Department of Justice
Office of Cybercrime

Funded by the European Union and the Council of Europe

EUROPEAN UNION

COUNCIL OF EUROPE
CONSEIL DE L'EUROPE

Implemented by the Council of Europe

Version 29 June 2017

REGIONAL CONFERENCE ON CYBERCRIME 2017

Enhancing regional and international cooperation
to improve the rule of law in cyberspace

27 – 29 June 2017
Cebu City, Philippines

organised by the Philippine Department of Justice
in cooperation with the Council of Europe under the GLACY+ joint project with the European Union

Conference summary

More than 60 representatives of governments and judiciary of Cambodia, Indonesia, Japan, Myanmar, Philippines, Singapore, Sri Lanka, Thailand, and USA, private sector experts from F-Secure, ICANN, Microsoft and Trend Micro, representatives of international organisations, such as the Council of Europe, European Union [European Commission and EUROPOL], INTERPOL, UNICEF and the UNODC as well as from civil society organisations like the International Centre for Missing and Exploited Children (ICMEC), International Justice Mission (IJM) and ABSCBN BantayBata 163 participated in the Regional Conference on Cybercrime 2017.

Key take-aways include:

- Cybercrime and issues related to electronic evidence undermine the social and economic development opportunities of information technologies as well as human rights, democracy and the rule of law. A more effective criminal justice response is needed.

- Legislation on cybercrime and electronic evidence is the basis for such a response. Good practices are available as some countries in the ASEAN region have already adopted consistent legislation in line with the international standards provided for by the Budapest Convention, while others are in the process of preparing legislation. It is noted that the Council of Europe under the GLACY+ project is ready to support countries the region in this process upon request.

- Data protection legislation should be considered to promote trust and to provide a clearer framework for public/private and international data sharing. Like the Budapest Convention, the Data Protection Convention 108 of the Council of Europe is open for accession by any country.

- As electronic evidence is increasingly stored on servers in the cloud, specific measures are needed to secure such evidence for criminal justice purposes. The work of the Cybercrime Convention Committee within the framework of the Budapest Convention is noted, including the recent decision to commence the negotiation of a Protocol on access to evidence in the cloud. It is also noted that private sector entities are prepared to cooperate with public authorities. Governments may consider:

- providing for domestic production orders in line with Article 18, Budapest Convention and the respective Guidance Note on the production of subscriber information recently adopted by the Cybercrime Convention Committee;
- to engage in a dialogue with multi-national service providers regarding the disclosure of subscriber information;
- to follow the work of the Cybercrime Convention Committee on a Protocol to the Budapest Convention and accession to this treaty.

- Electronic evidence is potentially part of any offence. Good practices to secure and analyse electronic evidence are available, should be shared and be used. Digital investigations are a collaborative effort of investigators, forensic investigators and prosecutors.

- A major capacity building effort is needed at all levels given that cybercrime and electronic evidence touch upon all areas of crime and core values of society. Sustainable, scalable and replicable training programmes are needed for law enforcement, prosecution services and the judiciary. Good practices are available in the ASEAN and the Asia/Pacific region, including through South-South cooperation. It is noted that the Council of Europe and the European Union through joint projects such as GLACY+, the Government of Japan, and UNODC are prepared to provide assistance. Governments should define their needs and expectations more clearly and donor organisations should improve their coordination with each other.

- The online sexual exploitation and abuse of children remains a major threat. Comprehensive approaches are required, including:
  - education and other preventive measures;
  - an effective criminal justice response based on clear legislation as well as investigation, prosecution and adjudication, and international cooperation;
  - measures to protect child victims and witnesses in criminal proceedings such as those provided in the UN Convention on the Rights of the Child and the Lanzarote Convention of the Council of Europe on the Protection of Children against Sexual Exploitation and Abuse;
  - cooperation between law enforcement, industry (including the financial sector) and civil society in view of prevention, protection and prosecution;

- As cybercrimes are aimed at generating profit, "follow the money" approaches should be considered. Close cooperation between cybercrime units, financial investigation and intelligence units and the financial sector should be promoted. Cybercrime investigations should be accompanied by financial investigations and vice versa.

In terms of the way ahead, ASEAN member states should:

- Adopt appropriate domestic legal frameworks that will tackle cybercrime and other cyber-related offenses, including electronic evidence regimes, in line with international standards such as the Budapest Convention;

- Harmonize national laws in order to address the cross-border nature of cybercrimes and electronic evidence and facilitate international cooperation;

- Continue to build capacities and skills of law enforcement agencies, prosecution services, and judiciary;

- Strengthen cooperation with the private sector that will enable timely access to data;
- Streamline procedures involved in the processing of mutual legal assistance requests.

Participants expressed their appreciation of the way the conference was organised and of the quality of the interventions by speakers.

A judicial conference between Judicial Training Institutions of countries in the ASEAN region is tentatively set in September 2017, to discuss training strategies and integration of cybercrime and electronic evidence modules in their respective curriculum.