to other international conventions, others are not included in any other global treaty. These include specific provisions regarding: expedited preservation of stored computer data; expedited disclosure of preserved traffic data; mutual assistance regarding accessing of stored computer data; and mutual assistance in the real-time collection of both traffic data and content data. In addition, the Second Additional Protocol to the Budapest Convention, adopted in November 2021 and opened for signature in May 2022, provides further tools to facilitate smoother cross-border cooperation between law enforcement and judicial authorities, including in emergency situations.

Mechanisms for spontaneous information sharing

Article 26 of the BC addresses spontaneous information sharing. When the authorities from a Party, within a domestic investigation, discover that some of the information they obtained could assist another Party in initiating or carrying out investigations or proceedings concerning offences under the BC, they can forward this information to the other Party without any formal mutual legal assistance request. This can be a powerful tool particularly in crisis situations, such as that caused by the COVID-19 pandemic.

There is a perceived lack of awareness and use of Article 26 as a tool to actively exchange cross-border electronic evidence. Consultation with countries in the regional workshops conducted in the preparation of this study shows that they do not view it as a proactive tool for sharing relevant information without formal requests. Indeed, none of the countries covered by this report indicated that they make use of this provision, and only a few – including Indonesia –have incorporated it into their domestic legal system.

Mechanisms for trans-border access to data

Article 32 of the BC allows criminal justice authorities, without the authorisation of another party or a request of international cooperation, to access the data computer stored outside their jurisdiction in two cases. The first is when the data is publicly available (open source), such as information on news websites or posted on social media; and the second is if authorities obtain the lawful and voluntary consent of the person who has the authority to disclose it.

Without this Article, an MLA request would be needed every time a law enforcement official checks the data posted publicly but stored in another country and even when the voluntary consent of the authorised person to access the data is given. This provision is absent from the legislation of most of the countries covered this report, except Singapore.

Availability of 24/7 Point of Contact (PoC)

Article 35 of the BC requires each Party to designate a point of contact available on a 24/7 basis to ensure the provision of immediate assistance criminal investigations or proceedings concerning criminal offences related to computer systems and data or the collection of electronic evidence. These 24/7 points of contact should be able to provide technical advice for stopping or tracing an attack, and facilitate the preservation of data pursuant to request, the collection of evidence and the provision of legal information. The Council of Europe supports cooperation between these 24/7 points of contact by facilitating the functioning of the 24/7 Networks established under Article 35, including maintaining a Directory of the contact points.[31]

Recommendations: strengthen formal and formal avenues of international cooperation

- Good international cooperation requires strong legal frameworks and robust central authorities for quick and effective responses. Countries should ensure they have transposed the international cooperation provisions of the Budapest Convention and its Second Additional Protocol into their domestic legal frameworks.
- Countries should simplify their procedures for mutual legal assistance, for example by accepting electronic requests.
- Countries should make further use of the spontaneous information provisions of the BC.
- Countries, with support from the Council of Europe, could develop case studies on best practices in the region on international cooperation.
- Countries should make full use of the 24/7 Network established under the BC, as well as other semi-formal or informal channels of communication, such as with Interpol, Europol or Eurojust.

[31] The 24/7 Network established under the Budapest Convention on Cybercrime - https://www.coe.int/en/web/cybercrime/24/7-network-new-

4.3 Public-private partnerships

Internet service providers (ISPs) possess significant amounts of the electronic data that is crucial for almost every contemporary criminal investigation. Public-private partnerships and effective mechanisms for the judiciary and police to access data stored by service providers in the private sector are therefore critical components of the investigation and prosecution of cybercrime. By sharing intelligence and expertise on past or imminent trends and threats in real-time as well as by providing technical assistance, private sector companies can serve as valuable partners for law enforcement agencies in combatting cybercrime.

Cooperation with national service providers usually poses relatively few problems, as they are clearly bound by the national legislation of the country in which they are located. In contrast, criminal justice authorities have often found cooperation with international service providers based outside their country challenging. Law enforcement authorities assume that, with respect to certain data, ISPs are obliged to cooperate; the service providers say they will cooperate – to a certain extent – not because they have to, but because they are willing to do so voluntarily.
Although the rising number of cybercrime cases during the pandemic has made public-private cooperation even more important, it has both exacerbated existing cooperation challenges and created new cooperation needs:

- Getting assistance from service providers in foreign jurisdictions became more difficult due to high numbers of staff in quarantine or working remotely.
- Cooperation with domain name providers and ISPs was needed to quickly take down fraudulent websites selling or offering products falsely claiming to treat or prevent COVID-19. Before COVID-19, this was not the first step in an investigation, as blocking a website might alert the criminal to an investigation and prompt them to delete evidence.
- The need for quick action made the traditional channels of sending an MLA request for a service provider to execute a production order or to remove of specified data from a computer system unfeasible, as these procedures are time consuming.

Working with the private sector to track cyber threats

Since January 2020, the INTERPOL Cybercrime Directorate has aggregated data and information on COVID-19 cyber threats from member countries, INTERPOL private partners, National Computer Emergency Response Teams (CERTs), the Internet Corporation for Assigned Names and Numbers (ICANN) and online information sharing groups such as Slack. INTERPOL aims to develop a database that all stakeholders can contribute to and access in developing the most effective cybercrime threat response. A strong relationship between law enforcement and private industry and forged sense of shared responsibility in the fight against COVID-19 cyber threats and enables timely and targeted response to emerging cyber threats.[32]

Recommendations: enhance mechanisms for public-private cooperation

- Governments should ensure they incorporate the provisions for direct cooperation with private service provides in the BC and its Second Additional Protocol into their national legal frameworks.

[32] Interpol, COVID-19 Cybercrime Analysis Report- August 2020. Available at: https://www.interpol.int/content/download/15526/file/COVID-19%20Cybercrime%20Analysis%20Report-%20August%202020.pdf

- Government agencies should seek to build more structured relationships with the private sector by, for example, signing memorandums of understanding with service providers, creating collaboration platforms or creating dedicated task forces.
- The capacity of 24/7 points of contact should be strengthened to enhance their ability to facilitate direct cooperation with (foreign) ISPs.

4.4 Digitalisation and resources

Cybercrimes are facilitated by technology, electronic evidence is digital, and the tools needed to carry out investigations and analyse electronic evidence are digital too. An effective criminal justice response is therefore not possible unless criminal justice authorities themselves are digitalized, both in terms to the tools at their disposal to identify and prevent cybercrimes, and the processes they use during criminal proceedings. Ensuring criminal justice authorities have the tools they need to respond to new and emerging cybercrimes requires sustainable investment in both human resources and technical equipment.

The COVID-19 pandemic forced criminal justice authorities to rapidly shift their work online without the necessary preparation or equipment. As a result, data was endangered, and vulnerabilities were exposed and exploited by criminals. More positively, the new working methods imposed during the pandemic period offer efficiency gains and more effective ways to track trends, share information and record cybercrime incidents.

Recommendations: enhance digitalisation and specialisation

- Governments should ensure their criminal justice authorities have the necessary digital tools for carrying out investigations and analysis of electronic evidence analysis.
- Countries should prioritise electronic communication wherever possible when exchanging case-related data nationally or internationally in cross-border criminal cases.
- Courts should, where possible and in line with domestic procedures, extend and expand the use of e-filing of pleadings, virtual hearings, or online corpus of judgments and orders.
- Countries should create specialised cyber or high-tech crime units, and ensure they are continuously retrained and retooled to meet changes in the criminal justice landscape. Situating them within police headquarters or central prosecutors' offices will help to harness specialization on handling electronic evidence.

4.5 Capacity building

States' response to cybercrime can only be effective if criminal justice practitioners possess the necessary legal and technical skills to undertake the tasks. As cyber threats continue to evolve, including within the pandemic context, judges, prosecutors, and law enforcement agencies must constantly upgrade their capacities, capabilities and technologies, and refine their protocols for internal and external communication and cooperation. Well-trained and well-equipped cybercrime and cybersecurity professionals are an essential resource in the fight against cybercrime.

A significant number of capacity building activities have been conducted in Asia with the support of the European Union and the Council of Europe through its Cybercrime Programme Office (C-PROC). Many of the states covered by this study have benefited from these trainings over a number of years. In addition, some participants in the regional workshops indicated they had participated in trainings organised by other actors such as the UN.

However, the pandemic had a significant effect on capacity building. Redeployment of staff to COVID-19-related tasks, prolonged lockdowns and high levels of staff sickness limited training opportunities. C-PROC adapted its working methods to provide online or hybrid trainings, allowing it to continue its work to build the capacity of criminal justice authorities in Asia. INTERPOL recently launched its Virtual Academy to provide a wide range of online training opportunities for law enforcement.[33] The INTERPOL Cybercrime Directorate is hosting online training courses and webinars to enhance member countries' capabilities to face the emerging cyber threats and successfully investigate cybercrime cases.[34]

To ensure complementarity, it is important to integrate capacity-building initiatives 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).[35]

Recommendations: enhance specialised capacity building

- Countries should make full use of the capacity building support provided by C-PROC and other actors, including with respect to the following recommendations.
- Countries should ensure that they include cybercrime and electronic evidence in the curriculum of training academies for criminal justice practitioners, and take steps to integrate the lessons learned from the COVID-19 pandemic into training courses.
- Countries should develop and adopt national training strategies on cybercrime and electronic evidence to ensure comprehensive and structured training and capacity building.
- Countries should promote online training and join available online learning platforms.

4.6 Information sharing and reporting

The nature of cybercrime means that successfully investigating and prosecuting it involves a wide range of different actors, from victims to the private sector and criminal justice authorities. For them to cooperate effectively, they need to share information.

In many cases, an investigation starts with victims – whether individuals or businesses – reporting the attack. Yet less than one percent of cybercrime is reported. A culture of acceptance, transparency and trust is needed to build a safe environment for reporting cybercrimes and embed the belief that reporting cases increases both individual and collective safety and security. Once reported, criminal justice authorities will need to work together to investigate and prosecute cybercrime. Structured information sharing based on trust, and implemented using channels for regular and fast dissemination of information is crucial.

Sharing information on types of cybercrimes and emerging threats, as well as lessons learned from this and previous crises, strengthens prevention measures and so mitigates the effect of criminals trying to take advantage of the COVID-19 pandemic. Such information sharing can also provide a basis for joint investigations. The INTERPOL Cybercrime Collaborative Platform, hosted within the Cybercrime Pavilion of INTERPOL's Global Knowledge Hub, is designed for knowledge exchange and operational coordination. It provides a secure solution for member counties to engage in multi-stakeholder and multi-jurisdictional joint task forces to combat crimes against computer systems. This facilitates direct communication

[33] https://www.interpol.int/en/How-we-work/Capacity-building/INTERPOL-Virtual-Academy

[34] Interpol, COVID-19 Cybercrime Analysis Report- August 2020. Available at: https://www.interpol.int/content/download/15526/file/COVID-19%20Cybercrime%20Analysis%20Report-%20August%202020.pdf

[35] https://asean.org/plan-of-action-to-implement-the-joint-declaration-on-comprehensive-partnership-between-asean-and-the-united-nations-2021-2025/

between operational teams in the member countries and with INTERPOL for the effective sharing of cybercrime information to develop timely operational responses.[36]

Recommendations: systematise information sharing and reporting

- Countries should update existing procedures and manuals to take into account the experiences and lessons learned during the pandemic. Crisis response and disaster management in the digital realm should be integrated into these procedures and manuals.
- Countries should acknowledge the specific lessons learned from the COVID-19 pandemic and formulate or revise policies to be used as a guide to future incidents. Using the experience gained during this and other crises, countries will be able to monitor selected factors to anticipate developments and be better prepared to face future crises.[37]

4.7 Prevention and awareness-raising

The evolution of cyber threats seen during the COVID-19 pandemic is projected to continue posing legal and operational difficulties for law enforcement agencies worldwide. Implementing prevention and awareness-raising measures helps to mitigate this impact.

Awareness can be promoted by educating and empowering the public on online behavior and operational hygiene on the internet. Given the evolving nature of cybercrime, information campaigns must be regularly updated and revised. With a better understanding of the threats, everyone can respond more effectively.

Up-to-date information on newly identified cyberattacks enables the INTERPOL Cybercrime Directorate to accurately project emerging trends and share criminal modus operandi via the INTERPOL global network to promote awareness and prevention. This particularly concerns cases of ransomware attacks against governments, critical information infrastructure including the healthcare sector that may cause a major risk and harm to public safety and security. Receiving timely and relevant information allows INTERPOL to support member countries in formulating and executing an effective response.[38]

Recommendations: strengthen public awareness on cyberhygiene

- Countries should adopt a whole-of-government approach to embedding cyber awareness. The same channels that disseminate misinformation can be used to effectively communicate and empower citizens on the nature, power and pitfalls of internet technology.
- Countries are encouraged to share the key messages of INTERPOL's global #WashYourCyberHands campaign within their communities through social media platforms and to launch similar awareness campaigns at the national level.[39]

4.8 Statistics and data collection

---

[36] Interpol, COVID-19 Cybercrime Analysis Report- August 2020. Available at: https://www.interpol.int/content/download/15526/file/COVID-19%20Cybercrime%20Analysis%20Report-%20August%202020.pdf

[37] https://www.europol.europa.eu/media-press/newsroom/news/beyond-pandemic-what-will-criminal-landscape-look-after-covid-19

[38] Interpol, COVID-19 Cybercrime Analysis Report- August 2020. Ibidem.

[39] ASEAN Cyber Threat Assessment 2021. Available at: https://www.interpol.int/content/download/16106/file/ASEAN%20Cyberthreat%20Assessment%202021%20-%20final.pdf

Understanding the type and trends of cybercrimes allows criminal justice to prioritise and plan effective measures to prevent and combat them, and to prioritise limited human and financial resources. However, many countries do not collect comprehensive data on a regular basis. In addition, the UN Crime Congress Kyoto Declaration[40] – adopted in March 2020 – acknowledges that the lack of uniformity of data collection methodology in Southeast Asia[41] hinders a unified response.

Defining priorities needs an accurate picture-of-threat. When the true scale of the phenomenon is gauged, authorities will be able to triage and direct resources towards the crimes that cause the most serious harm. Those crimes pose the greatest threats to children, livelihoods, wellbeing, health, life and societal development[42] as well as national security, critical information infrastructure and particular groups such as women.

Data collected during the pandemic has been used to shift priorities. Evidence showing increases in online child exploitation and targeting of health facilities prompted governments to reallocate resources to defend against these attacks. Pre-pandemic, the health sector was not considered a national security issue, but the COVID-19 pandemic placed it at the heart of critical infrastructure.[43]

Recommendations: use data to inform decision-making

- Countries should ensure that they systematically collect data on the type and extent of cybercrimes.
- Data should then be fed into decisions on prioritisation and resource allocation.

5 Conclusions

The information collected for this study confirms that, across Asia, cybercrime significantly increased during the COVID-19 pandemic. Cybercrime also increased in severity and mutated into new forms, including crimes involving procurement of medical supplies and services, as well as crimes that took advantage of widespread lockdowns and work-from-home requirements.

Criminal justice authorities' preparedness and response to the pandemic varied significantly. Some countries were more prepared in terms of government offices or agencies tasked to manage certain aspects of cybercrime and cybersecurity. For example, the task force established in Japan in 2019 to address cyberattacks linked to the 2020 Tokyo Olympics (postponed to 2021) provided a structure to respond to the new threats associated with the pandemic.

Governmental responses, in contrast, were broadly similar. Specific legislation to address the pandemic situation was passed, while other laws were modified or amended to bring them up to speed with the evolving situation. Some countries, such as Laos, Philippines, Singapore, and Sri Lanka, implemented legislation on so-called "fake news" to specifically counter misinformation that endangered public health and security. Evidence suggests that countries with a strong legal framework covering electronic transactions and signatures, cybercrimes, data privacy and cybersecurity – with the accompanying

[40] https://documents-dds-ny.un.org/doc/UNDOC/LTD/V21/006/54/PDF/V2100654.pdf?OpenElement

[41] UNODC CYBERCRIME AND COVID19 in Southeast Asia – April_2021. Available at: https://www.unodc.org/documents/Advocacy-Section/UNODC_CYBERCRIME_AND_COVID19_in_Southeast_Asia_-_April_2021_-_UNCLASSIFIED_FINAL_V2.1_16-05-2021_DISSEMINATED.pdf

[42] UNODC CYBERCRIME AND COVID19 in Southeast Asia - April_2021. Ibidem.

[43] Healthcare is not yet one of the sectors under the ambit of the National Critical Information Infrastructure Protection Centre (NCIIPC), a statutory body in India https://nciipc.gov.in

procedural rules – tend to be better placed to revise or pass new legislation as part of the continuing development of their legal frameworks. Another similarity in the responses was the adoption and use of technology in the form of apps and other technologies for contact tracing and health assessments, with varying degrees of success.

The experiences captured in this report indicate that the underlying difficulties and challenges encountered by criminal authorities did not change during the pandemic:

- The normative question of what is or what is not cybercrime persisted, with overlaps in activities to address cybercrime and cybersecurity continuing. Lack of definitional and practical clarity continues to impede effective responses from both policymakers and criminal justice authorities.
- Institutional inertia remained a challenge, with some authorities struggling to respond to the urgent and wide-ranging difficulties presented by the pandemic. The importance of upholding rule of law and human rights standards, and implementing due process and procedural safeguards, was sometimes experienced as constraining rapid responses.
- Effective cooperation at the national and international levels was in some cases hampered by information silos and competition between different authorities. The proliferation of entities involved in combatting cybercrime requires more coordination and collaboration to promote synergies between entities with different mandates and functions, particularly as the threat landscape becomes more complex.
- The need for specialised procedures and technical capabilities for handling electronic evidence remains significant given the importance of this information for the investigation of cybercrimes and other offences.
- The importance of establishing clear data protection frameworks setting out what personal data can be shared, who has access to it and how long it can be kept for, to ensure that criminal justice authorities are able to effectively investigate and prosecute cybercrimes and crimes involving electronic evidence while upholding privacy and data protection rights.

Despite these common challenges, the COVID-19 related cybercrime situation in each country is unique. As such, solutions and responses must always be customised to fit the country's traditions, socio-legal context, institutional architecture and current practices.

6 Appendix

6.1 Resources

1. TelSoc Telecommunications & the Digital Economy, Journal, AJTDE Volume 5 No. 3 August 2017, https://telsoc.org/journal/ajtde-v5-n3/a96
2. Center for Indonesian Policy Studies, Policy Brief, March 2021, https://repository.cips-indonesia.org/publications/341779/cybersecurity-protection-in-indonesia
3. Reuters, (22 May 2020), Indonesia probes breach of data on more than two million voters, https://www.reuters.com/article/us-indonesia-cyber-breach-idUSKBN22Y15K
4. Straits Times, (10 July 2020), https://www.straitstimes.com/asia/se-asia/indonesia-moves-to-beef-up-cyber-security-with-data-protection-law
5. The Jakarta Post, (23 August 2020), https://www.thejakartapost.com/news/2020/08/23/civil-groups-condemn-cyberattacks-on-indonesian-government-critics.html
6. The Jakarta Post, (4 June 2020) https://www.thejakartapost.com/news/2020/06/04/crime-in-indonesia-surges-in-late-may-police.html
7. The Jakarta Post (25 November 2020), https://www.thejakartapost.com/news/2020/11/25/online-sexual-abuse-has-more-than-doubled-during-pandemic.html
8. The Jakarta Post (12 January 2021), https://www.thejakartapost.com/paper/2021/01/12/coronavirus-pandemic-leads-to-rise-in-domestic-violence-cases-in-indonesia.html
9. Cybersecurity laws and regulations: Japan, available at https://iclg.com/practice- areas/cybersecurity-laws-and-regulations/japan
10. Dr. Brian Grant (August 2021), The Tokyo Olympics are a cybersecurity success story, https://www.securitymagazine.com/articles/95880-the-tokyo-olympics-are-a-cybersecurity-success-story
11. ICLG, 2021. Impact of Covid-19 on employment in Japan, https://iclg.com/practice-areas/employment-and-labour-laws-and-regulations/3-the-impact-of-covid-19-on-employment-in-japan
12. Adelstein J. March 2, 2020. Criminals are taking advantage of fear over COVID-19, https://www.japantimes.co.jp/news/2020/03/02/national/media-national/criminals-taking-advantage-fear-covid-19
13. Kyodo (July 2021), Tokyo Olympics ticket purchasers; login IDs and passwords leaked online, https://www.japantimes.co.jp/news/2021/07/21/national/crime-legal/olympic-ticket leak
14. Kyodo (June 2021), Japanese police to launch team to fight cyberattacks, https://www.japantimes.co.jp/news/2021/06/24/national/crime-legal/police-cybercrime-team
15. Maslow S. & O'Shea P. August 27, 2021, How Japan's Olympic success has been followed by COVID failure, https://theconversation.com/how-japans-olympic-success-has-been-followed-by-covid-failure-166204
16. NISC. n.d. "Police promotion system for cyber attack countermeasures", https://www.nisc.go.jp/conference/cs/ciip/dai03/pdf/03shiryou0206.pdf
17. NPA 2020a, Crime Situation in 2020, https://www.npa.go.jp/english/crime_situation_in_2020_en.pdf
18. NPA 2021, Cyber Forces, https://www.npa.go.jp/cyberpolice/english/action01_e.html
19. Tomohira Osaki, April 16, 2020, Japanese police warn that criminals are making most of the virus outbreak, https://www.japantimes.co.jp/news/2020/04/16/national/crime-legal/japan-police-crime-coronavirus
20. Trend Micro, August 18, 2021. Tokyo Olympics Leveraged in Cybercrime Attack, https://www.trendmicro.com/fr_fr/research/21/h/tokyo-olympics-leveraged-in-cybercrime-attack.html
21. Yoshioka, Katsunari. 2013. "PRACTICE - Proactive Response Against Cyber-Attacks Through International Collaborative Exchange." ieice.org, https://www.ieice.org/ken/paper/20130325JB2Y/eng
22. International Telecommunication Union, United Nations, (2017), https://www.itu.int/en/ITU-D/Regional-Presence/AsiaPacific/Documents/Events/2017/Sep SCEG2017/ SESSION-1_Lao_Ms_Kesone_Soulivong.pdf

23. DFDL, https://www.dfdl.com/resources/legal-and-tax-updates/lao-pdr-legal-alert-new-data-and-it-security standards-applicable-to-companies-are-you-compliant/
24. The Diplomat (03 June 2021), https://thediplomat.com/2021/06/laos-establishes-task-force-to-police-social-media-platforms/Global Initiative against Transnational Organized Crime, Policy Brief, (March 2020), https://globalinitiative.net/wp-content/uploads/2020/03/CovidPB1rev.04.04.v1.pdf
25. Save the Rhino Org, https://www.savetherhino.org/asia/china/coronavirus-and-rhino-horn
26. Dass, R. A. S. (2019). Crime Trends and Patterns in Malaysia. Kyoto Review of Southeast Asia, https://kyotoreview.org/trendsetters/crime-trends-and-patterns-in-malaysia
27. Cybersecurity in a COVID-19 World: The Future of Fighting Cybercrime for ASEAN and Australia. (2021). Cybersecurity in a COVID-19 World: The Future of Fighting Cybercrime for ASEAN and Australia
28. Rahman, R. (2019). CYBERCRIME CASES IN A DECADE: The Malaysian Experience
29. Sovereign, Will of the People, https://sovereignph.com/2021/02/15/pnp-claims-crime-volume-down-almost-50-in-january-2020/
30. Department of Interior and Local Government, https://dilg.gov.ph/news/DILG-Crime-down-by-4666-amid-COVID-19-pandemic-urges-leftists-and-critics-to-stop-spreading-fake-news/NC-2020-1318
31. Save the Children Foundation, https://www.savethechildren.org.ph/our-work/our-stories/story/online-sexual-abuse-of-children-rising-amid-covid-19-pandemic
32. International Justice Mission, https://osec.ijm.org/documents/16/IJM-Philippines-Child-Protection-Efforts-in-the-Time-of-COVID-19.pdf
33. Manila Bulletin, https://mb.com.ph/2021/08/13/police-presence-in-online-platforms-fighting-fake-news-preventing-scams
34. Criminal Code of Vietnam, https://www.dfdl.com/resources/legal-and-tax-updates/vietnam-legal-alert-new penal-code-enters-into-force
35. Abke, T. (2021, May 11). Vietnam reduces cybercrime with security initiatives. Indo-Pacific Defense Forum, https://ipdefenseforum.com/2021/05/vietnam-reduces-cybercrime-with-security-initiatives/
36. Campaign launched to detect loopholes on anti-COVID-19 tech platforms. (2021 October 6). Ministry of Information and Communications, https://english.mic.gov.vn/Pages/TinTuc/149079/Campaign-launched-to-detect-loopholes-on-anti-COVID-19-tech-platforms.html
37. Das, K. (2018, June 21). Vietnam Approves New Law on Cybersecurity, https://www.vietnam-briefing.com/news/vietnam-approves-new-law-cybersecurity.html
38. Fighting hi-tech crimes faces challenges | Sci-Tech | Vietnam+ (VietnamPlus). (2021 July 13). Vietnam Plus, https://en.vietnamplus.vn/fighting-hitech-crimes-faces-challenges/204561.vnp
39. Luong, H. (2019). Understanding Cybercrimes in Vietnam: From Leading-Point Provisions to Legislative System and Law Enforcement. International Journal of Cybercriminology, 13(2), 290-308. 10.5281/zenodo.3700724
40. Luong, H. T. (2021). Prevent and Combat Sexual Assault and Exploitation of Children on Cyberspace in Vietnam: Situations, Challenges, and Responses. In Combating the Exploitation of Children in Cyberspace: Emerging Research and Opportunities, IGI Global. 10.4018/978-1-7998-2360-5.ch004
41. Nghia, P. (2019 November 29). Vietnam introduces new information security system to facilitate e-governance. VnExpress International, https://e.vnexpress.net/news/news/vietnam-introduces-new-information-security-system-to-facilitate-e-governance-4019639.html
42. Nguyen, H. V. (2019 April). Cybercrime in Vietnam: A critical analysis of its regulatory framework. University of Portsmouth, https://pure.port.ac.uk/ws/portalfiles/portal/14426757/ 15.04.2019_Hai _new_submision_version.pdf
43. Over 3,100 cyber attacks hit Vietnam in six months. (2019 July 5) VietnamPlus, https://en.vietnamplus.vn/over-3100-cyber-attacks-hit-vietnam-in-six-months/155622.vnp
44. Over 5,100 cyber-attacks hit Vietnam in 2020 | Sci-Tech | Vietnam+ (VietnamPlus), (2021 January 1). Vietnam Plus,https://en.vietnamplus.vn/over-5100-cyberattacks-hit-vietnam-in-2020/194118.vnp
45. Vietnam hit by 2900 cyber attacks in first half of 2021. (2021). VNISA, https://vnisa.org.vn/en/vietnam-hit-by-2900-cyber-attacks-in-first-half-of-2021/

46. Vietnam: MIC announces statistics on cyber attacks for the first half of 2021. (2021 October 1). DataGuidance, https://www.dataguidance.com/news/vietnam-mic-announces-statistics-cyber-attacks-first
47. Sophisticated cybercrime on the rise in Việt Nam. (2018 August 14). Vietnam News, https://vietnamnews.vn/society/463726/sophisticated-cyber-crime-on-the-rise-in-viet-nam.html
48. Treutler, T. (2016, April 4). Legal Update: New Regulations In The ICT Sector In Vietnam. Conventus Law, https://www.conventuslaw.com/report/legal-update-new-regulations-in-the-ict-sector-in/
49. Vietnam: AIS addresses cyber attacks in Vietnam during 2021, (2021 October 7). DataGuidance,https://www.dataguidance.com/news/vietnam-ais-addresses-cyber-attacks-vietnam-during-2021
50. Vietnam faces risks from cyberspace: experts | Sci-Tech | Vietnam+ (VietnamPlus), (2020 September 11). Vietnam Plus, https://en.vietnamplus.vn/vietnam-faces-risks-from-cyberspace-experts/189030.vnp
51. https://www.europol.europa.eu/media-press/newsroom/news/beyond-pandemic-what-will-criminal-landscape-look-after-covid-19
52. www.covid19.gov.ph
53. wfh.gov.ph

6.2 Regional workshop on COVID-19-related cybercrime and electronic evidence in Asia

6.2.1 Agenda

Monday, 7 March 2022	
09h00	**Welcome and opening remarks** – Sri Lanka representative (TBC) – Ambassador Takeshi Akamatsu, Permanent Observer of Japan to the Council of Europe – Alexander Seger, Head of Cybercrime Division and Executive Secretary Cybercrime Convention Committee, Council of Europe Moderator – Jayantha Fernando, General Counsel, ICT Agency of Sri Lanka (ICTA), Director, Sri Lanka CERT
09h30	**Impact of COVID-19 on cybercrime and electronic evidence** – Cybercrime landscape in Asia – Challenges faced by the criminal justice authorities during the COVID-19 pandemic – *Simon Hirrle, Special Officer, Cybercrime Directorate, INTERPOL* – *Deepak Maheshwari, Hania El Helweh and Geronimo Sy, Council of Europe Experts* – *Sri Lanka National Police-Criminal Investigation Department representative (TBC)*
11h00	*Coffee break*
11h30	**Criminal justice responses to COVID-19 related cybercrime in Asia**

	Introduction of the study on COVID-19 related cybercrime in Asia – *Hania El Helweh, Deepak Maheshwari and Geronimo Sy, Council of Europe Experts* – *Interventions by participants*
13h00	*Lunch break*
14h30	**Domestic and international frameworks on cybercrime and e-evidence: their relevance for the COVID-19 pandemic** – International frameworks: Budapest Convention on Cybercrime and its Protocols *(Alexander Seger, Head of Cybercrime Division and Executive Secretary Cybercrime Convention Committee, Council of Europe)* – Country-study Philippines *(Geronimo Sy, Council of Europe Expert)* – *Philippines representatives* – *Interventions by participants*
	Summary of the first day
Tuesday, 8 March 2022	
09h00	**International cooperation on cybercrime and electronic evidence** – Challenges faced by criminal justice authorities – Mutual Legal Assistance and channels for cooperation – Cooperation with service providers – Data protection – *Hania El Helweh, Deepak Maheshwari and Geronimo Sy, Council of Europe Experts* – *Simon Hirrle, Special Officer, Cybercrime Directorate, INTERPOL* – *Alexandru Caciuloiu, Cybercrime and Cryptocurrency Advisor and Regional Coordinator for Southeast Asia and the Pacific, UNODC* – *Jayantha Fernando, General Counsel ICTA and* Director *of CERT, Sri Lanka* – *Interventions by participants*
10h45	*Coffee break*
11h15	**Enhanced cooperation and disclosure of electronic evidence** Introduction to the 2nd Additional Protocol to the Budapest Convention on Cybercrime – *Alexander Seger, Head of Cybercrime Division and Executive Secretary Cybercrime Convention Committee, Council of Europe* – *Interventions by participants*
13h00	*Lunch break*

14h30	**Capacity building on cybercrime and electronic evidence in response to the COVID-19 pandemic** – *Alexandru Caciuloiu, Cybercrime and Cryptocurrency Advisor and Regional Coordinator for Southeast Asia and the Pacific, UNODC* – *Martha Stickings, Programme Manager, Global Action on Cybercrime Extended (GLACY+), Council of Europe Cybercrime Programme Office* – *National initiatives*
16h15	**Summary of the second day**
Wednesday, 9 March 2022	
09h00	**Preparing criminal justice authorities to respond to future crises** Policies and strategies, cybercrime and e-evidence legislation, specialised units, interagency cooperation, LEA and judicial training, private-public partnerships and international cooperation – *Deepak Maheshwari, Hania El Helweh and Geronimo Sy, Council of Europe Experts* – *Simon Hirrle, Special Officer, Cybercrime Directorate, INTERPOL* – *Alexandru Caciuloiu, Cybercrime and Cryptocurrency Advisor and Regional Coordinator for Southeast Asia and the Pacific, UNODC* – *Interventions by participants*
11h00	*Coffee break*
11h30	**Proposals for further action and capacity building** Priorities and recommendations. National and international initiatives – *Hania El Helweh, Deepak Maheshwari and Geronimo Sy, Council of Europe Experts* – *Simon Hirrle, Special Officer, Cybercrime Directorate, INTERPOL* – *Alexandru Caciuloiu, Cybercrime and Cryptocurrency Advisor and Regional Coordinator for Southeast Asia and the Pacific, UNODC* – *Martha Stickings, Programme Manager, Global Action on Cybercrime Extended (GLACY+), Council of Europe Cybercrime Programme Office* – *Irina Drexler, Senior Project Officer, OCTOPUS Project, Council of Europe Cybercrime Programme Office* – *Interventions by countries*
13h00	**Closing session**

6.2.2 List of participants

Country	Name	Position
Laos	Vongvilai INTHASANH	Deputy Head of Division
Laos	Khonesavanh SOUVANNACHACK	Officer
Laos	Sounetto XAPHAKDY	Director of Division
Malaysia	Azleyna BINTI ARIFFIN	National Cyber Security Agency (NACSA)
Malaysia	Maizatul KHAIRANI BINTI MOHAMAD	National Cyber Security Agency (NACSA)
Malaysia	Navinthar GUNASEGRAN	Legal Advisor; Office of ICHIP Attorney-Advisor for Southeast Asia (Cybercrime) U.S Department of Justice-OPDAT U.S. Embassy Kuala Lumpur
Malaysia	Norsalimi BINTI SHALEH	National Cyber Security Agency (NACSA)
Malaysia	Parthiban KANDASAMY	Ministry of Foreign Affairs
Maldives	Ahmed NAUFAL	Public Prosecutor; Prosecutor General's Office
Maldives	Adam NAVEEDH	Sub Inspector of Police; Maldives Police Service
Maldives	Ye-Ting WOO	Office of Overseas Prosecutorial Development, Assistance and Training (OPDAT) U.S. Embassy for Sri Lanka and Maldives
Nepal	Krishna Jeevi GHIMIRE	Deputy Attorney General
Nepal	Samata SHARMA GELAL	Section Officer, Ministry of Law, Justice and Parliamentary Affairs
Philippines	Richel ABELIDA	Agent; NBI – Cybercrime Division
Philippines	Ferdinand LAVIN	Deputy Director and Spokesperson; National Bureau of Investigation
Philippines	Cezar II O. MANCAO	Executive Director; Cybercrime Investigation and Coordinating Center
Philippines	Alain Bert REGIS	Legal Officer, Investigation and Prosecution Group Office of the General Counsel and Legal Services
Sri Lanka	Jayantha FERNANDO	Director, Sri Lanka CERT & Director, Colombo Stock Exchange General Counsel, ICTA
Sri Lanka	Nirosha ANANDA	Chief Information Security Engineer; SL CERT
Sri Lanka	Samadhi SILVA	Information Security Engineer; SL CERT
Sri Lanka	Nelushie BANDARA	Information Security Engineer; SL CERT

Sri Lanka	Mr. JAYANETHSIRI	Assistant Superintendent of Police; Computer Crime Investigation Division – Criminal Investigation Department – Sri Lanka Police
Sri Lanka	Mrs. NADEEKA DISSANAYAKE	Women Inspector of Police; Computer Crime Investigation Division – Criminal Investigation Department – Sri Lanka Police
Sri Lanka	Mr. GAYASRI	Inspector of Police; Computer Crime Investigation Division – Criminal Investigation Department – Sri Lanka Police
Sri Lanka	Mr. SUBASINGHA	Sub-Inspector of Police; Computer Crime Investigation Division – Criminal Investigation Department – Sri Lanka Police
Sri Lanka	K. V. INDIKA	State Counsel; Attorney General's Department
Sri Lanka	Navodi DE SOYZA	State Counsel; Attorney General's Department
Sri Lanka	Printha KUNARATHNAM	State Counsel; Attorney General's Department
Sri Lanka	Haleema FAIZ	State Counsel; Attorney General's Department
Sri Lanka	Savini IDDAMALGODA	State Counsel; Attorney General's Department
Sri Lanka	Thushara SURAWEERA	Additional Secretary (Reforms); Ministry of Justice
Sri Lanka	Madushanka DISSANAYAKE	Director (Reforms); Ministry of Justice
Sri Lanka	Imali KOTALAWELA	Assistant Secretary (Legal); Ministry of Justice
USA	John GOLLOGLY	Advisor with International Criminal Investigative Training Assistance Program (ICITAP); US Embassy in Sri Lanka
USA	Deepamala JAYASINGHE	Legal Specialist; US Embassy in Sri Lanka
Lebanon	Hania EL HELWEH	Consultant/ Speaker
India	Deepak MAHESHWARI	Consultant/ Speaker
Philippines	Geronimo SY	Consultant/ Speaker
Singapore	Simon Sascha HIRRLE	Specialized Officer, CCCDP, Cybercrime Directorate, INTERPOL
Council of Europe	Alexander SEGER	Head of the Cybercrime Division
Council of Europe	Martha STICKINGS	Programme Manager, GLACY+, C-PROC
Council of Europe	Irina DREXLER	Senior Project Officer, Octopus Project, C-PROC
Council of Europe	Andrada ANTOFIE	Project Assistant, Octopus Project, C-PROC

6.2.3 Proposals made by participants

Below is a synthesis of proposals made by participants without attribution to countries making the proposal.

Capacity building and other support:

- To offer higher selection of trainings by several international organisations, with differentiation of the level of complexity of the trainings. Examples of the topics for which the training is sought by CSIRTS, law enforcement, judiciary, legal practitioners, but also financial and banking system to handle the complexity of cybercrime cases:
  - electronic evidence,
  - standard operating procedures,
  - digital forensics
  - human trafficking, smuggling (especially related to sexual exploitation),
  - online child sexual exploitation and abuse,
  - financial investigations (especially related to money laundering),
  - virtual currencies
- To improve accessibility of information about the capacity building support available to counties and institutions. For example, calendars of organisations providing capacity building support to be shared on a single online portal;
- Council of Europe to maintain a database of trained persons and continuously train the same officers to the extent possible, to update their skills.
- To support setting up of the necessary infrastructure to detect, investigate and prosecute cybercrime;
- To support development of skills and knowledge regarding Metaverse and in general on emerging technologies and potential threats;

Awareness raising:

- To consider bottom-up approach to awareness raising, as well as take into consideration country specifics;
- To extend awareness raising efforts to the general public;

Cooperation at all levels:

- To promote and support cooperation at national and internationals levels, including interagency and public/private cooperation;
- Enhancing cooperation between financial institutions (central bank, banking system) and criminal justice authorities (legislation enforcers, prosecutors, etc.), for example through meetings to discuss how to address cybercrime;
- To encourage big companies (such as Google etc.) to respond to requests from 'small' countries;

Strategic approach:

- To develop strategies on cybercrime, statistics;
- To consider development and implementation National Cybercrime Enforcement Plans;

Victims oriented approach:

- Focus on support to victims and their recovery and how officers are to cover sensitive cases. It can be assumed that if these cases are reported, it means they are serious/sensitive;

Other proposals:

- To maintain a centralized international criminals' database by law enforcement agencies;
- To develop annual cybercrime analysis/landscape report depicting positions and views of different stakeholders;

- To develop a manual for prosecutors and investigators on how to present cybercrime-related electronic evidence;
- To develop a platform that will facilitate easier reporting of crimes.