GLACY+
Global Action on Cybercrime Extended

REGIONAL CONFERENCE ON CYBERCRIME 2017
27 – 29 June 2017, Cebu City, Philippines
Organised by the Philippine Department of Justice
in cooperation with the Council of Europe under the GLACY+ project

Cybercrime and the rule of law in cyberspace: How to secure electronic evidence in the cloud?

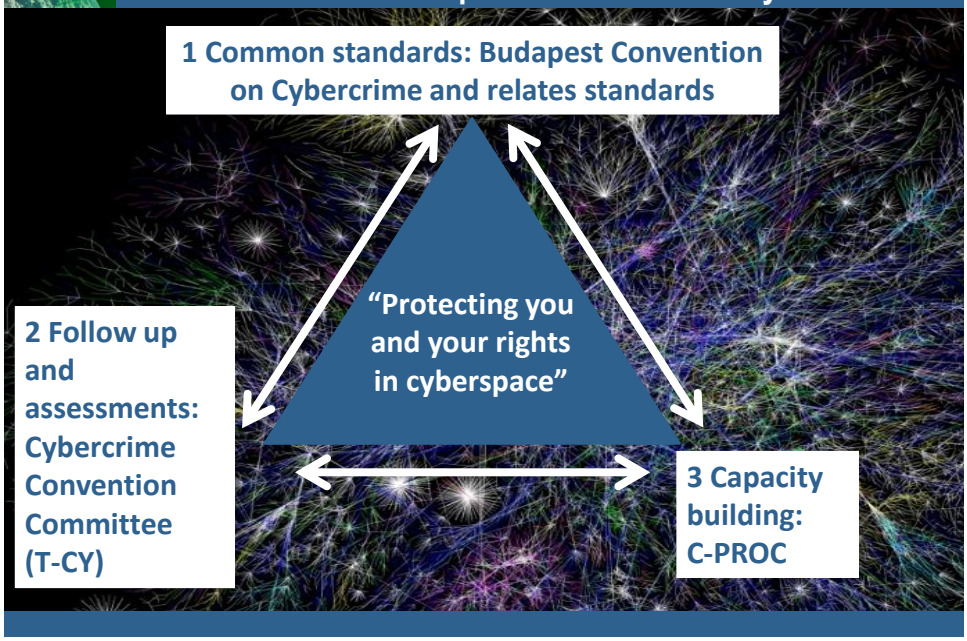
Alexander Seger
Council of Europe
alexander.seger@coe.int

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

www.coe.int/cybercrime

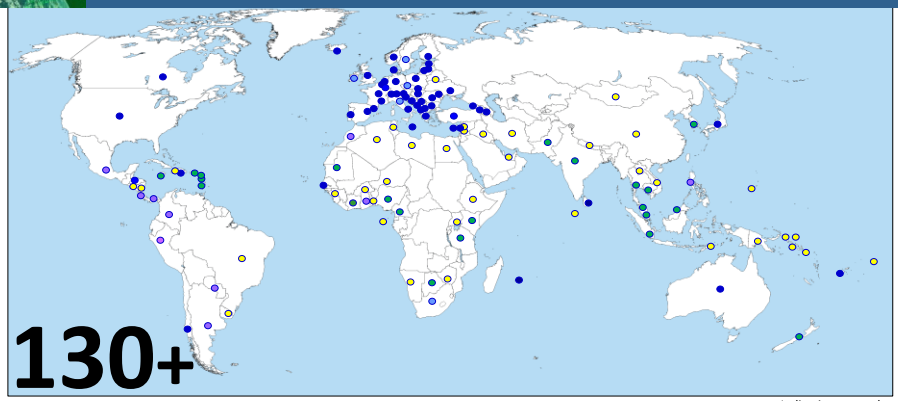
1

Strengthening the rule of law in cyberspace: The framework of the Budapest Convention on Cybercrime



2

Reach of the Budapest Convention and capacity building



Indicative map only

Ratified/acceded: 55

+ Signed: 5

+ Invited to accede: 8

= 68

Other States with laws/draft laws largely in line with Budapest Convention = 20+

Further States drawing on Budapest Convention for legislation = 45+

3

Adopt legislation in line with 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
- Production orders
- Search and seizure
- Interception of computer data
- + Safeguards!

+

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

Harmonisation

4

Benefits of Budapest Convention

- ✓ Coherent legal framework that meets rule of law requirements
- ✓ Trusted and efficient cooperation with other Parties
- ✓ Participation in the Cybercrime Convention Committee (T-CY)
- ✓ Participation in future standard setting (Guidance Notes, Protocols and other additions to Budapest Convention)
- ✓ Enhanced trust by private sector
- ✓ Capacity building

"Cost": Commitment to cooperate

Disadvantages?

5

Cybercrime and electronic evidence: challenges

Offences against and by means of computers (Cybercrime)

- ► Attacks against core values of democratic societies

+

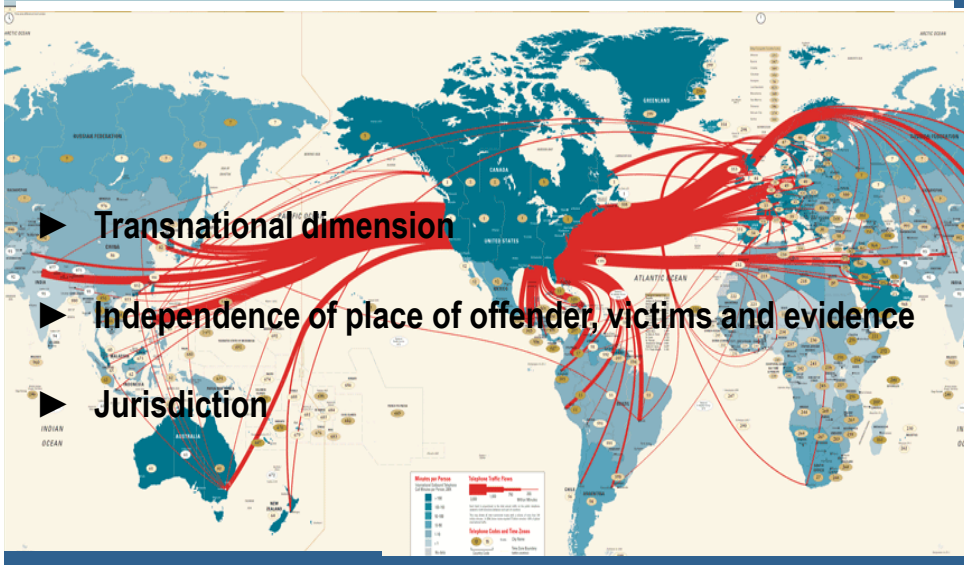
Evidence in relation to any crime stored on computer systems or storage devices

- ► Often "somewhere" in the cloud)

6

7

Where is the evidence in cyberspace?



- Transnational dimension
- Independence of place of offender, victims and evidence
- Jurisdiction

8

Cybercrime and electronic evidence: Challenges for criminal justice

- The scale and quantity of cybercrime, devices, users and victims
- Technical challenges (VPN, anonymisers, encryption, VOIP, NATs etc.)
- Cloud computing, territoriality and jurisdiction
  - Cloud computing: distributed systems ▶ distributed data ▶ distributed evidence
  - Unclear where data is stored and/or which legal regime applies
  - Service provider under different layers of jurisdiction
  - Unclear which provider for which services controls which data
  - Is data stored or in transit ▶ production orders, search/seizure or interception?
- The challenge of mutual legal assistance
- No data ▶ no evidence ▶ no justice

9

Crime and jurisdiction in cyberspace ▶ solutions proposed under the Budapest Convention on Cybercrime

Issues:

- Differentiating subscriber versus traffic versus content data
- Limited effectiveness of MLA
- Loss of location and transborder access jungle
- Provider present or offering a service in the territory of a Party
- Voluntary disclosure by US-providers
- Emergency procedures
- Data protection

Solutions:

1. More efficient MLA
2. Guidance Note on Article 18
3. Domestic rules on production orders (Article 18)
4. Cooperation with providers: practical measures
5. Protocol to Budapest Convention

10

Discussion: Production orders

For discussion

- What are the rules and procedures in ASEAN countries to order a service provider (or another (legal) person to produce:
  - Subscriber information
  - Traffic data
  - Content data
- Who can issue an order?
- What are the conditions?
- How do you obtain data from a domestic provider/person?
- How do you obtain data from a multi-national service provider (e.g. Facebook, Google, Microsoft etc.)?

11

Discussion: Production orders

Budapest Convention Article 18 – Production order

1 Each Party shall adopt such legislative and other measures as may be necessary to empower its competent authorities to order:

a a person in its territory to submit specified computer data in that person's possession or control, which is stored in a computer system or a computer-data storage medium; and

b a service provider offering its services in the territory of the Party to submit subscriber information relating to such services in that service provider's possession or control.

12

Discussion: Production orders

► **Example Philippines**

SEC. 14. Disclosure of Computer Data (Cybercrime Prevention Act 2012)
Law enforcement authorities, upon securing a court warrant, shall issue an order requiring any person or service provider to disclose or submit subscriber's information, traffic data or relevant data in his/its possession or control within seventy-two (72) hours from receipt of the order in relation to a valid complaint officially docketed and assigned for investigation and the disclosure is necessary and relevant for the purpose of investigation.

13

Discussion: Production orders

► **Example Laos** (Law on Prevention and Combating Cyber Crime No. 61/NA of 15 July 2015

Article 45. Opening of investigation
In case of having sufficient information and evidence of any offence regarded as cyber crime, the head of investigation organization of police or public prosecutor shall issue the ordinance of opening of investigation basing on the scope of rights and duties of the issuing the ordinance in according to the Law on Criminal Procedure.
In case of emergency, necessity and having sufficient information and evidence proving that there is a preparation or committing of cyber crime, head of investigation organization of police or public prosecutor shall issue an ordinance for protection and storage computer's data and information as well computer traffic data.
Service providers or sectors having duties of data and information management have obligations of protection and storage the prescribed data and information in good condition till the final process of cyber crime case procedure in order to ensure that they are not being lost or damaged.

Article 46. Conducting of Investigation
The investigation organization of police or office of public prosecutor shall coordinate with sector of post and telecommunication and other sectors concerned in order to search and trace information and evidence as well as source of cyber crime for regarding as the basis of investigation conducting.
The conducting of cyber crime case investigation shall apply the investigation procedures and the prevention measures as prescribed under the Law on Criminal Procedures.

14 14

14

Discussion: Production orders

► **Example Malaysia**

Specific provisons in relation with the handling and producing of evidence:-

- Section 10 of the CCA:- Powers of search, seizure and arrest
- Chapter 3 of the CMA :- Powers of entry, investigation into offences and prosecution (Section 245 to Section 262)
- Section 51 of the Criminal Procedure Code (summons to produce document or other things)
- Section 23 Mutual Assistance in Criminal Matters 2002 (production order for criminal matters)
- Section 90A of the Evidence Act 1950 Admissibility of documents produced by computers and of statements, contained therein.

(1) In any criminal or civil proceeding a document produced by a computer or a statement contained in such document, shall be admissible as evidence of any fact stated therein if the document was **produced by the computer in the course of its ordinary use**, **whether or not the person tendering the same is the maker** of such document or statement.

Provisioning of subscribers information

Service Providers are obliged to share subscriber's information to the Regulator and relevant authorities' for investigation of offences through the General Consumer Code, application of which is mandated through the Service Providers' standard licence condition. The above requirement is also duplicated in the terms and conditions of the contractual agreement for subscription of service between the Service Providers and their customers.

Discussion: Production orders

► **Example Thailand**

Computer Crime Act B.E 2550 (2007) as amended by the Computer-related Crime Act (No. 2) B.E. 2560 (2017)
Section 18.
Within the power of Section 19 and for the benefit of an investigation, if there is reasonable cause to believe that there is the perpetration of an offence under this Act, then a relevant competent official shall have any of the following authorities only as necessary to identify a person who has committed an offence in order to:
(1) issue an inquiry letter to any person related to the commission of an offence under this Act or summon them to give statements, forward written explanations or any other documents, data or evidence in an understandable form.
(2) call for computer traffic data related to communications from a service user via a computer system or from other relevant persons.
(3) instruct a service provider to deliver to a relevant competent official service users related data that must be stored under Section 26 or that is in the possession or under the control of a service provider;

Discussion: Production orders

- Production orders:
  - Different rules/thresholds for subscriber vs traffic vs content data?
  - Who can authorise?
  - What about emergency situations?
- The problem of jurisdiction. Does location matter?
  - Can your authorities issue an order to a service provider or other person IN your territory even is data stored OUTSIDE your territory?
  - When is a service provider IN your territory?
  - What about a service provider "offering a service in your territory?"
- The practice of voluntary cooperation: Can you request a provider in another country directly to give you data? Can you use this as evidence in criminal proceedings?

17

Current practice: "Voluntary" disclosure by private sector entities

	Requests for data sent to Apple, Facebook, Google, Microsoft, Twitter and Yahoo in 2015		
Parties	Received	Disclosure	%
Australia	6 777	4 580	47%
Belgium	1 992	1 453	68%
Bulgaria	8	2	25%
Canada	1 157	884	76%
Finland	227	172	76%
France	27 213	14 746	54%
Germany	29 092	15 469	53%
Japan	2 018	1 112	55%
Netherlands	1 605	1 213	76%
Portugal	3 255	1 751	54%
Romania	76	30	39%
United Kingdom	29 937	21 075	70%
USA	89 350	70 116	78%
Total excluding USA	**138 612**	**82 529**	**60%**
Total including USA	227 962	152 644	67%

18

"Voluntary" disclosure by private sector entities to ASEAN countries

	Requests for data sent to Facebook, Google, Microsoft in 2016		
Parties	Received	Disclosure	%
Brunei	3	0	0%
Cambodia	0	0	0%
Indonesia	39	7	18%
Laos	0	0	0%
Malaysia	44	26	59%
Myanmar	1	0	0%
Philippines	15	2	13%
Singapore	3 169	1 594	50%
Thailand	15	0	0%
Vietnam	0	0	0%
Australia	5 794	3 819	66%
France	26 055	15 869	61%
Germany	34 169	19 094	56%
Portugal	3 809	2 269	60%

19

Issue: "Voluntary" disclosure by private sector entities

- More than 135,000 requests/year by Parties to Budapest Convention to major US providers
- Disclosure of subscriber or traffic data (ca. 60%)
- Providers decide whether or not to respond to lawful requests and whether to notify customers
- Provider policies/practices volatile
- Data protection concerns
- No disclosure by European providers
- No admissibility of data received in some States

► Clearer / more stable framework required

www.coe.int/cybercrime

20

Issue: Data protection and other safeguards

- Data protection requirements normally met if powers to obtain data defined in domestic criminal procedure law and/or MLA agreements
- MLA not always feasible
- Increasing "asymmetric" disclosure of data transborder
  - From LEA to service provider ► Permitted with conditions
  - From service provider to LEA ► Unclear legal basis ► providers to assess lawfulness, legitimate interest ► risk of being held liable ▌ Confidentiality requirements

= Clearer framework for public to private to public disclosure transborder required

Evidence in the Cloud: towards solutions

Solutions:

1. More efficient MLA
2. Guidance Note on Article 18
3. Domestic rules on production orders (Article 18)
4. Cooperation with providers: practical measures
5. Protocol to Budapest Convention

Solution 2: Guidance Note on Article 18

Guidance Note on Article 18 Budapest Convention on production of subscriber information:

- Domestic production orders for subscriber information if a provider is in the territory of a Party even if data is stored in another jurisdiction (Article 18.1.a)
- Domestic production orders for subscriber information if a provider is NOT necessarily in the territory of a Party but is offering a service in the territory of the Party (Article 18.1.b)

► Foresee this in your domestic law

Agreed by T-CY on 28 Feb 2017

www.coe.int/cybercrime

23

Solution 2: Guidance Note on Article 18

The production of subscriber information under Article 18 Budapest Convention could be ordered if the following criteria are met in a specific criminal investigation and with regard to specified subscribers

IF

The criminal justice authority has jurisdiction over the offence;

AND IF

the service provider is in possession or control of the subscriber information;

AND IF

Article 18.1.a The person (service provider) is in the territory of the Party.	OR	Article 18.1.b A Party considers that a service provider is "offering its services in the territory of the Party" when, for example: – the service provider enables persons in the territory of the Party to subscribe to its services (and does not, for example, block access to such services); and – the service provider has established a real and substantial connection to a Party. Relevant factors include the extent to which a service provider orients its activities toward such subscribers (for example, by providing local advertising or advertising in the language of the territory of the Party), makes use of the subscriber information (or associated traffic data) in the course of its activities, interacts with subscribers in the Party, and may otherwise be considered established in the territory of a Party.

24

24

Solution1: More efficient MLA

- Implement legal and practical measures
  ► Recommendations 1 – 15 of T-CY assessment report on MLA at domestic levels
  - More resources and training
  - Electronic transmission of requests
  - Streamlining of procedures
  - Etc.
- Parties to establish emergency procedures for obtaining data in their MLA systems
- Parties to facilitate access to subscriber information in domestic legislation (full implementation of Article 18 Budapest Convention)

Solution 5: Protocol to Budapest Convention

A. Provisions for more efficient MLA

B. Provisions for direct cooperation with providers in other jurisdictions

C. Framework and safeguards for existing practices of transborder access to data

D. Data protection

Terms of reference for preparation of a Protocol agreed by T-CY in June 2017. Work will start in September 2017.

Discussion: What solutions?

- More efficient international cooperation
  - Streamline MLA procedures?
  - Joint agreements such as Budapest Convention?

- Production orders:
  - Different rules/thresholds for subscriber vs traffic vs content data?
  - Who can authorise?
  - What about emergency situations?

- The problem of jurisdiction. Does location matter?
  - Can your authorities issue an order to a service provider or other person IN your territory even is data stored OUTSIDE your territory?
  - When is a service provider IN your territory?
  - What about a service provider "offering a service in your territory?"

- The practice of voluntary cooperation: Can you request a provider in another country directly to give you data? Can you use this as evidence in criminal proceedings?

27