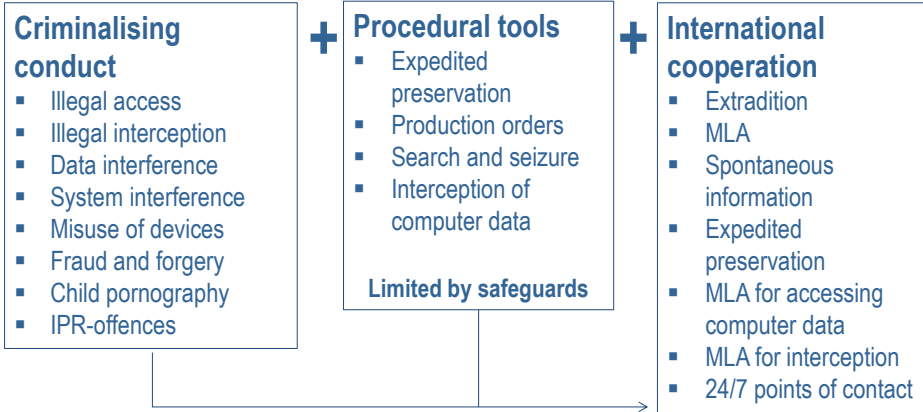






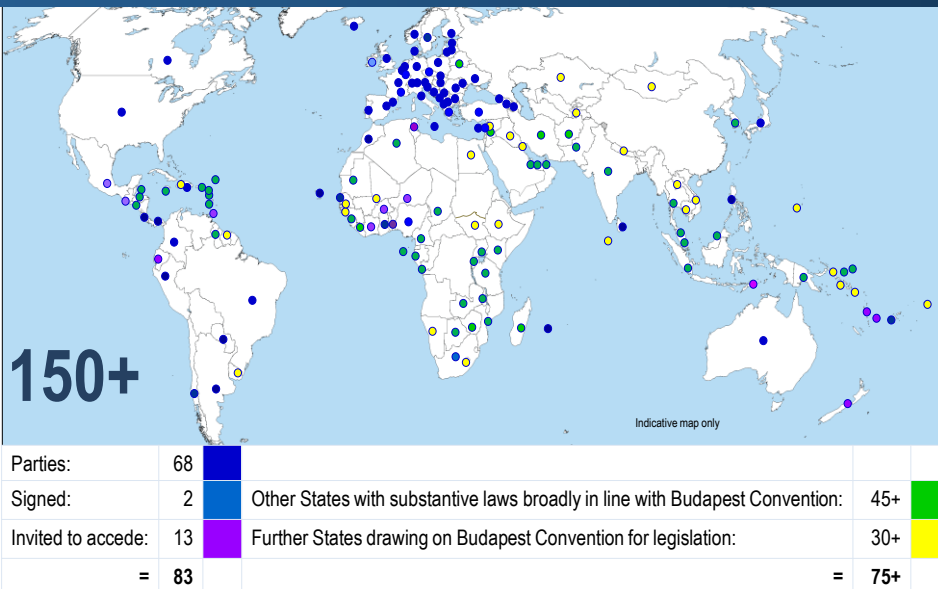
## Content of the Budapest Convention



*Procedural powers and international cooperation for any criminal offence involving evidence on a computer system!*

5

## Reach of the Convention on Cybercrime



6



## The first Protocol on Xenophobia and Racism: about

### ADDITIONAL PROTOCOL TO THE CONVENTION ON CYBERCRIME, CONCERNING THE CRIMINALISATION OF ACTS OF A RACIST AND XENOPHOBIC NATURE COMMITTED THROUGH COMPUTER SYSTEMS (ETS 189)

Opened for signature on 28 January 2003

---

7



## The first Protocol on Xenophobia and Racism: background

- Convention for the Protection of Human Rights and Fundamental Freedoms and its Protocol No. 12 concerning the general prohibition of discrimination
  - United Nations International Convention on the Elimination of All Forms of Racial Discrimination of 21 December 1965 (177 Parties by June 2015)
  - the European Union Joint Action of 15 July 1996 adopted by the Council on the basis of Article K.3 of the Treaty on European Union, concerning action to combat racism and xenophobia
  - Council of Europe: European Commission against Racism and Intolerance, ECRI, established in 2002 ([www.coe.int/ecri](http://www.coe.int/ecri))
  - The Internet offers new opportunities for acts of xenophobia and racism
  - Acts of racism and xenophobia are crimes (not only if speech presents a “clear and present danger”)
- = Need for Protocol to Budapest Convention

---

8



## The first Protocol on Xenophobia and Racism: background

Action Plan

### The fight against violent extremism and radicalisation leading to terrorism

(Adopted by the Committee of Ministers, Brussels, 19 May 2015)

- ▶ Reinforcing international legal framework against terrorism and violent extremism, including implementation of:
  - Convention on the Prevention of Terrorism
  - Additional Protocol on Foreign Terrorist Fighters
  - **Protocol to Budapest Convention on Xenophobia and Racism**
- ▶ Education
- ▶ Addressing radicalisation in prisons
- ▶ Internet: No Hate Speech

---

9



## The first Protocol on Xenophobia and Racism: purpose

### Protocol XR – Preamble

- Need to secure a full and effective implementation of all human rights without any discrimination or distinction;
- **Acts of a racist and xenophobic nature constitute a violation of human rights and a threat to the rule of law and democratic stability;**
- Computer systems offer an unprecedented means of facilitating freedom of expression and communication around the globe;
- **Risk of misuse or abuse of computer systems** to disseminate racist and xenophobic propaganda;
- Need to ensure a **proper balance between freedom of expression and an effective fight against acts of a racist and xenophobic nature;**
- This Protocol is not intended to affect established principles relating to freedom of expression in national legal systems.

---

10



## The first Protocol on Xenophobia and Racism: scope

### Article 2: Definition

*“racist and xenophobic material”* means any written material, any image or any other representation of ideas or theories, which advocates, promotes or incites hatred, discrimination or violence, against any individual or group of individuals, based on race, colour, descent or national or ethnic origin, as well as religion if used as a pretext for any of these factors.

11



## The first Protocol on Xenophobia and Racism: scope

**Article 3 – Dissemination of racist and xenophobic material through computer systems** ► Distributing, or otherwise making available, racist and xenophobic material to the public through a computer system.

**Article 4 – Racist and xenophobic motivated threat** ► Threatening, through a computer system, with the commission of a serious criminal offence as defined under its domestic law,

- (i) persons for the reason that they belong to a group, distinguished by race, colour, descent or national or ethnic origin, as well as religion, if used as a pretext for any of these factors, or
- (ii) (ii) a group of persons which is distinguished by any of these characteristics.

**Article 5 – Racist and xenophobic motivated insult** ► Insulting publicly, through a computer system,

- (i) persons for the reason that they belong to a group distinguished by race, colour, descent or national or ethnic origin, as well as religion, if used as a pretext for any of these factors; or
- (ii) a group of persons which is distinguished by any of these characteristics.

**Article 6 – Denial, gross minimisation, approval or justification of genocide or crimes against humanity** ► distributing or otherwise making available, through a computer system to the public, material which denies, grossly minimises, approves or justifies acts constituting genocide or crimes against humanity ...

**Article 7 – Aiding and abetting**

12



## The first Protocol on Xenophobia and Racism: implementation

Parties		Signatories
Albania	Morocco	Canada
Andorra	Montenegro	Austria
Armenia	Netherlands	Belgium
Bosnia and Herzegovina	North Macedonia	Estonia
Croatia	Norway	Iceland
Cyprus	Paraguay	Italy
Czech Republic	Poland	Liechtenstein
Denmark	Portugal	Malta
Finland	Romania	Slovakia
France	San Marino	Switzerland
Germany	Senegal	South Africa
Greece	Serbia	Türkiye
Latvia	Slovenia	
Lithuania	Spain	
Luxembourg	Sweden	
Moldova	Ukraine	
Monaco		

**Status as at 28 January 2023**

▶ **33 Parties + 12 Signatories**

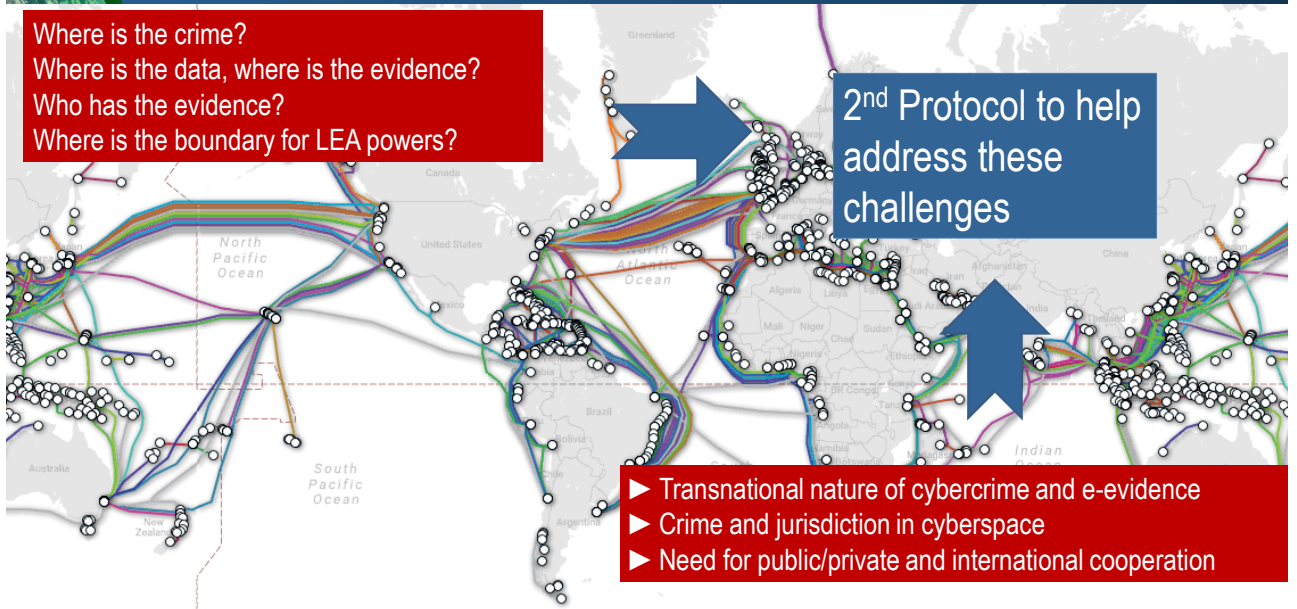
13



## Cybercrime and e-evidence: the problem of territoriality and jurisdiction

Where is the crime?  
 Where is the data, where is the evidence?  
 Who has the evidence?  
 Where is the boundary for LEA powers?

2<sup>nd</sup> Protocol to help address these challenges



- ▶ Transnational nature of cybercrime and e-evidence
- ▶ Crime and jurisdiction in cyberspace
- ▶ Need for public/private and international cooperation

14



## 2<sup>nd</sup> Additional Protocol to the Convention on Cybercrime: content

**Preamble****Chapter I: Common provisions**

- Article 1 Purpose
- Article 2 Scope of application
- Article 3 Definitions
- Article 4 Language

**Chapter II: Measures for enhanced cooperation**

- Article 5 General principles applicable to Chapter II
- Article 6 Request for domain name registration information
- Article 7 Disclosure of subscriber information
- Article 8 Giving effect to orders from another party for expedited production of subscriber information and traffic data
- Article 9 Expedited disclosure of stored computer data in an emergency
- Article 10 Emergency mutual assistance
- Article 11 Video conferencing
- Article 12 Joint investigation teams and joint investigations

**Chapter III – Conditions and safeguards**

- Article 13 Conditions and safeguards
- Article 14 Protection of personal data

**Chapter IV: Final provisions**

- Article 15 Effects of this Protocol
- Article 16 Signature and entry into force
- Article 17 Federal clause
- Article 18 Territorial application
- Article 19 Reservations and declarations
- Article 20 Status and withdrawal of reservations
- Article 21 Amendments
- Article 22 Settlement of disputes
- Article 23 Consultations of the Parties and assessment of implementation
- Article 24 Denunciation
- Article 25 Notification

15



## 2<sup>nd</sup> Additional Protocol to the Convention on Cybercrime: next

### 2<sup>nd</sup> Additional Protocol to the Convention on Cybercrime on enhanced cooperation and disclosure of electronic evidence (CETS 224)

Signatories (status 29 January 2023):

- |               |                     |
|---------------|---------------------|
| 1. Andorra    | 18. Luxembourg      |
| 2. Austria    | 19. Montenegro      |
| 3. Belgium    | 20. Moldova         |
| 4. Bulgaria   | 21. Morocco         |
| 5. Chile      | 22. Netherlands     |
| 6. Colombia   | 23. North Macedonia |
| 7. Costa Rica | 24. Portugal        |
| 8. Croatia    | 25. Romania         |
| 9. Estonia    | 26. Serbia          |
| 10. Finland   | 27. Slovenia        |
| 11. France    | 28. Spain           |
| 12. Germany   | 29. Sri Lanka       |
| 13. Greece    | 30. Sweden          |
| 14. Iceland   | 31. Ukraine         |
| 15. Italy     | 32. United Kingdom  |
| 16. Japan     | 33. USA             |
| 17. Lithuania |                     |

**Next:**

- ▶ Signature by other Parties
- ▶ Ratification (5 needed for entry into force)
- ▶ Capacity building

16



## Addressing XR through the framework of the Convention on Cybercrime

