MAKING INTERNATIONAL COOPERATION WORK

ATTY. MARKK L. PERETE
Undersecretary
Department of Justice
Philippines

Outline

- Legal Framework
- Case Study
- Challenges
- Recommendations
- Conclusion

Budapest Convention on Cybercrime

- Acceded to by 65 parties globally.
- First and only international treaty that deals with cybercrime and electronic evidence.
- Provided legal framework on cybercrime to nearly half of the UN Member-States.
- Philippines became the first country in the ASEAN region to accede to the convention in 2018.

In the Philippines, the Budapest Convention paved the way for:

- The enactment of its domestic law on cybercrime – Republic Act No. 10175 or the Cybercrime Prevention Act of 2012.

- The designation of its Justice Department (DOJ) as the Central Authority and of the Office of Cybercrime, within the DOJ, as the 24/7 Point-of-Contact pursuant to the Convention.

In the Philippines, the Budapest Convention paved the way for:

- Greater cooperation with 64 other members of the convention on matters of legal and other forms of assistance.
- Participation in the further negotiations of the convention to ensure that it will be consistent with its laws, rules, and regulations.

Scope of the Budapest Convention

Criminalising conduct

- Illegal access
- Illegal interception
- Data interference
- System interference
- Misuse of devices
- Fraud and forgery
- Child pornography
- IPR-offences

+

Procedural tools

- Expedited preservation
- Search and seizure
- Production order
- Interception of computer data

+

International cooperation

- Extradition
- MLA
- Spontaneous information
- Expedited preservation
- MLA for accessing computer data
- MLA for interception
- 24/7 points of contact

Harmonisation

Proposed Provisions of 2nd Protocol to the Convention

- Language of requests
- Emergency MLA
- Video Conferencing
- Direct disclosure of subscriber information
- Giving effect to orders from another Party for expedited production of data

3 General Principles of International Cooperation

1. Provided to the widest extent possible;
2. Applicable to all cybercrimes and crimes entailing the collection of electronic evidence; and
3. In accordance with the: (a) tenor of the Convention; (b) relevant international agreements on international cooperation in criminal matters; (c) reciprocal arrangements; and (4) domestic laws.

LEGAL REQUEST LANDSCAPE IN THE PHILIPPINES

2018	2019	2020
• Total of **eight (8)** requests.	• Total of **three (3)** Requests	• Total of **three (4)** Requests
➢ In all these requests, PH is the Requesting State. ➢ Nature of cases: hazing, sextortion, libel, inciting to sedition and copyright infringement. ➢ Basis of the request: MLAT on Criminal Matters with the US. ➢ Two (2) MLARs were pursued with India and UAE on the basis of reciprocity.	➢ In all these requests, PH is the Requesting State. ➢ Nature of cases: cyber libel; computer-related identity theft; and murder. ➢ Basis of the request: MLAT on Criminal Matters with the US.	➢ In all these requests, PH is the Requested State. (Requesting State is Switzerland). ➢ Nature of the crime: Illegal Access and Computer-related Fraud. ➢ Request for assistance in the preservation of data under Articles 29 and 30 of the Budapest Convention.

Case Study

Basis: Data Preservation under Articles 29 and 30 of the Budapest Convention

Crimes: Illegal Access and Computer-related Fraud

Facts: In May 2020, the PH received a request from the Switzerland for preservation of all computer data relating to IP addresses used by an unknown subject to manipulate a Swiss airline booking system by intercepting messages between the airline's booking system and its payment processor. Four (4) ISPs were identified to be located in the Philippines, where only one (1) was able to preserve the data.

Case Study

Challenges: ISPs in the PH are constrained to use Carrier Grade Network Address Translation (CGNAT) technologies. Thus, technical limitations exist as to their capacity to preserve and disclose computer data that are crucial in cybercrime investigations.

Another challenge noted is the inability of requesting states to coordinate directly with the foreign ISPs when it comes to preservation of computer data. Thus, added level and procedure are undertaken that result in delay in the processing of the request.

The Main Problem

Electronic evidence gathering is difficult and time-consuming. It can be anywhere. Thus, the need for efficient and swift mechanisms in collecting electronic evidence.

versus

The need to respect other States' sovereignty and for complying with international conventions.

Challenges

1. Gaps in domestic legislation that result in apparent conflict of law.

2. Inefficiency of mutual legal assistance request procedures.

3. Willingness/capacity of the service providers to cooperate.

Recommendations

1. Harmonize national legislations (*i.e., utilize the Budapest Convention on Cybercrime as your legal framework*)

2. Adopt mechanisms that provide lenient requirements for facilitating international cooperation (*e.g., 2nd Protocol to the Convention on Direct Cooperation and Giving Effect to Orders from another Party for Expedited Production of Data, among others*)

3. Implement clear regulations for service providers to ensure their cooperation in cybercrime and cyber-related investigations.

Conclusion

Increased, **rapid** and **well-functioning international cooperation** between parties of the Convention and between States and private industry, which the **Budapest Convention provides**, is crucial in combatting cybercrimes.

THANK YOU!

mlpdocus@gmail.com
Department of Justice
Padre Faura Street
Manila, Philippines