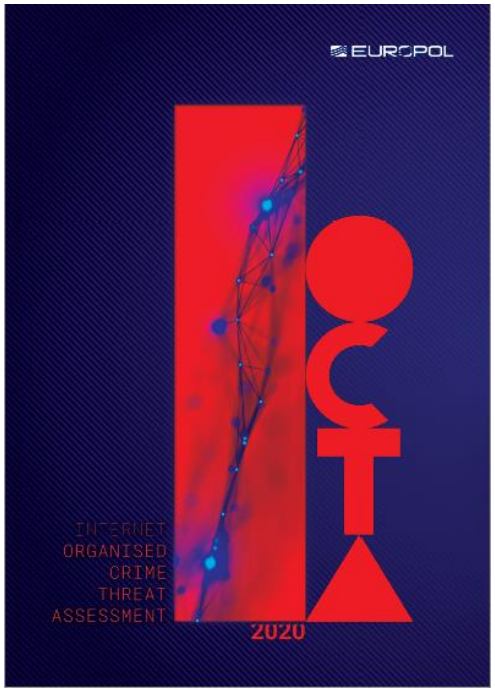
THE BUDAPEST CONVENTION ON CYBERCRIME AND ELECTRONIC EVIDENCE: ITS ELEMENTS AND BENEFITS

Catalina STROE
Programme manager
Cybercrime Programme Office

Cybercrime global trends

- **Cyber-dependent crime**
  - Ransomware, malware, DDoS
- **Online child sexual exploitation**
- **Computer-related payment frauds**
  - BEC and terminal attacks on the rise
- **Criminal abuse of Darknets**
  - On-line criminal markets, CaaS
  - Use of cyber to support terrorism
- **Fake news, Deepfake and Election interference**
- **Intellectual property and Internet piracy**
- **Cross-cutting issues**
  - COVID-19 demonstrating criminal opportunism



Challenges for Criminal Justice Authorities

- **Heterogeneous legal frameworks, often not in line with international standards**

- **Scale and quantity of criminal conducts online, data, devices, users and victims vs. limited capacities and resources**

- **Identification, collection and use of electronic evidence and admissibility issues – Standardization**

Cybercrime and e-evidence legislation: issues at stake

Cybercrime and crimes involving e-evidence

- challenges to rights of individuals

Obligation to effectively protect against crime

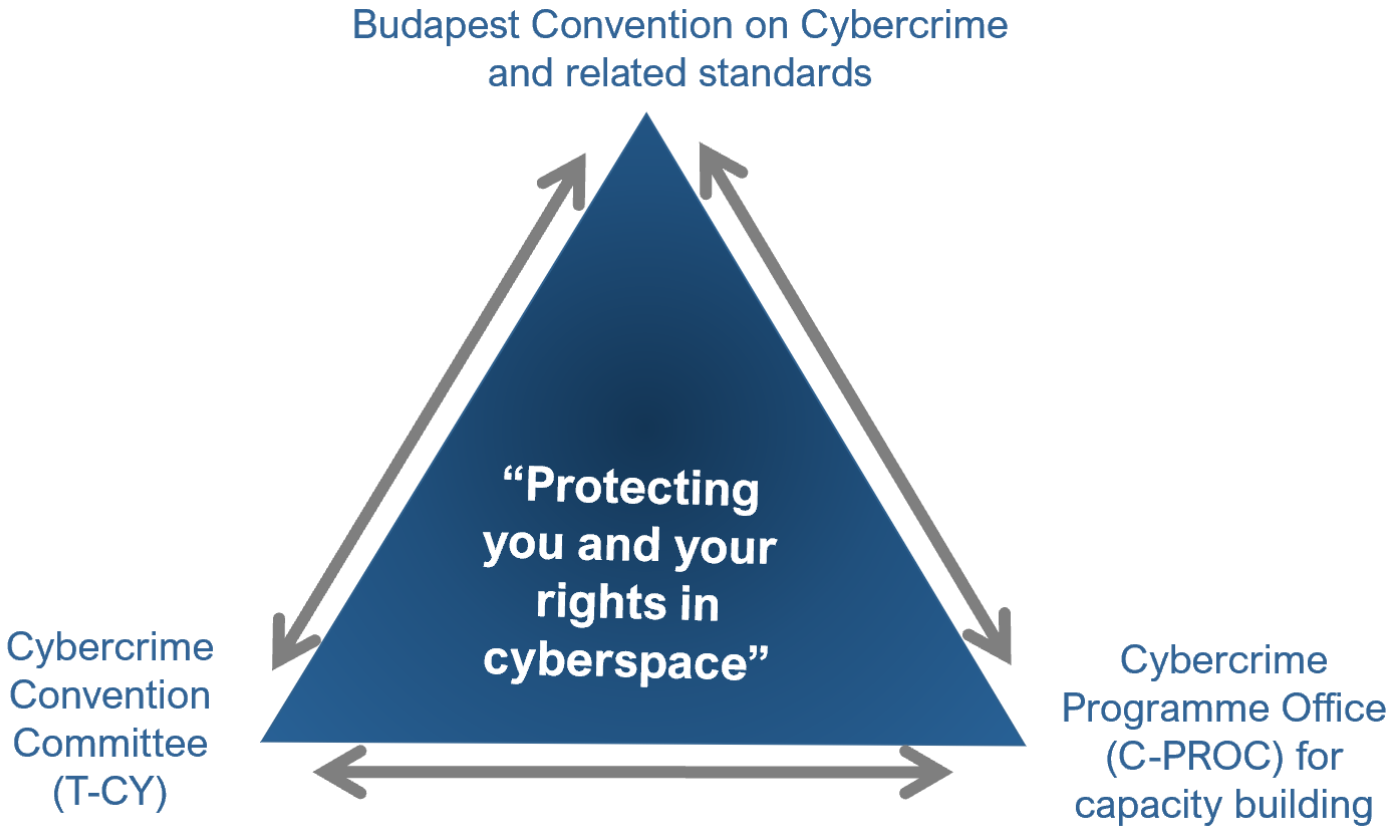
Criminalising cybercrime and other offences in cyberspace

- Risks of overcriminalisation
- Risks of undercriminalisation

Investigating cybercrime and securing electronic evidence

- Challenges to effectively securing evidence
- Rule of law requirements for investigative measures

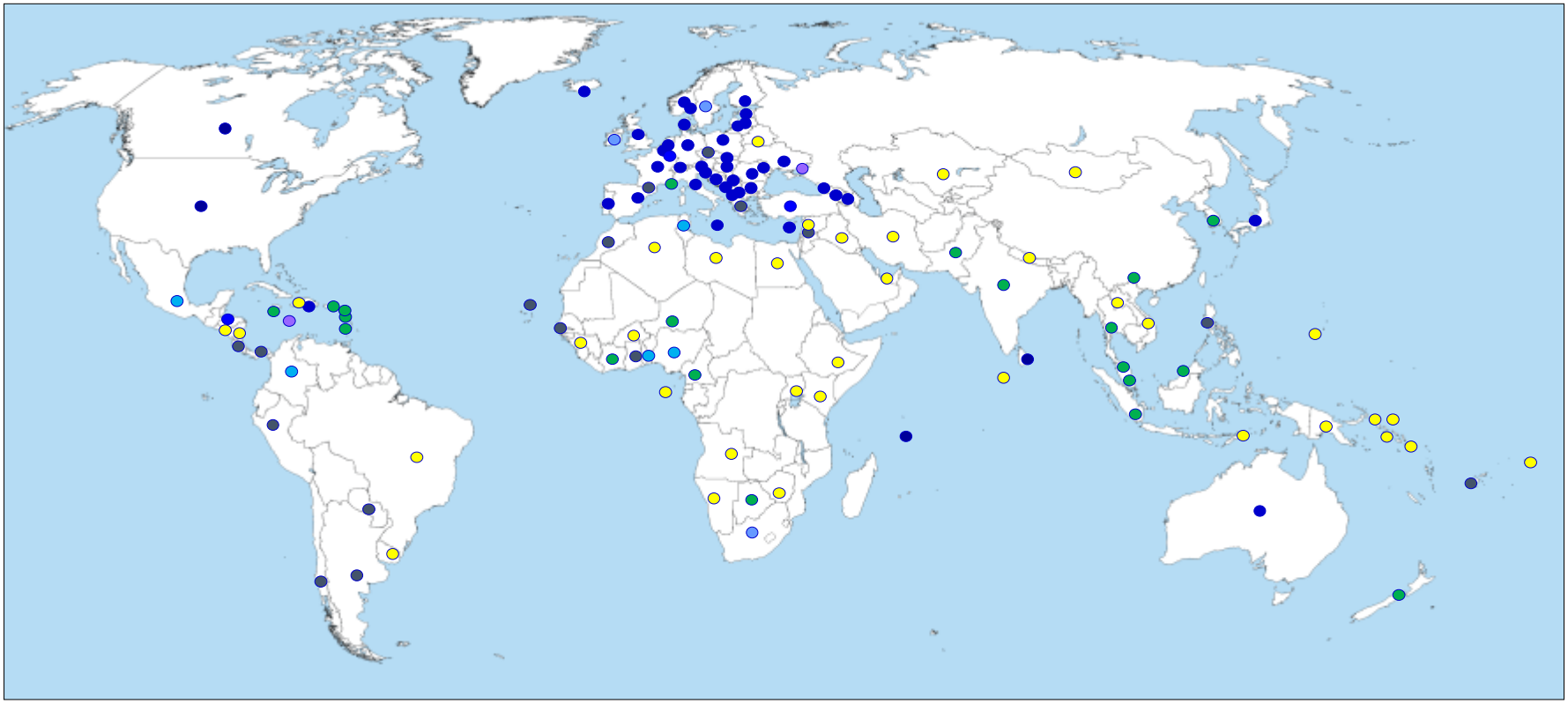
The approach of Council of Europe



Council of Europe's Convention on Cybercrime – The Budapest Convention

- **Negotiated by Council of Europe (47 members), Canada, Japan, South Africa and USA**
- **Opened for signature on 23 November 2001 in Budapest**
- **Protocol on Xenophobia and Racism via computer systems (2003) and Protocol on enhanced co-operation and disclosure of electronic evidence (2022)**
- **Open for accession by any State – 68 Accessions/ Ratifications**
- **As of today, the only international Treaty on cybercrime and electronic evidence**
- **Followed by Cybercrime Convention Committee (T-CY)** – Guidance Notes, Interpretation, Monitoring

Reach of the Budapest Convention



Budapest Convention

Ratified/acceded: 68

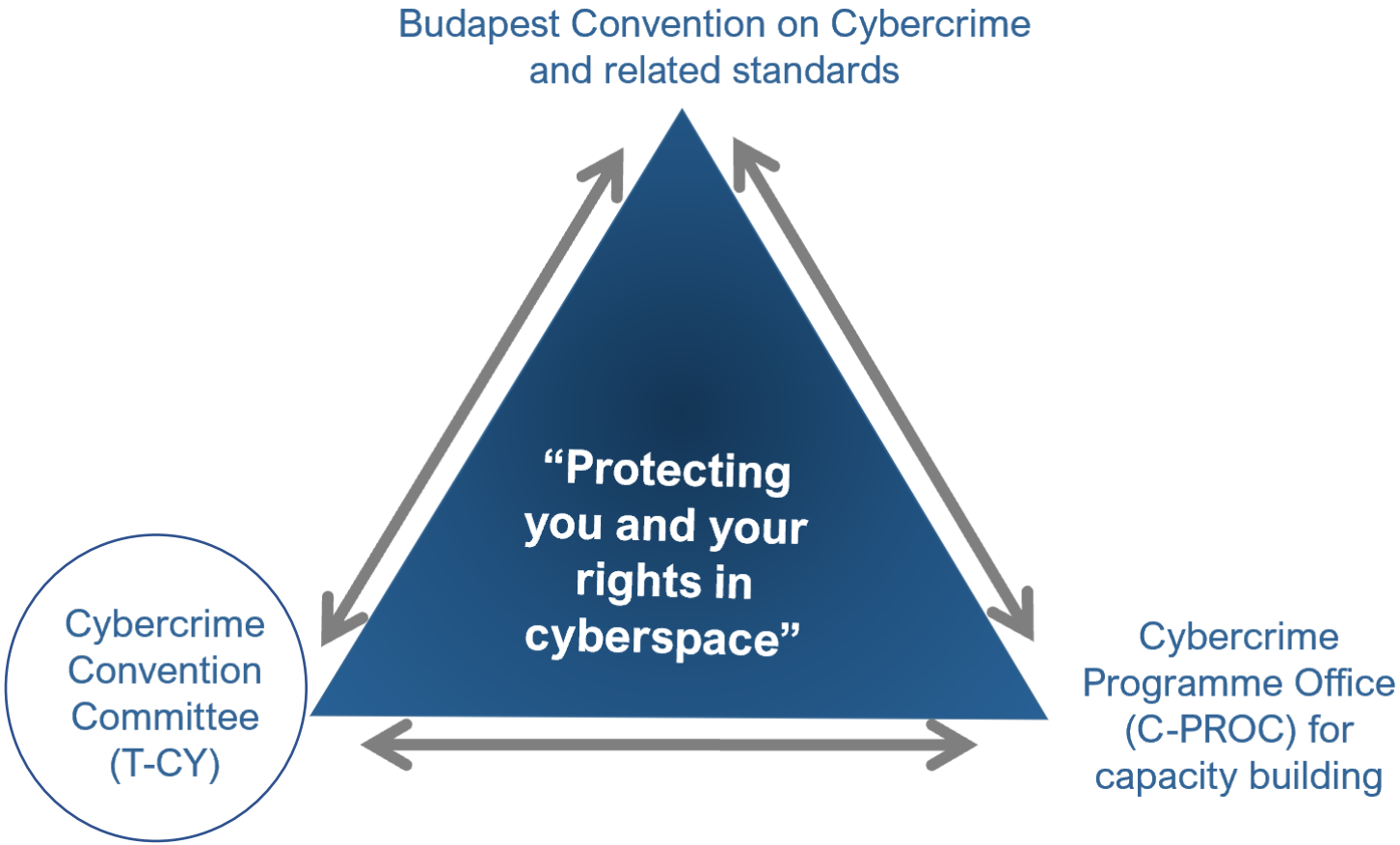
Signed: 2

Invited to accede: 17

Other States with laws/draft laws largely in line with Budapest Convention = 45

Further States drawing on Budapest Convention for legislation = 25+

The approach of Council of Europe



The Cybercrime Convention Committee (T-CY)

Established under Article 46 Budapest Convention

Membership (March 2023):

- **68 Members** (State Parties)
- **19 Observer States**
- **12 organisations**
  (African Union Commission, Commonwealth Secretariat, ENISA, European Union, Eurojust, Europol, INTERPOL, ITU, OAS, OECD, OSCE, UNODC)

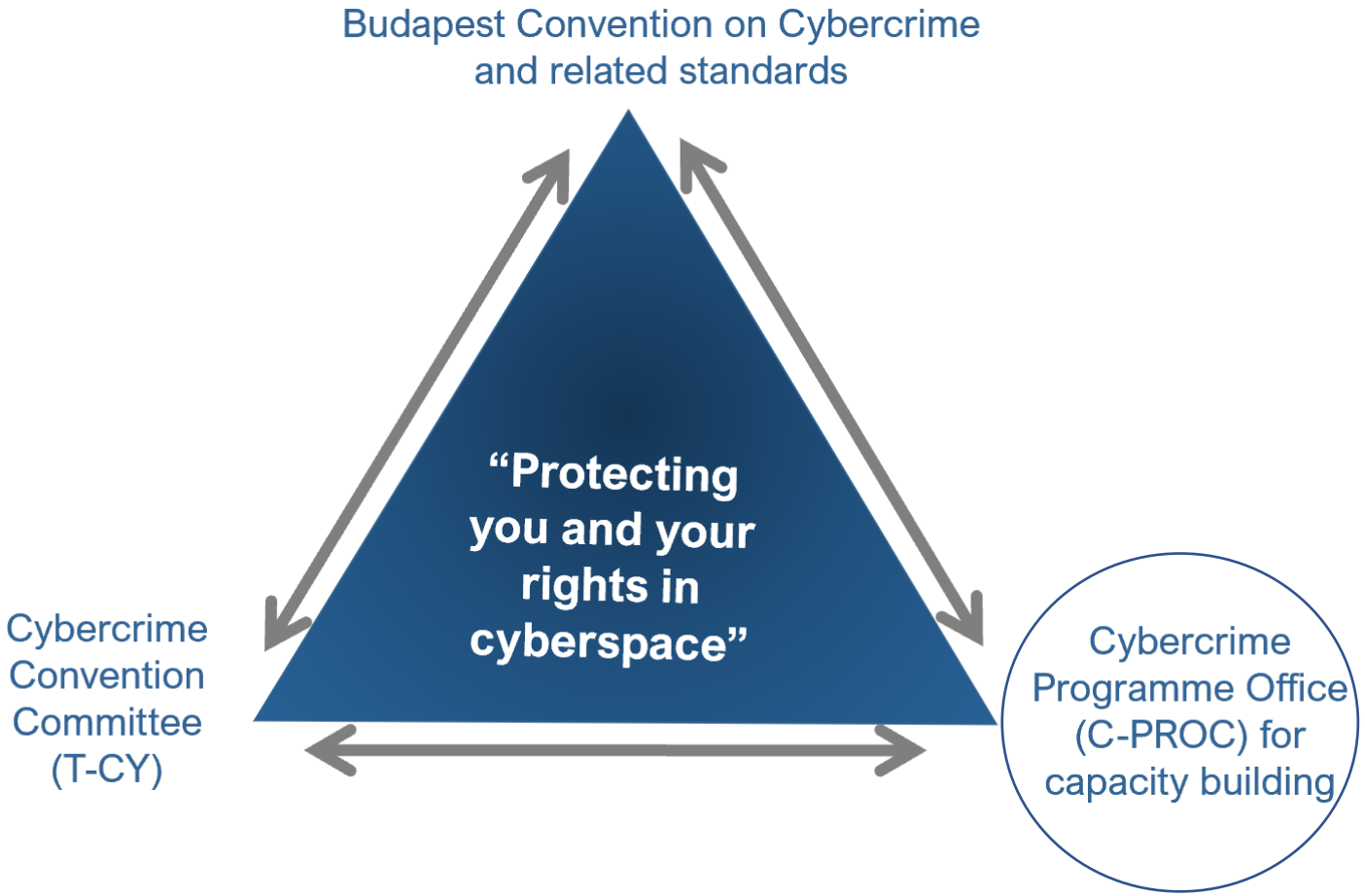
Functions:

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

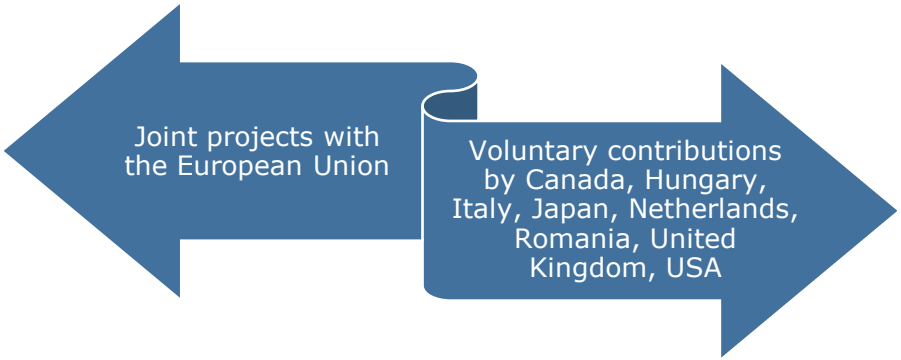
Two plenaries/year as well as Bureau and working group meetings

- **An effective follow up mechanism**
- **The T-CY appears to be the main inter-governmental body on cybercrime matters internationally**

The approach of Council of Europe



Cybercrime Programme Office (C-PROC)



In a nutshell

- The convention improves domestic criminalisation and criminal procedure as well as international cooperation
- It covers electronic evidence in physical-world crimes as well as classic cybercrime
- It makes it easier to obtain data from foreign providers, especially the big ones
- It was always intended to be open to any country. It has 68 Parties, including Cabo Verde, Ghana, Morocco, Mauritius, Nigeria, Senegal. Benin, Burkina Faso, Cameroon, Côte d'Ivoire, Niger, Sierra Leone and Tunisia have been invited to accede. South Africa is a signatory

In a nutshell , cont'd.

- It's a current, working treaty used every day. Its text is technology-neutral
- The Council of Europe offers a vast cybercapacity building program (free of charge) driven by countries' requests
- Participation in COE activities, even before a country becomes a Party, provides a network of helpful colleagues
- The process to become a Party is straightforward

Joining the Budapest Convention

Treaty open for accession (article 37)

Phase 1:

- A country with legislation in place or advanced stage
- Letter from Government to CoE expressing interest in accession
- Consultations (CoE/Parties) in view of decision to invite
- Invitation to accede

Phase 2:

- Domestic procedure (e.g. decision by national Parliament)
- Deposit of the instrument of accession

The Budapest Convention on Cybercrime
BENEFITS of membership in the Convention

Substantive law – provides for a minimum standard of criminalisation of specific illegal acts, thus offering a common understanding and harmonised legislation between the Parties

Procedural powers – provides for a minimum set of specific procedural measures for obtaining electronic evidence, therefore offering a common operational standard strategy between the Parties in investigating specific crimes committed with the use of a computer system or traditional crimes that involve electronic evidence

Moreover, the Convention provides a **legal basis for international cooperation** on cybercrime and electronic evidence. Chapter III of the treaty comprises general and specific provisions for cooperation among Parties "to the widest extent possible" not only with respect to cybercrime (offences against and by means of computers) but also with respect to any crime involving electronic evidence

Membership in the Budapest Convention means membership in **networks of practitioners** – the 24/7 network of contact points among them – and thus the ability to engage in trusted cooperation.

Parties to the Convention are able to improve their **cooperation with the private sector**. Indications are that private sector entities are more likely to cooperate with criminal justice authorities of Parties to the Convention given that Parties need to have a domestic legal framework on cybercrime and electronic evidence in place, including the human rights safeguards of Article 15.

BENEFITS of membership in the Convention

Parties are **members of the Cybercrime Convention Committee,** the T-CY. They share information and experience, assess implementation of the Convention, or prepare templates for mutual assistance requests and other tools to facilitate the application of the treaty to counter cybercrime more effectively

Through the T-CY, Parties contribute to the further evolution of the Budapest Convention, for example, in the form of Guidance Notes or negotiation of additional protocols. Thus, even if a State did not participate in the negotiation of the original treaty, a new Party is able to participate in the **negotiation of future instruments such as the** 2nd Additional Protocol on enhanced international cooperation and access to electronic evidence

States requesting accession or having acceded may become **priority countries for capacity building** programmes. Such technical assistance is to facilitate full implementation of the Convention and to enhance the ability to cooperate internationally. Donors are consistently providing resources to support countries in this undertaking, in particular through the Cybercrime Programme Office of the Council of Europe (C-PROC).

Octopus Community

Octopus Community

Platform for information sharing and cooperation on cybercrime and electronic evidence

- **Country Wiki**
- **Training Materials**
- **Newsletters**
- **Webinars**

Human Rights Education for Legal Professionals

Subscribe to our Newsletters

https://www.coe.int/en/web/octopus/home

Contact:

Catalina STROE
Programme Manager, Cybercrime Programme Office of the Council of Europe (C-PROC)
Bucharest, ROMANIA
Catalina.STROE@coe.int

Find out more:
https://www.coe.int/en/web/cybercrime/glacyplus

Useful links

- The Budapest Convention and its Explanatory Report (in numerous languages) Full list (coe.int)

- Other materials, usually in English and French:
  - Guidance notes Guidance Notes (coe.int)
  - Protocol on Xenophobia and Racism via Computer Systems Full list (coe.int)
  - Protocol on enhanced international cooperation https://www.coe.int/en/web/cybercrime/second-additional-protocol
  - Information about the Council of Europe's capacity-building programs Worldwide Capacity Building (coe.int)
  - Home page of the COE's cybercrime activities Action against Cybercrime (coe.int)