Cyber3 Conference / Track C - Cybercrime

Okinawa, 7-8 November 2015
Alexander Seger, Council of Europe

COUNCIL OF EUROPE
CONSEIL DE L'EUROPE

- ✓ Budapest Convention on Cybercrime in place and functioning
- ✓ Backed up by Cybercrime Convention Committee (T-CY) for quality of implementation + additional solutions
- ✓ Backed up by capacity building programmes (C-PROC) to enable implementation

Core challenge: Access to electronic evidence for criminal justice purposes with rule of law safeguards

- Need for more efficient police2police cooperation and mutual legal assistance ► T-CY assessment and recommendations (December 2014)
- Need for international solutions on access to data in the cloud ► T-CY Cloud Evidence Group (proposals in 2016) ► Additional Protocol?
- Need for specific rules permitting access to evidence to meet rule of law and privacy standards

www.coe.int/cybercrime

1

The approach of the Council of Europe

1 Common standards: Budapest Convention on Cybercrime and relates standards

2 Follow up and assessments: Cybercrime Convention Committee (T-CY)

3 Capacity building: C-PROC ► Technical cooperation programmes

2

Budapest Convention: scope

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
- Interception of computer data

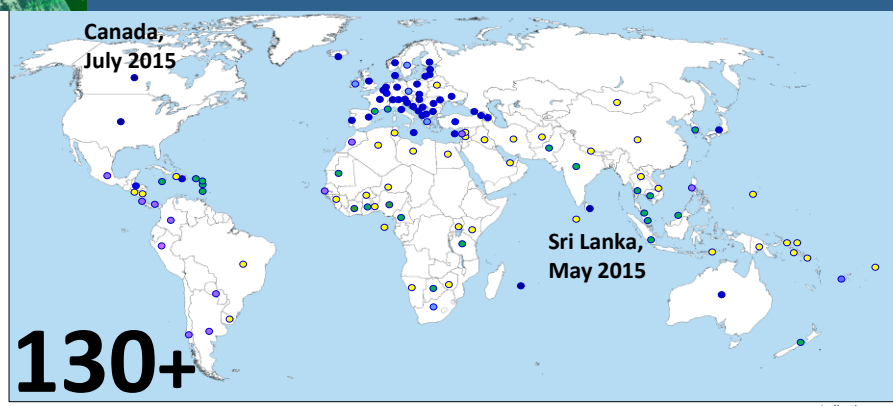
+

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

Harmonisation

3

Reach of the Budapest Convention



Budapest Convention
Ratified/acceded: 47
Signed: 7
Invited to accede: 12
= 66

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

Further States drawing on Budapest Convention for legislation = 45+

4

Budapest Convention: The role of the Cybercrime Convention Committee (T-CY)

Established under Article 46 Budapest Convention

Membership (August 2015):

- 47 Members (State Parties)
- 19 Observer States
- 12 organisations (African Union Commission, Commonwealth Secretariat, ENISA, European Union, Eurojust, Europol, INTERPOL, ITU, OAS, OECD, OSCE, UNODC)

Functions:

- Assessments of the implementation of the Convention by the Parties
- Guidance Notes
- Draft legal instruments

Two plenaries/year as well as Bureau and working group meetings

- ► An effective follow up mechanism
- ► The T-CY appears to be the main inter-governmental body on cybercrime matters internationally

5

International cooperation on cybercrime and electronic evidence: what solutions?

Cybercrime Convention Committee (T-CY)

(= Committee of Parties to Budapest Convention)

- Transborder access to data: clarification of Article 32b and its limits → Guidance Note (adopted December 2014)
- Assessment of effectiveness of mutual legal assistance provisions (24 recommendations adopted in December 2014)
  - Follow up by Parties
  - Capacity building programmes
  - Review of progress made by T-CY in 2016
- Establishment of "Cloud Evidence Group"
  - "Challenges report" June 2015
  - Private sector hearing on 30 November 2015
  - Guidance Notes?
  - Negotiation of a Protocol to Budapest Convention?

6

Capacity building programmes

GLACY EU/COE Joint Project on Global Action on Cybercrime

Cybercrime@EAP II EU/COE Eastern Partnership

Cybercrime@Octopus (voluntary contribution funded)

All projects are managed by:

✓ **C-PROC** (Cybercrime Programme Office of the Council of Europe, Bucharest, Romania)

7

Cybercrime Programme Office of the Council of Europe (C-PROC) in Romania

- Committee of Ministers decision October 2013
- Operational as from April 2014
- Currently 10 staff

- **Task: Support to countries worldwide to strengthen criminal justice capacities on cybercrime and electronic evidence**

8

Cybercrime and electronic evidence: Challenges for criminal justice

Challenges for criminal justice:

- The scale and quantity of cybercrime, devices, users and victims
- Technical challenges (VPN, P2P, 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
- Uncertainty regarding the availability of data ▶ no data ▶ no evidence ▶ no justice

9

T-CY assessment: findings

Types of requests

Types of data requested:

1. **Subscriber information** (80+%?)
2. **Traffic data**
3. **Content data**

Underlying offences

1. **Fraud and other financial crimes**
2. **Violent and serious crime** (murder, assault, trafficking, child abuse etc.)
3. **Offences against computer systems**

10

T-CY assessment: recommendations

Recommendations falling under the responsibility of domestic authorities

- Implement provisions of Budapest Convention
- Statistics or other measures to monitor efficiency of the MLA process
- More technology-literate staff for MLA
- More training
- Strengthen 24/7 contact points
- Streamline procedures and reduce the number of steps required for MLA at domestic levels
- Make use of all available channels for international cooperation
- Establish emergency procedures
- Confirm receipts of MLA requests
- Open domestic investigations upon a foreign request or spontaneous information
- Electronic transmission of requests (art. 25.3)
- Make sure requests are specific and complete
- Consult foreign authorities before sending MLA requests

11

T-CY assessment: recommendations

Recommendations falling under the responsibility of CoE capacity building programmes

- **Multi-language templates for Article-31 type MLA requests**
- **Online resource on MLA requirements by Parties to Budapest Convention**

12

T-CY assessment: recommendations

Recommendations falling under the responsibility of CoE capacity building programmes

- Multi-language templates for Article-31 type MLA requests
- Online resource on MLA requirements by Parties to Budapest Convention

13

T-CY CEG report: Evidence in the cloud

About the T-CY Cloud Evidence Group:

- Established in December 2014
- Task: To explore solutions for criminal justice access to evidence stored on servers in the cloud and in foreign jurisdictions, including through mutual legal assistance
- Take into account:
  - T-CY assessment on MLA
  - Work of Transborder Group
  - Analysis of challenges
  - Views of industry and other stakeholders
- By December 2016: report with draft options and recommendations for consideration by T-CY

14

T-CY CEG report: Evidence in the cloud

Cybercrime and the question of electronic evidence:

- Impact of cybercrime ▶ Attacks against core values of societies (human rights, democracy and rule of law)
- Confusion between national security and criminal justice ▶ "We need more effective criminal justice and we need stronger safeguards regarding national security measures."
- Uncertainty regarding the availability of data ▶ no data ▶ no evidence ▶ no justice
- Cloud computing: distributed systems ▶ distributed data ▶ distributed evidence

15

T-CY CEG report: Evidence in the cloud

Types of data needed for criminal justice purposes:

1. Subscriber information
2. Traffic data
3. Content data

16

T-CY CEG report: Evidence in the cloud

Challenges for criminal justice:

- The scale and quantity of cybercrime, devices, users and victims
- Technical challenges (VPN, P2P, anonymisers, encryption, VOIP, NATs etc.)
- Cloud computing, territoriality and jurisdiction
  - 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

17

T-CY CEG report: Evidence in the cloud

Questions:

<u>Jurisdiction</u>

1. Which government would be the addressee of a lawful request for data by a country attacked in a cloud context where the territorial origin of a cyber offence is not clear, the controller of data is hidden behind layers of service providers, or data is moving, fragmented or mirrored in multiple jurisdictions?

18

T-CY CEG report: Evidence in the cloud

Questions: Jurisdiction

2. What governs jurisdiction to enforce for criminal justice purposes:

a) Location of data?
b) Nationality of owner of data?
c) Location of owner of data?
d) Nationality of data owner?
e) Location of data controller?
f) Headquarters of a cloud service provider?
g) Subsidiary of a cloud service provider?
h) Territory where a cloud provider is offering its services?
i) Laws of the territory where the data owner has subscribed to a service?
j) Territory of the criminal justice authority?

19

T-CY CEG report: Evidence in the cloud

Questions: Jurisdiction

3. What does it mean "offering its services in a territory" (see Article 18.1.b 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.

20

T-CY CEG report: Evidence in the cloud

Questions: **Jurisdiction**

4. If a domestic court order authorizes the interception of a communication between two nationals or persons on its territory, why would MLA be required even if technically the provider would carry out the interception on a server on a foreign country?

To what extent would the sovereignty of that foreign country be affected?

To what extent would the rights of the defendants not be protected?

Similar for production orders regarding content data?

21

T-CY CEG report: Evidence in the cloud

Questions: **Mutual legal assistance**

8. What additional international legally binding solutions

Rec 19 Parties should consider allowing – via legal domestic amendments and international agreement – for the expedited disclosure of the identity and physical address of the subscriber of a specific IP address or user account.

Rec 20 Interested Parties may consider the possibility and scope of an international production order to be directly sent by the authorities of a Party to the law enforcement authorities of another Party.

Rec 21 Parties should consider enhancing direct cooperation between judicial authorities in mutual legal assistance requests.

22

T-CY CEG report: Evidence in the cloud

Questions: **Mutual legal assistance**

8. What additional international legally binding solutions

Rec 22 Parties may consider addressing the practice of law enforcement and prosecution services obtaining information directly from foreign service providers, and related safeguards and conditions.

Rec 23 Parties should consider joint investigations and/or the establishment of joint investigation teams between Parties.

Rec 24 Parties should consider allowing for requests to be sent in English language. Parties should in particular allow for preservation requests to be sent in English.

23