



Budapest Convention Cybercrime

- Update -

Wellington, New Zealand, 7 July 2017

Alexander Seger
Executive Secretary
Cybercrime Convention Committee
Council of Europe
Strasbourg, France
alexander.seger@coe.int



www.coe.int/cybercrime

1

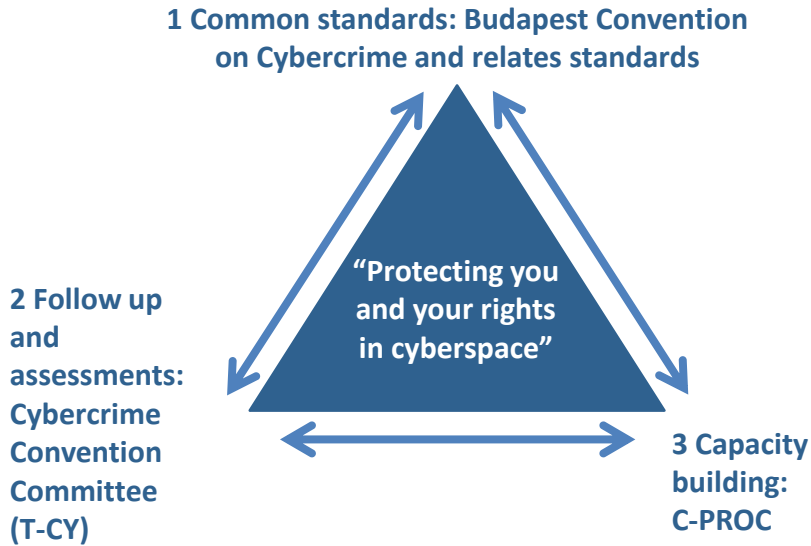


Snapshot of recent activities (7 June / 7 July 2017)

- **Cybercrime Convention Committee (T-CY), Strasbourg**
- **Eastern Partnership meeting, Brussels**
- **EGTEG meeting on access to judicial training materials, Brussels**
- **iPROCEEDS meeting, Luxemburg**
- **C-PROC, Bucharest**
- **Training workshops, Philippines**
- **ASEAN regional workshop, Philippines**
- **ICANN, South Africa**
- **Advice on CERT, legislation and cybercrime reporting, Tonga**
- **Belarus, Armenia etc.**

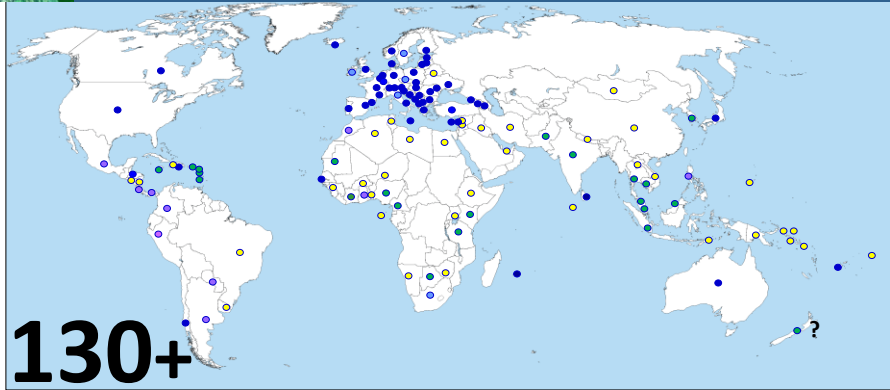
2

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



3

Reach of the Budapest Convention



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+



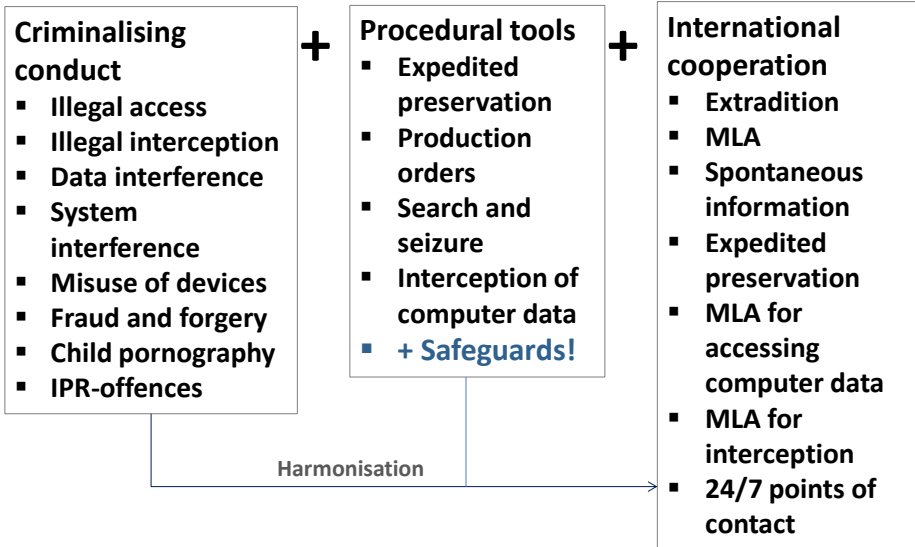
Further States drawing on Budapest Convention for legislation = 45+



4



Scope of Budapest Convention



5



Scope of Budapest Convention

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



Cybercrime Convention Committee (T-CY)

Established under Article 46 Budapest Convention

Membership

(status June 2017):

- 55 Members (State Parties)
- 14 Observer States
- 10 International organisations (African Union Commission, Commonwealth Sec, 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.

2 x plenaries per year
+ Bureau and Working Group meetings

7



T-CY Guidance Notes

Guidance Notes adopted:

- ✓ Notion of "Computer Systems"
- ✓ Botnets
- ✓ Identity theft
- ✓ DDOS attacks
- ✓ Critical Infrastructure Attacks
- ✓ Malware
- ✓ Transborder access to data (Article 32)
- ✓ Terrorism
- ✓ Production orders for subscriber information (Article 18)

8



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

Context:

Budapest Convention on Cybercrime ► Cybercrime Convention Committee (T-CY)
 ► Cloud Evidence Group ► Recommendations September 2016 ► now under consideration by T-CY

Rationale:

- Cybercrime AND electronic evidence in relation to any crime
- E-evidence on servers in foreign, unknown, multiple or shifting jurisdictions, in the cloud
- No data, no evidence, no prosecution, no justice, no rule of law (in cyberspace)

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

www.coe.int/cybercrime

9



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)

*Agreed by T-CY
on 28 Feb 2017*

www.coe.int/cybercrime

10



“Voluntary” disclosure by private sector entities: examples

	Requests for data sent to Facebook, Google, Microsoft in 2016		
	Received	Disclosure	%
Indonesia	39	7	18%
Malaysia	44	26	59%
Philippines	15	2	13%
Singapore	3 169	1 594	50%
Australia	5 794	3 819	66%
France	26 055	15 869	61%
Germany	34 169	19 094	56%
Portugal	3 809	2 269	60%
New Zealand	304	167	55%

11



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.

Participation by New Zealand in negotiation of Protocol?

www.coe.int/cybercrime

12