



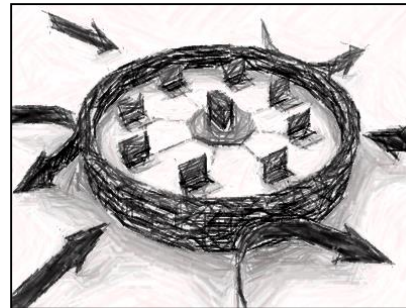
Funded
by the European Union
and the Council of Europe



Implemented
by the Council of Europe

Regulatory Framework for Security in Cyberspace

Council of Europe approach

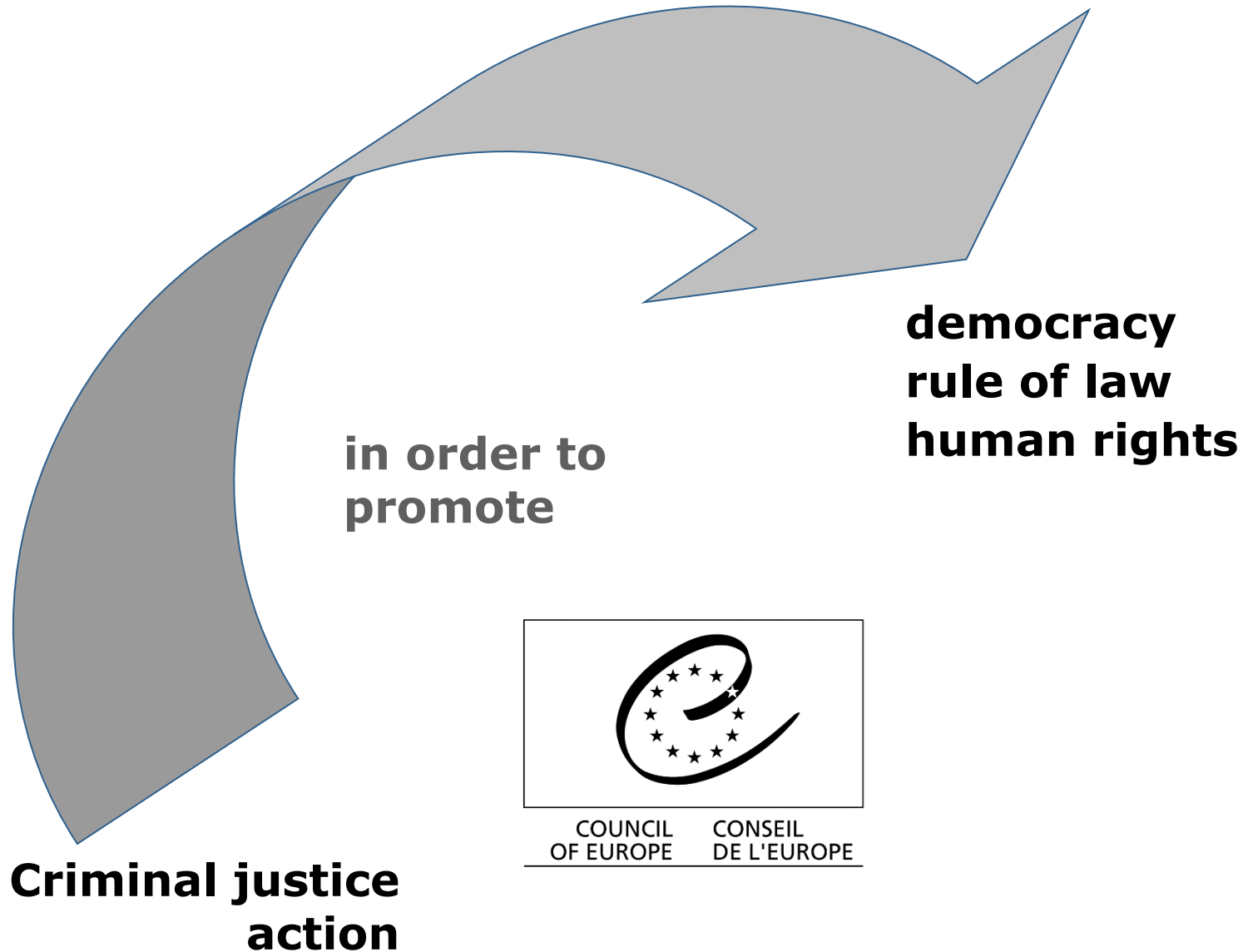


***Prepared by the Cybercrime Programme Office
of the Council of Europe***

Partnership for Good Governance



Council of Europe and cybercrime: rationale



The approach of Council of Europe

1 Common standards: **Budapest Convention on Cybercrime and related standards**

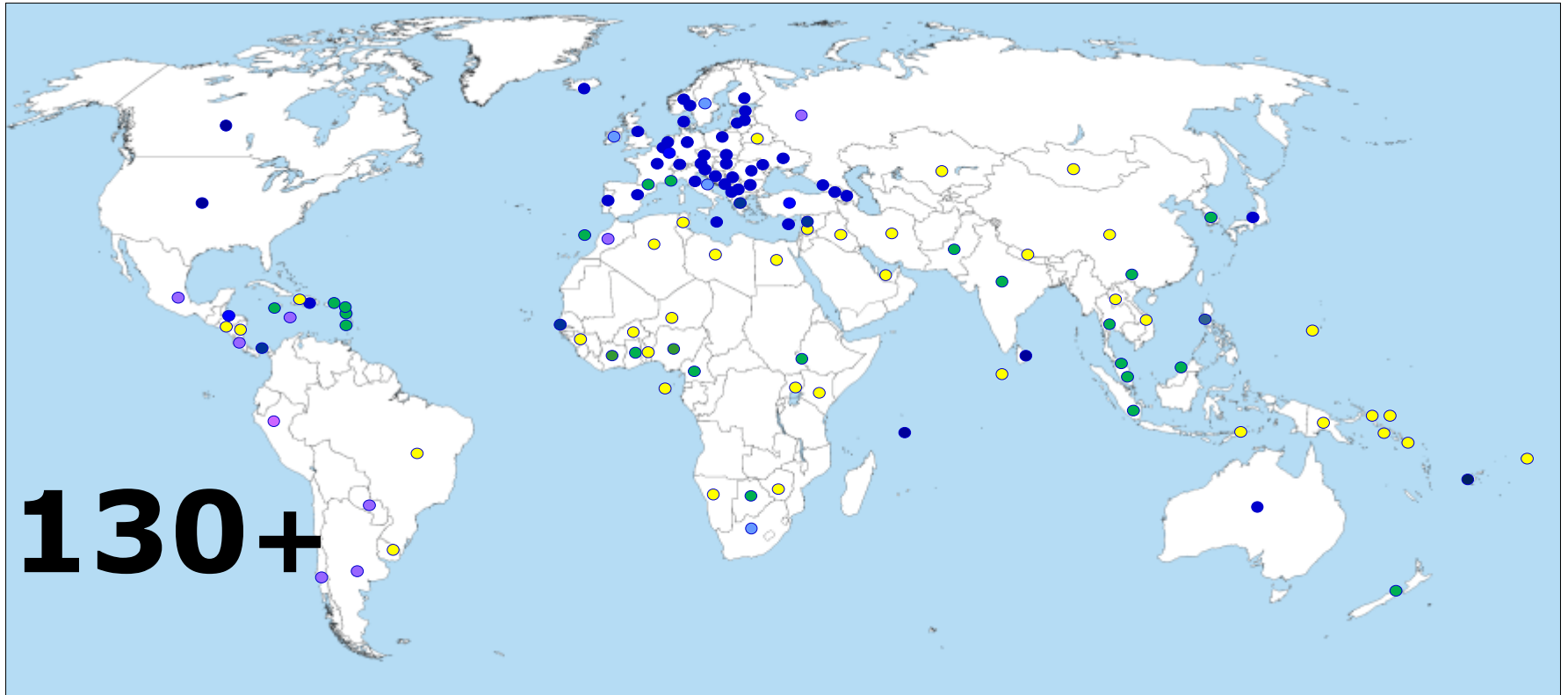
2 Follow up and assessments:
Cybercrime Convention Committee (T-CY)

“Protecting you and your rights in cyberspace”

3 Capacity building:
C-PROC
Technical cooperation programmes



Reach of the Budapest Convention



130+

**Budapest Convention
Ratified/acceded: 61**

Signed: 4

**Invited to accede: 7
= 72**



**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/seizure
- Production orders
- Monitoring/int 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




Need to regulate: Substantive law & definitions

- Offences against and by means of computer systems and data
- Content-related offences (especially child abuse)
- Any other offences that may be “on the edge”: CSIRT taxonomies
- Sufficiently dissuasive sanctions (Art. 13)
- Definitions :
 - Computer system;
 - Computer data/electronic evidence (?);
 - Service provider;
 - Subscriber information, traffic data, etc.



Need to regulate: Procedural powers

- Data preservation
- Production orders
- Search and seizure
- Real-time monitoring and interception
- Need to balance procedural powers with Article 15 guarantees
- Balance between operative/detective powers and criminal procedure
- Investigative competencies division



Need to regulate: International cooperation

- Enabling environment for mutual legal assistance for cases of cybercrime and electronic evidence
- Regulations to make all procedural powers work in international cooperation context
- Spontaneous information
- Transborder access to data
- Operation of the 24/7 points of contact network
- National regulations: efficiency, coordination, quality



Need to regulate: Less obvious considerations

- ISP liabilities and specifically data retention regulations
- Data protection oversight and efficiency
- Security and intelligence operations and limits
- Cyber security framework and critical infrastructure regulations
- Increased role of Computer Emergency Response Teams
- Financial intelligence and source of data for investigations
- Interagency cooperation and data exchange/reporting



Funded
by the European Union
and the Council of Europe



Implemented
by the Council of Europe

GLACY+ EU/COE Joint Project on Global Action on Cybercrime

iPROCEEDS EU/COE Targeting crime proceeds on the Internet

Cybercrime@EAP 2018 EU/COE Eastern Partnership

CyberSouth EU/COE Joint Project on Cybercrime and Electronic Evidence

Cybercrime@Octopus (voluntary contribution funded)





Funded
by the European Union
and the Council of Europe



Implemented
by the Council of Europe

Thank you for your attention

Giorgi Jokhadze
Project Manager
Cybercrime Programme Office
Council of Europe - Conseil de l'Europe
Bucharest, Romania
Giorgi.Jokhadze@coe.int