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

Version 7 August 2024

Regional workshop on cybercrime and electronic evidence in Southeast Asia

organised by the Office of the Attorney General of Thailand in cooperation with the Council of Europe
in the framework of Octopus Project[1]

Bangkok, Thailand [2-4 September 2024]

[Abridged] Outline

Background

Cybercrime is a complex and rapidly evolving transnational phenomenon that poses a significant threat to human rights, democracy and the rule of law as well as to national and international security. Moreover, with the increasing use of information and communication technologies, any type of crime may entail evidence on computer systems. Such electronic evidence is often stored in foreign, multiple, shifting or unknown jurisdictions; obtaining e-evidence poses major challenges to criminal justice authorities.

This is equally true for Southeast Asia[2], especially given high internet penetration rates in some countries of the region, such as Brunei, Malaysia, Singapore, Thailand[3]. The most common types of cybercrime threats in recent years included cyber scams (human trafficking-fueled fraud)[4], business e-mail compromise campaigns, phishing, ransomware, e-commerce data interception, crimeware-as-a-service, cryptojacking as well as online child sexual exploitation and abuse (OCSEA). The COVID-19 pandemic has additionally exacerbated these trends as shown in a regional study by the Council of Europe on COVID-19 related cybercrime in Asia[5].

[1] With the financial support of Japan
[2] See the 2021 ASEAN Cyberthreat assessment report / INTERPOL
[3] Brunei: 98%, Malaysia: 97%, Singapore: 91%, Thailand: 85%, Vietnam: 74%, Indonesia: 62%, Lao PDR: 62%, Cambodia: 60%, Philippines: 53%. Source: https://data.worldbank.org/indicator/IT.NET.USER.ZS
[4] INTERPOL operation reveals further insights into 'globalization' of cyber scam centres
[5] See the 2022 Regional Study on COVID-19 related cybercrime / CoE https://rm.coe.int/covid-19-cybercrime-asia-regional-study/1680a7112d

Governments all over the world have taken a range of measures to address the challenge of cybercrime and electronic evidence. Often this includes the adoption of legislation based on the Budapest Convention on Cybercrime and international cooperation mechanism under this treaty.

In Asia, Japan had been in the lead by participating in the negotiation of this Convention and by becoming in 2012, the first Party from Asia. Subsequently, the Philippines and Sri Lanka also joined this treaty. In Southeast Asia, a number of countries have adopted legislation largely in line with the Budapest Convention (Thailand, Singapore, Malaysia in addition to the Philippines)[6]. In some others, reforms are underway (Cambodia, Indonesia, etc). It is understood that more capacity building efforts are needed in Asia to strengthen the ability of countries to counter cybercrime and other crimes entailing electronic evidence on the basis of the Budapest Convention.

To this end, and following the conclusions of the Regional Conference on COVID-19 related cybercrime held in March 2022 in Sri Lanka, the Council of Europe – under the Octopus Project – is ready to support the Southeast Asian countries in strengthening their response to cybercrime and the challenges of electronic evidence.

The initiative begins with organizing a regional workshop aimed at fostering a deeper understanding of regional and domestic efforts, priorities, and challenges. As a framework for discussions, an initial high-level analysis of the current legislation on cybercrime and electronic evidence in Southeast Asia will be conducted, setting the foundation for coordinated efforts in the region.

Expected outcome of the conference

Following the regional workshop it is expected that:

- participants will have a better understanding of the benefits of international agreements and standards on cybercrime and electronic evidence as well as on online child sexual exploitation and abuse, and will have considered opportunities for accession to the Budapest Convention on Cybercrime and the Lanzarote Convention on Protection of Children against Sexual Exploitation and Sexual Abuse;

- priorities for capacity building on cybercrime and electronic evidence and OCSEA will have been identified;

- an analysis of current legislation and avenues for the further strengthening of domestic legislation on cybercrime and electronic evidence in selected countries of Southeast Asia will be available.

Participants

It is recommended that each of the eight participating countries in addition to Thailand (Brunei Darussalam, Cambodia, Indonesia, Laos, Malaysia, Philippines, Singapore, Vietnam) nominates up to 4 officials from relevant authorities (such as Ministries of Justice, prosecution services, law enforcement, policy makers or legislators).

[6] https://www.coe.int/en/web/octopus/country-wiki

Location and administrative arrangements

The conference will take place in-person in Bangkok, Thailand [Venue in downtown, TBC]. The working language of the workshop will be English.

Contacts

At the Council of Europe:

Nina LICHTNER
Programme Manager
Octopus Project
Cybercrime Division
Nina.LICHTNER@coe.int

Cristiana MITEA
Senior Project Officer
Octopus Project
Cristiana.MITEA@coe.int

In Thailand:

Puvadet PROMMAKRIT
Public Prosecutor
International Affairs Department
Office of the Attorney General of Thailand
puvadet.p@ago.mail.go.th

Agenda

DAY 1	
09h00-09h30	***Arrival and registration of participants***
09h30	**Welcome and opening remarks**
10h00	**Setting the scene: background and objectives of the programme** – Background and objectives of the programme, Virgil Spiridon, Council of Europe – Expectations from the programme [Tour de table]
11h00-11h30	***Coffee break and group picture***

11h30	**Threats and trends on cybercrime and e-evidence in Southeast Asia**
	
	Purpose: The purpose of this session is to enhance the understanding of current threats and trends of cybercrime and related challenges encountered in Southeast Asia. This will then serve as a basis for identifying responses to such challenges in subsequent sessions.
	
	– Cybercrime landscape in Southeast Asia
	– Challenges in addressing regional/national cybercrime threats and trends
	– Case studies:
	  – Cyberscams: human trafficking-fueled fraud
	  – Online child sexual exploitation and abuse
	
	Presentations followed by discussions with participants

13h00	***Lunch break***
14h00	**International legal frameworks on cybercrime and OCSEA** Purpose: The purpose of this session is to provide an overview of the frameworks of the Budapest Convention on Cybercrime and Lanzarote Convention on on Protection of Children against Sexual Exploitation and Sexual Abuse. This is to facilitate subsequent sessions on legislation and policies and on tools for cooperation. – Budapest Convention on Cybercrime and its Protocols – Lanzarote Convention and its practical implications – Case study on implementation of the Budapest Conventon *Presentations followed by discussions with participants*
14h45 15h45-16h00 Coffee break	**Legislation, policies and strategies on cybercrime and electronic evidence** Purpose: The purpose of this session is to learn about policies, legislation and other strategic aproach taken at domestic levels to address the challenges of cybercrime and electronic evidence. – Findings of the high-level regional analysis of legislation on cybercrime and electronic evidence – Case studies: Examples of application of legislation (substantive, procedural powers and international cooperation) for investigation and prosecution of cybercrime cases – Presentation of the key elements of the national strategies to fight against cybercrime

	– Strategic approach and good practices at domestic level: interventions by each of the participating States on legislative and other measures taken to address the challenges of cybercrime and e-evidence		
17h15	**Summary of the first day**		
17h30	**End of the first day**		
DAY 2			
09h00	**International cooperation on cybercrime and electronic evidence** Purpose: The purpose of this session is to provide a platform for dialogue to identify key challenges and good practices in the region in relation to international cooperation on cybercrime and electronic evidence. In particular, the session will aim to address what are the specific problems of international cooperation on cybercrime and e-evidence in Southeast Asia and how criminal justice authorities in Southeast Asia obtain evidence from other states. – Challenges faced by criminal justice authorities – Good practices and examples of successful cooperation in cybercrime cases – Tools and channels for international cooperation – 2nd Additional Protocol of the Budapest Convention on enhanced cooperation and disclosure of electronic evidence		
11h00-11h30	***Coffee break***		
11h30	**Public/private cooperation on cybercrime and electronic evidence** Purpose: The purpose of this session is to obtain a better understanding of the tools and opportunities for public/private cooperation in the region. Public/private partnerships are essential to counter cybercrime and obtain electronic evidence. – Public/private cooperation on cybercrime – what works and how can be improved – Available tools, initiatives and general principles for direct cooperation with service providers – How to prepare a successful data request – processes, challenges and clarifications		
13h00-14h00	***Lunch break***		
14h00-17h00	**Bilateral sessions and networking** Purpose: The purpose of the bilateral sessions is to provide an opportunity for detailed discussions of the Council of Europe representatives with countries on findings on domestic legislation, and identify areas for further cooperation. It will also permit delegations to meet bilaterally for networking and discussing matters of mutual interest.		**Workshops on OCSEA** Purpose: Two consecutive workshops will offer insights from the Lanzarote Committee perspective into case studies on OCSEA
14h00 - 14h45 14h45 - 15h30 15h30 - 16h15 16h15 - 17h00	– Session with Thailand – Session with Singapore – Session with Indonesia – Session with Brunei	– Session with Malaysia – Session with Laos – Session with Vietnam – Session with Cambodia	[14:00-15:00] Grooming, online exploitation, and CSAM [16:00-17:00] Exploitation of children through live streaming and coercion

17h15	**Summary of the second day**
17h30	**End of the second day**
DAY 3	
09h00	**Relevant international and regional initiatives on cybercrime and electronic evidence for Southeast Asia** Purpose: The purpose of this is to facilitate coordination between different cooperation initiatives and agreements and to permit participants to make better use of the opportunities that they provide. Panel discussion followed by open dialogue with participants
10h30	*Coffee break*
10h45	**Capacity building as enabler for effective criminal justice response on cybercrime and electronic evidence** – Law enforcement training strategies and practices – Judicial training strategies and practices – Integrating gender in cybercrime capacity-building activities – Priorities and recommendations for the region [interventions by countries] Panel discussion followed by open dialogue with participants
12h30	**Closing session**
13h00	**End of the Conference**
13h00-14h30	**Farewell lunch / reception**