EUROJUST

Strategic Meeting on Cybercrime (The Hague, 19-20 November 2014)

Budapest Convention on Cybercrime and the question of transborder access

Alexander Seger
Council of Europe

www.coe.int/cybercrime

COUNCIL OF EUROPE
CONSEIL DE L'EUROPE

1

Conclusions

1. Budapest Convention is functioning and evolving in terms of quality of implementation and membership (quantity)

2. Dynamic framework of :
   - ✓ Standards (Budapest Convention)
   - ✓ Follow up (T-CY)
   - ✓ Capacity building (C-PROC)

3. Additional solutions required, but negotiations will be challenging

COE approach on cybercrime

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

3

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

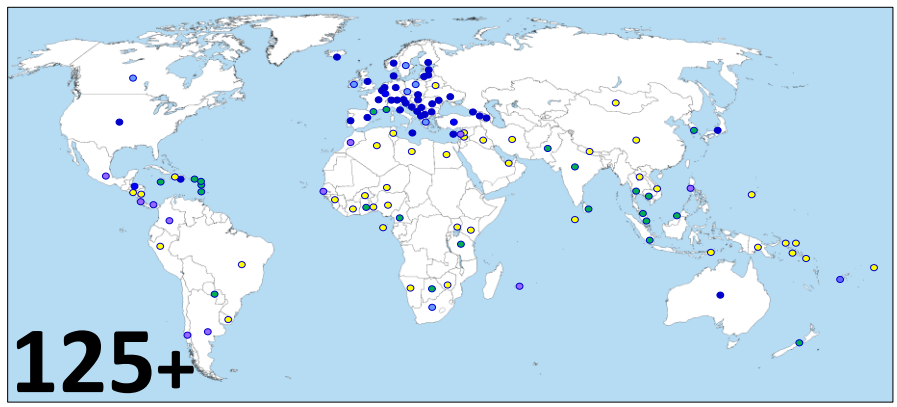
+

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

Harmonisation

4

Reach of the Budapest Convention



Indicative map only

Budapest Convention
Ratified/acceded: 44
Signed: 9
Invited to accede: 10
= 63

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

Further States drawing on Budapest Convention for legislation = 43+

5

Capacity building programmes

GLACY EU/COE Joint Project on Global Action on Cybercrime

Cybercrime@EAP 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)

6

Cybercrime Convention Committee (T-CY)

Established under Article 46 Budapest Convention

Membership
(status November 2014):

- 44 Members (State Parties)
- 19 Observer States
- 10 International organisations (African Union Commission, ENISA, European Union, Europol, INTERPOL, ITU, OAS, OECD, OSCE, UNODC)

Functions:

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

7

Cybercrime Convention Committee (T-CY): Guidance Notes

Guidance Notes adopted:

- ✓ Notion of "Computer Systems"
- ✓ Botnets
- ✓ Identity theft
- ✓ DDOS attacks
- ✓ Critical Infrastructure Attacks
- ✓ Malware

Guidance Notes under negotiation:

- SPAM
- Article 32 b (Transborder access)

8

Cybercrime Convention Committee (T-CY): Assessments

2nd round of T-CY Assessments:

Efficiency of international cooperation provisions:

- **Article 31 on mutual assistance regarding accessing of stored computer data.**
- **And related Articles 23, 25, 26, 27, 28 and 35.**

Aim:

- **Better use of existing provisions**
- **Additional solutions**

Procedure and status:

- **Questionnaire February 2013.**
- **Plenary discussions June 2013, Dec 2013, June 2014.**
- **Revised report to be discussed (adopted) in December 2014.**

9

T-CY assessment: draft 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**

10

T-CY assessment: draft 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

11

T-CY assessment: draft recommendations

Recommendations that may require an Additional Protocol

- Allow for expedited disclosure of subscriber information
- Introduce international production order
- Direct cooperation between judicial authorities
- Directly obtain specified traffic and subscriber information from foreign service providers
- Joint investigations and JITs
- Requests in English language

12

Cybercrime Convention Committee (T-CY)

T-CY work on transborder access

- Analysis of question of transborder access to data and jurisdiction, including Article 32 since 2009
- T-CY subgroup on Transborder Access established in November 2011 and its report adopted by T-CY in December 2012:
  1. Work on a Guidance Note on the existing Article 32b
  2. Work on an Additional Protocol to the Budapest Convention
- Dialogue with civil society, data protection and industry in 2013.
- T-CY decision December 2013 ▶ Before commencing negotiation of a Protocol:
  1. Continue dialogue with stakeholders
  2. Take into account results of T-CY assessment of MLA provisions
  3. Submit proposals regarding a Protocol to 12th Plenary of T-CY (Dec 2014)

13

Cybercrime Convention Committee (T-CY):
T-CY work on transborder access

Article 19 Budapest Convention - Search and seizure of stored computer data

1 Each Party shall adopt such legislative and other measures as may be necessary to empower its competent authorities to search or similarly access:
a a computer system or part of it and computer data stored therein; and
b a computer-data storage medium in which computer data may be stored in its territory.

2 Measures to ensure that where authorities search or similarly access a specific computer system or part of it, pursuant to paragraph 1.a, and have grounds to believe that the data sought is stored in another computer system or part of it in its territory, and such data is lawfully accessible from or available to the initial system, the authorities shall be able to expeditiously extend the search or similar accessing to the other system.

14

Cybercrime Convention Committee (T-CY): T-CY work on transborder access

Article 32 Budapest Convention – Trans-border access to stored computer data with consent or where publicly available

A Party may, without the authorisation of another Party:

a access publicly available (open source) stored computer data, regardless of where the data is located geographically; or

b access or receive, through a computer system in its territory, stored computer data located in another Party, if the Party obtains the lawful and voluntary consent of the person who has the lawful authority to disclose the data to the Party through that computer system.

15

Cybercrime Convention Committee (T-CY): T-CY work on transborder access

Typical scenarios:

- **A person's e-mail may be stored in another country by a service provider, or a person may intentionally store data in another country. These persons may retrieve the data and, provided that they have the lawful authority, they may voluntarily disclose the data to law enforcement officials or permit such officials to access the data, as provided in the Article**
- **A suspected drug trafficker is lawfully arrested while his/her mailbox – possibly with evidence of a crime – is open on his/her tablet, smartphone or other device. If the suspect voluntarily consents that the police access the account and if the police are sure that the data of the mailbox is located in another Party, police may access the data under Article 32b.**

16

Cybercrime Convention Committee (T-CY): T-CY work on transborder access

(Draft) Guidance Note on Article 32

General considerations: Article 32b is a measure to be applied in specific criminal investigations and proceedings within the scope of Article 14.

On the notion of "access without the authorisation of another Party": Article 32b does not require mutual assistance, and the Budapest Convention does not require a notification of the other Party. At the same time, the Budapest Convention does not exclude notification. Parties may notify the other Party if they deem it appropriate.

On the applicable law: In all cases, law enforcement authorities must apply the same legal standards under Article 32b as they would domestically. If access or disclosure would not be permitted domestically it would also not be permitted under Article 32b.

17

Cybercrime Convention Committee (T-CY): T-CY work on transborder access

(Draft) Guidance Note on Article 32

On the person who can provide access or disclose data: Service providers are unlikely to be able to consent validly and voluntarily to disclosure of their users' data under Article 32.

Domestic lawful requests versus Article 32b: Article 32b is not relevant to domestic production orders or similar lawful requests internal to a Party.

On the location of the person consenting to provide access or disclose data: The standard hypothesis is that the person providing access is physically located in the territory of the requesting Party. However, multiple situations are possible.

18

Cybercrime Convention Committee (T-CY): T-CY work on transborder access

Proposals for a Protocol to provide for additional possibilities:

1. Transborder access with consent without the limitation to data stored "in another Party"
2. Transborder access without consent but with lawfully obtained credentials
3. Transborder access without consent in good faith or in exigent or other circumstances
4. Extending a search without the limitation "in its territory" in Article 19.3
5. The power of disposal as connecting legal factor

With conditions and safeguards!

19

Cybercrime Convention Committee (T-CY): T-CY work on transborder access

Need for a Protocol?

Yes, because:

- Difficulty in securing data for criminal justice + technological evolution
- More crime, more evidence online
- Significant to address violent crime
- Cost of crime to human rights / need to protect rights of victims
- MLA procedures often not applicable
- Cooperation by providers decreasing
- Enormous share of cases abandoned
- Unilateral solutions + informal arrangements

Feasibility?

No (not yet), because:

- Governments divided
- Reports on mass surveillance
- Data protection framework still in the making
- Regulations on criminal justice access unstable following data retention ruling
- Developments regarding jurisdiction

"The lack of concern for the rights of victims has been a distressing revelation for the Transborder Group"

20

Cybercrime Convention Committee (T-CY): T-CY work on transborder access

Report of the Transborder Group for discussion by T-CY (2-3 December 2014) – draft proposals:

- **Adopt Guidance Note on Article 32**
- **Protocol on Transborder Access needed but not feasible in the current context.**
- **Option: follow up to T-CY assessment of MLA provisions and work of the Transborder Group by ▶ setting up a working group on criminal justice access to evidence stored in the cloud, including through mutual legal assistance ("Cloud evidence group").**

The Transborder Group believes that in the absence of an agreed upon international framework with safeguards, more and more countries will take unilateral action and extend law enforcement powers to remote transborder searches either formally or informally with unclear safeguards. Such unilateral or rogue assertions of jurisdiction will not be a satisfactory solution.

21