Funded
by the European Union
and the Council of Europe

EUROPEAN UNION

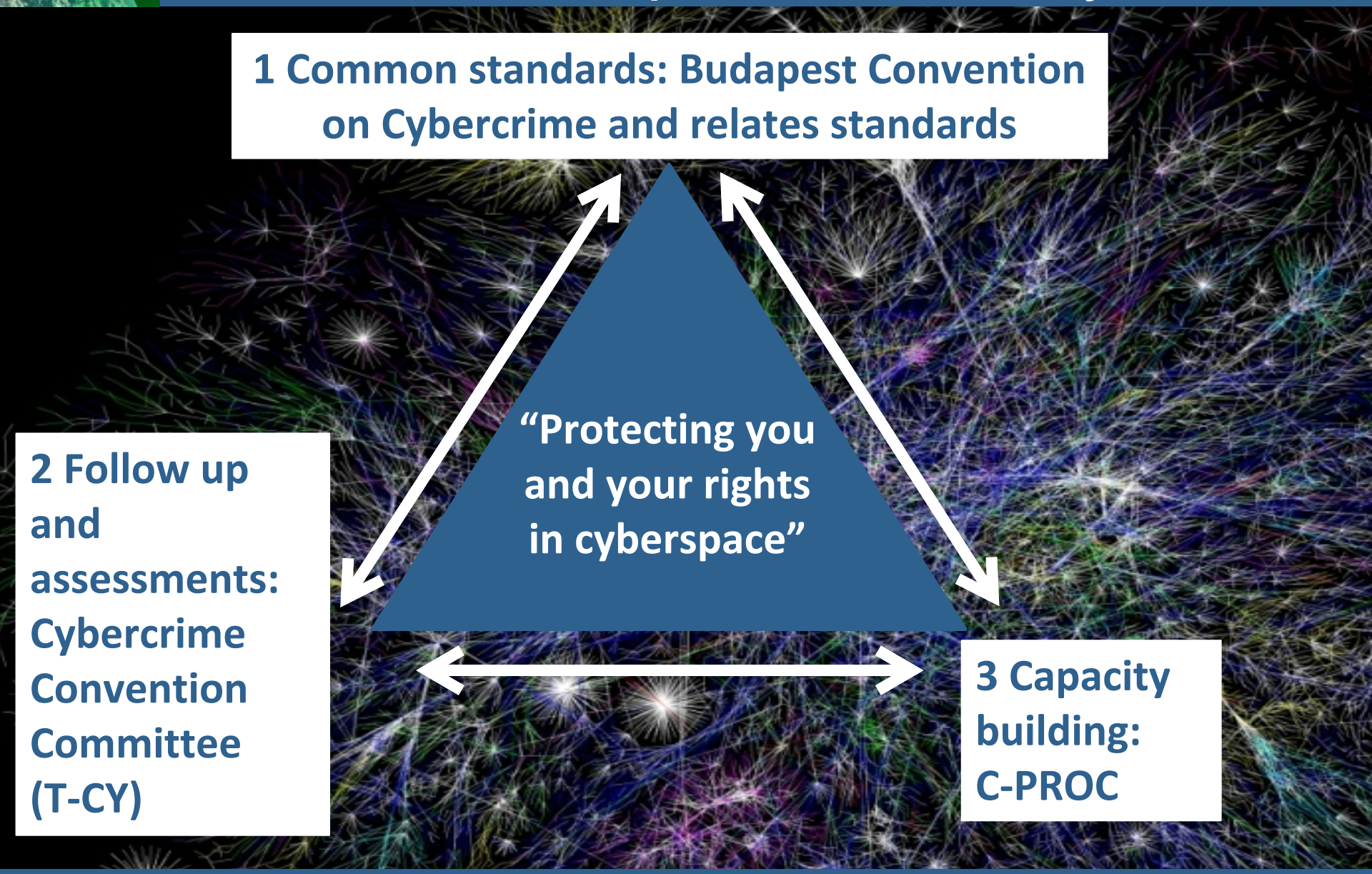
COUNCIL OF EUROPE

CONSEIL DE L'EUROPE

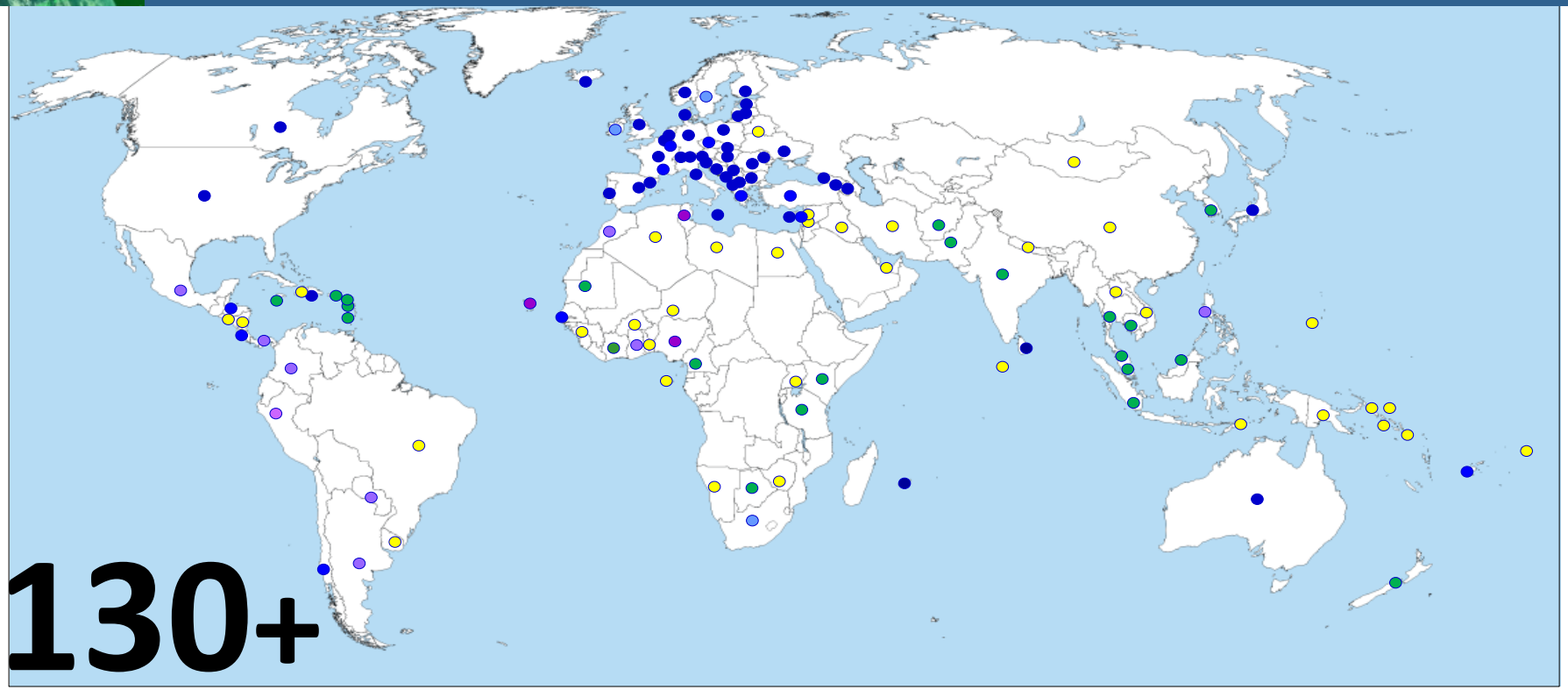
Implemented
by the Council of Europe

EUROJUST

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



Reach of the Budapest Convention



Indicative map only

Budapest Convention
Ratified/acceded: 56
Signed: 4
Invited to accede: 11
= 71

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

Further States drawing on Budapest Convention for legislation = 45+

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

Limited by conditions and safeguards (article 15)

+

International cooperation

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

Harmonisation

The approach of the Council of Europe on cybercrime

Cybercrime Convention Committee (T-CY)

- 55 members (Parties to Convention), 14 observer States, 10 observer organisations (including EUROPOL and INTERPOL)
- Plenaries and working groups
- Assessing implementation of the Convention by the Parties
- Guidance Notes to use existing provision to address new challenges
- Preparation of new instruments ▸ Protocol to the Budapest Convention

Capacity building by C-PROC: Support to implementation of Budapest Convention and follow up to T-CY decisions

- Cybercrime@Octopus
- Cybercrime@EAP II and III
- iPROCEEDS - Cooperation on Cybercrime: targeting crime proceeds on the Internet
- GLACY+ EU/COE - Joint Project on Global Action on Cybercrime
- CyberSouth - Strengthen legislation and institutional capacities on cybercrime and electronic evidence

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

Crime and jurisdiction in cyberspace ► Issues

Specific issues to be addressed:

- 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

Example: voluntary cooperation by providers

	Requests for data sent to Apple, Facebook, Google, Microsoft, Twitter and Yahoo in 2015		
Parties	Received	Disclosure	%
Austria	254	119	47%
Belgium	1 992	1 453	73%
Canada	1 157	884	76%
France	27 213	14 746	54%
Germany	29 092	15 469	53%
Italy	7 847	3 591	46%
Netherlands	1 605	1 213	76%
Poland	2 378	820	34%
Portugal	3 255	1 751	54%
Spain	4 151	2 092	50%
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%

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

Solutions:

1. More efficient MLA [agreed by T-CY]
2. Guidance Note on Article 18 [approved by T-CY in February 2017]
3. Domestic rules on production orders (Article 18) [agreed by T-CY]
4. Cooperation with providers: practical measures [agreed by T-CY]
5. Protocol to Budapest Convention [negotiations started in Sep 2017]

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

Solution 5: Protocol to Budapest Convention

A. Provisions for more efficient MLA

- Expedited MLA for subscriber information
- International production orders
- Direct cooperation between judicial authorities
- Joint investigations
- Emergency procedures for access to data
- Role of 24/7 contact points

B. Provisions for direct cooperation with providers in other jurisdictions

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

D. Safeguards/data protection

Terms of reference approved in June 2017.
Negotiations: Sep 2017 – Dec 2019.

Support of LEA community needed to conclude Protocol for more efficient access to evidence in the cloud!

Save-the-dates

- UN Intergovernmental Expert Group on Cybercrime, Vienna, 3-5 April 2018 ▶ Focus on legal frameworks and criminalisation
- UN Commission on Crime Prevention and Criminal Justice, Vienna, 14-18 May 2018 ▶ Focus on cybercrime
- GLACY+ Steering Committee, Vienna, Monday, 14 May
- Cybercrime week at the Council of Europe, Strasbourg, 9-13 July 2018
  - 9 July: Plenary of Cybercrime Convention Committee
  - 10-11 (AM) July: Protocol Drafting Plenary
  - 11 July: (AM): Workshop for 24/7 contact points
  - 11 (PM) – 13 July: Octopus Conference


www.coe.int/cybercrime