Discussion Guide

for the Substantive Topics of the 2nd ACCPCJ

TOPIC 1

Promoting Prevention through a Culture of Good Governance and Respect

Rationale

In line with the ASEAN Vision 2025 and the 2030 Agenda for Sustainable Development (SDGs), the adoption of the ASEAN Declaration on Culture of Prevention (CoP) for a Peaceful, Inclusive, Resilient, Healthy and Harmonious Society in 2017 has created a paradigm shift in people mindset towards upstream measures in addressing challenges to sustainable social and human development. Given that the root causes of problems require more inclusive and preventive strategies, ASEAN needs to institutionalise a culture of good governance as a basis to promote responsible citizenship and equitable socio-economic development that enable people access to justice, quality education and employment, healthcare, which are key elements for peace and development.

Objectives and Scope

The topic will focus on the role of formal and informal institutions in promoting the culture of prevention, and in responding to cybercrime. This may cover:

- Public awareness of cybercrime threats, behaviours of cyber attackers and how online criminal groups operate and interact with victims
- Guidelines for the private platform operators to inform its users of protection policies against abuses and attacks and how the private providers could cooperate with government institutions
- Online reporting and referral mechanisms for complaints on cyber-related crime which are user-friendly and easily accessible for the victims, general public, and private service providers
- Development of database and statistical information system to keep track of records and monitor incidences

TOPIC 1

Promoting Prevention through a Culture of Good Governance and Respect

Questions for discussion

- What is the role of formal and non-formal education in engaging and empowering youth to promote the culture of prevention?
- What measures can be ta en by relevant institutions to educate people on cybercrime, particularly among the young and elderly of the population?
- What are approaches and practices to promote people awareness on cybercrime?

TOPIC 2

International Cooperation in Criminal Matters

Rationale

Cyber criminals operate in cyberspace which cuts across jurisdictions. Most often the perpetrators act anonymously from unknown or remote location beyond the physical reach of justice authorities which have the jurisdiction powers, and take advantage of the disparities in the law enforcement between countries. It is noteworthy that Southeast Asia has witnessed the boom of internet economy in the past decade with 360 million users now connected to the internet market of $100 billion in value.[1] This unprecedented level of online penetration signifies that not only public agencies and major industries are exposed to cybercrime threats but also the masses of ASEAN citizens including the most vulnerable groups such as children.

In recognition of the harmful effects of cybercrime on societies, ASEAN Member States have endorsed the ASEAN Declaration to Prevent and Combat Cybercrime in 2017 and resolved to strengthen international cooperation including but not limited to technical expertise to tackle cybercrimes. However, gaps remain in the area of cooperation in criminal matters which must also be effectively addressed to ensure those involved are brought to justice and the victims are given legal protection and remedies.

Objectives and Scope

This session will discuss the development of ASEAN legal framework and cooperation in law and justice among the ASEAN Member States as part of the regional efforts to prevent and combat cybercrime. The scope of the discussion may cover:

- Application of Mutual Legal Assistance in cybercrime-related offences
- Facilitation of cross-border access to electronic evidence
- Regional cooperation on the access to justice and protection of cybercrime victims

[1] *https://www.bain.com/globalassets/noindex/2019/google_temasek_bain_e_conomy_sea_2019_report.pdf*

TOPIC 2

International Cooperation in Criminal Matters

- Recommendations on the legal framework and harmonization of regulatory rules related to cybercrime in ASEAN in consultation with the relevant ASEAN sectoral bodies
- Multilateral and bilateral cooperation, with possible reference to models in international treaties

Questions for discussion

- What are some of the recent examples of cybercrime-related offences which draw attention to the need for strengthening of ASEAN legal cooperation?
- Does the diversity of national approaches to the criminalization of cybercrime offences have an impact on the scope of international cooperation?
- To what extent Mutual Legal Assistance could provide a useful basis for international cooperation against cybercrime? Should there be a common guideline for this?
- How have the ASEAN Member States applied the existing ASEAN instruments such as The Treaty on Mutual Legal Assistance in Criminal Matters among like-minded ASEAN Member Countries and the ASEAN Extradition Treaty and the relevant provisions in relation to cybercrime? What more is needed to support the actual implementation of such instruments?
- Do different types of cybercrime require the same approach to cooperation and specific measures? For example, cyber-dependent crime including attacks on data and infrastructure; content-related offences as in the case of online child sexual exploitation, and; cyber-enabled offences which are online criminal activities such as online frauds, human trafficking, and terrorism may be addressed differently?
- How could different ASEAN Sectoral Bodies contribute to the development of ASEAN legal framework and the strengthening of ASEAN cooperation in criminal matters?

TOPIC 3

Building Capacity through Partnership

Rationale

As reflected in the ASEAN Declaration on Culture of Prevention for a Peaceful, Inclusive, Resilient, Healthy and Harmonious Society, and ASEAN Declaration to Prevent and Combat Cybercrime, both documents prominently recognized the importance of capacity building as a necessary tool to combat challenges facing national and international resiliency. As vulnerabilities in one country create risks for others, Member States need to build up their skills and knowledge as well as to partner with every sectors in society to stay ahead of crime. However, the main challenges in enhancing cyberspace in ASEAN are the knowledge, skills and public awareness of cybercrime. This therefore constitutes the increasing needs for Member States to fostering their cooperation on crime prevention, i.e. specialized training for law enforcement and criminal justice officials.

Objectives and Scope

The topic aims to steer the discussion on how to strengthen partnership to effectively address cybercrimes. This may cover:

- Exchange of best practices on fighting cybercrime in the region
- Examples of the provision of technical assistance for enhancing cybercrime response between ASEAN Member States, and beyond
- Ongoing funding programmes and activities to build capacity on cybercrime
- Explore possible areas of future capacity building activities

TOPIC 3

Building Capacity through Partnership

Questions for discussion

- What are some of the obstacles and challenges in promoting cybercrime capacity building for criminal justice professionals in the region?
- How to leverage the advancement of information and communication technologies available to relevant stakeholders and to have the latest data for managing cyber threats.
- In what way can public-private partnership help to address cybercrime?
- What are the technical assistance needs and priorities of the region to strengthen regional cooperation in cybercrime?
- What approaches should be considered to support Member States in establishing or updating national policies and laws on cybercrime?
- How Member States better identify and address gaps in national legal and institutional frameworks in responding to cybercrime?
- What mechanisms can be developed to promote a more coordinated law enforcement in the region?

TOPIC 4

Promoting Prevention through a Culture of Peace and Moderation

Rationale

With the advancement of technology information and communication that provides more accessible online platforms and nontraditional channels for people at large to reflect their thoughts freely, cyberspace has often become a fertile ground for cultivating violence, radicalization, and dispute, potentially leading to greater social disparity. Additionally, it enables cyber threats to multiply in scope, magnitude, and forms, which substantially impact the confidentiality, integrity, and availability of data.

Objectives and Scope

The topic will discuss issues related to the promotion of literacy in all aspects and at all levels to prevent deliberate falsehoods and radicalization among others. This may cover:

- Challenges in enhancing cyberspace in ASEAN in promoting the inclusive society and respect for all
- The role of Confidence Building Measures (CBMs) among all stakeholders, ranging from government agencies, private sectors, regional and international organizations, to media
- The role of stakeholders across sectors to promote values-based education

Questions for discussion

- How to enhance public-private partnership to promote cyber wellness in ASEAN?
- How ASEAN Member States respond to harmful content such as hate speech or fake news that spread-out through internet while guaranteeing respect for freedom of expression?
- To what extent youth and young generation promote a culture of respect, and media literacy to fight against cyber bullying?

TOPIC 5

National legislative Framework

Rationale

Cybercrime is rapidly evolving in forms, modus operandi, and sophistication. National legislative framework should be reviewed to keep pace with cybercrime trends to ensure effective prevention and law enforcement. Cyber attackers have moved on to target not only against user data but increasingly aiming for operating and information systems. Mobile platforms now account for over 60 per cent of online frauds. In addition, rising connectivity has allowed criminals to migrate their traditional criminal activities into cyberspace and this has led to the expansion of online criminal markets and cyber-facilitated crimes. Development of the relevant national legislative framework or law reform should consider the dynamics of cybercrime and the related criminal offences, its transnational nature, and including the rule of law and human rights.

Objectives and Scope

The scope of the discussion may cover

- Criminalization of cybercrime and cyber-related offences
- Substantial and procedural laws that have been or would be enacted Legal provisions on jurisdiction over cybercrime
- Access to justice for cybercrime victims and available remedies
- Protection of human rights and data privacy
- National legal framework for the gathering of electronic evidence, cyber forensics, evidentiary rules and its admissibility in court
- Harmonization of laws on cybercrime in line with international and regional legal framework
- Surveying of relevant national legislative framework of the ASEAN Member States

[2] *https://www.weforum.org/agenda/2019/03/here-are-the-biggest-cybercrime-trends-of-2019/*

TOPIC 5

National legislative Framework

Questions for discussion

- To what extent should criminal justice responses to cybercrime be updated or improved?
- How do we balance between protection of data privacy, human rights, business interests, and criminal investigation?
- How do we safeguard against extensive application of discretion and illegitimate use of procedural powers which may be harmful to human rights, business interests and consumer trust in a digital economy?
- What are the loopholes in the existing national legal framework that should be addressed?
- What are the legal tools that support preventive measures against cybercrime which is constantly evolving and becoming more complex?
- What are good practices in cybercrime-related criminal investigation, prosecution, collection of evidence, and use of digital evidence in court that could be shared?

TOPIC 6

Opportunities and Challenges of Industry 4.0

Rationale

Increased access to cyberspace and internet users mean that growing number of people and businesses are being exposed to cybercrime risks. While governments and businesses have limited capabilities and resources to deal with cybercrime, we have witnessed in recent years the exponential growth of data in cyberspace and rising cyber-related incidences internationally. This underlines the need for investment in technology and technical assistance to help guard against attacks and online criminal activities. These may include, for instance, improvement in cybersecurity, identification of risks and vulnerabilities and digital evidence analytics.

Objectives and Scope

This topic will focus on the new developments of technology and innovation and how these could be used to prevent and combat cybercrime. The scope of this session may cover:

- Impact of increased access to cyberspace, internet of things, cloud system, and business platform model on cybercrime threats
- Why technology and innovation can have important role in dealing with cybercrime, for example, by speeding up response and saving costs
- Improvements in cybersecurity protection and recent investments by governments and private industries to protect its system, data and consumers
- Innovative technological solutions to prevent and combat cybercrime such as data monitoring, detection, and reporting by machine learning and artificial intelligence
- International and public-private cooperation on technological investments and using of innovative tools against cybercrime such as simulation of incidences

TOPIC 6

Opportunities and Challenges of Industry 4.0

Questions for discussion

- Which aspects of cybercrime-related measures and strategies have high priority for technical assistance and capacity-building, in particular in view of the evolving nature of cybercrime and the new and emerging threats associated with it?
- What are the key drivers and actors needed for technological cooperation and technical assistance?
- To what extent has the private industry been able to constructively engage with the governments in developing formal and informal cooperation on exchange of expertise, information, and development of the necessary regulatory framework?