

Mutual legal assistance in responding to cybercrime: the international framework and the national needs in ASEAN member states

Matti Joutsen
Special Advisor, Thailand Institute of Justice

Second ASEAN Conference on Crime Prevention and Criminal Justice
Bangkok, 27-28 February 2020

Strengthening the ASEAN response to cybercrime: What is needed for better mutual legal assistance?

- a **shared legal framework** for working together: international instruments
- **national substantive criminal law** based on the shared framework (approximation / harmonization of core offences)
- **national law enforcement and procedural provisions** based on the shared framework
- **training and resources** (technical assistance)
- **cooperation with the private sector** and key stakeholders

Existing regional instruments related to cybercrime

examples from other regions:

- **Commonwealth of Independent States** Agreement on Cooperation in Combating Offences Related to Computer Information of 2001
- **Arab League** Convention on Combating Information Technology Offences of 2010
- **Shanghai Cooperation Organization** Agreement on Cooperation in the Field of International Information Security of 2010
- **African Union** Convention on Cybersecurity and Personal Data Retention of 2014
- **Southern African Development Community (SADC)** Model Law on Computer Crime and Cybercrime of 2012
- **Economic Community of West African States (ECOWAS)** Directive on Fighting Cybercrime of 2011

Existing regional instruments related to cybercrime (continued)

examples from European Union instruments:

- 2000 **Electronic Commerce** Directive (creates internal market framework for online services to provide business and consumers with legal certainty)
- 2006 Directive on **Data Retention** (obligation of service providers to retain data that has been generated or processed)
- 2011 Directive on **combating the sexual exploitation of children online** and child pornography
- 2013 EC Directive on **attacks against information systems**
- 2019 EC Directive on **non-cash means of payment** (enhanced law enforcement cooperation against fraud and counterfeiting)
- under preparation: proposed Regulation and Directive facilitating **cross-border access to electronic evidence for criminal investigations**

International and regional instruments related to cybercrime (open also to ASEAN member states):

- **United Nations** Convention against Transnational Organized Crime of 2000
 - ratified by all ASEAN member states
- **Council of Europe** Convention on Cybercrime of 2001
 - not limited to CoE members; ratified by e.g. the Philippines 2018
 - 2003 protocol on criminalisation of acts of a racist or xenophobic nature committed through computer systems
 - current work on protocol on the sharing of cross-border electronic evidence in criminal investigations

proposed UN Convention on countering the use of information and communication technologies for criminal purposes

- General Assembly resolution adopted on 27 December 2019 (79 votes for, 60 against, 33 abstentions)
- three-day organizational session in New York in August 2020
- actual negotiations expected to begin in 2021
- **divisive issue** within the UN Crime Programme:
 - should focus be on proposed new global convention, or on more effective implementation of existing instruments?
 - state sovereignty and non-interference vs borderless cyberspace
 - unclear how to define “use of information and communications technologies for criminal purposes” (human rights concerns)

national provisions on substantive criminal law

based on the shared framework (approximation / harmonization of core offences)

- **offences specific to the Internet**, such as attacks against information systems or phishing
- **computer-related** offences, such as fraud, and criminal misuse and falsification of identity
- **illegal online content**
 - regarding criminalization of content, general agreement in respect of
 - racism and xenophobia,
 - incitement to terrorist acts, and
 - abuse and sexual exploitation of children,
 - but what of promotion of different religious or political views?

national provisions on law enforcement and procedure

- (UNTOC provides a partial basis; all ASEAN member states are parties)
- **investigation of cybercrime**
 - expedited order for preservation of stored computer data
 - “production order” for specified stored information or subscriber information
 - search and seizure of stored computer data
 - real-time collection of computer data (traffic data and content data)
- **electronic evidence**
 - data retention obligation among service providers
 - general provisions on the preservation and integrity of data
 - provisions on admissibility of electronic evidence in court
- **jurisdictional issues**
 - the “elephant in the room”: **cross-border access to computer data!**

training and resources (technical assistance!)

- investigators (new criminalizations; cybercrime investigations; electronic evidence)
 - need for appropriately staffed, trained, organized and funded 24/7 specialist units
 - for MLA purposes, establishment of national contact points that are available 24/7
- prosecutors (new criminalizations; electronic evidence; requesting of MLA)
- defence counsel (new criminalizations; electronic evidence)
- judges (new criminalizations; electronic evidence)

cooperation with the private sector and other stakeholders

examples:

- **cybercrime prevention**: responsibility of technology companies (encryption?), service providers, companies in general, individual users and consumers
- **regulations on e-commerce and non-cash payments**
- **reporting obligation** of companies in event of cybercrime breach?
- **data retention** obligation of service providers
- **assistance to victims**

challenges in responding to cybercrime in ASEAN member states

- reluctance to exchange information (e.g., no regional database)
- at times, lack of trust and uneven willingness to cooperate
- uneven law enforcement capacity
- lack of an interagency approach
- insufficient joint investigations
- language difficulties
- differences in legal frameworks
- competing national interests, principle of non-interference
- time-consuming national bureaucracy
- lack of money

To return to the first point: What does ASEAN need for better MLA?

- a **shared legal framework** , which can be provided by existing or future international instruments, including through ASEAN action
- approximated / harmonized **national substantive criminal law**
- approximated / harmonized **national provisions on law enforcement and procedure**
- **training and resources**
- **cooperation with the private sector** and key stakeholders

... but above all

- a **shared vision** of what the ASEAN priorities are, based on mutual trust
- and the **political will** to take that shared vision forward