the future

Second Additional Protocol

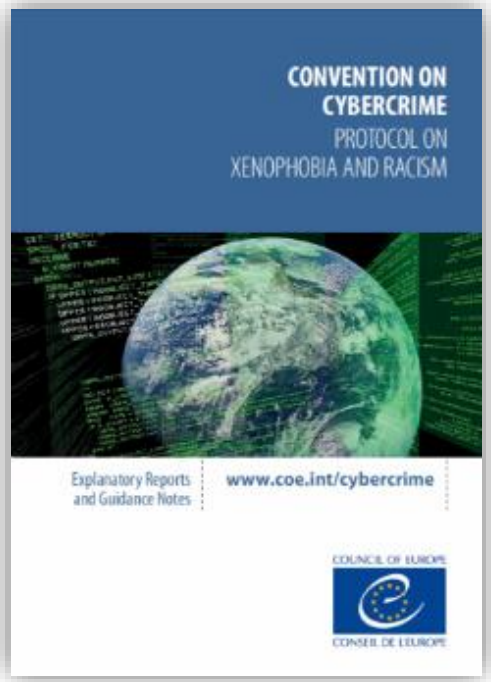
to the

Budapest Convention

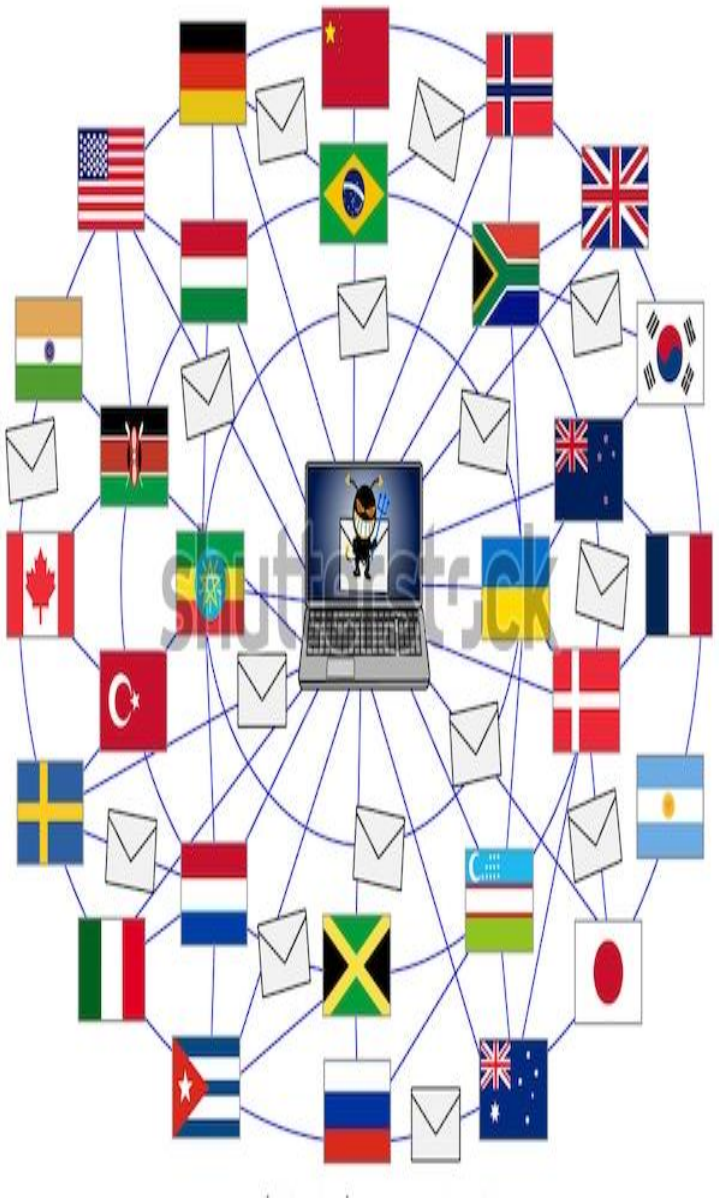
“Second Additional Protocol to the Convention on Cybercrime on enhanced co-operation and disclosure of electronic evidence”

Budapest Convention

- **opened for signature** in 2001 and in **force** in 2004
- currently (December 2023) **68 Parties**
- **other 23** other States have already signed it or been invited to accede
- **the most important reference around the world** on cybercrime and electronic evidence



- **2003: First Additional Protocol** (on the criminalization of acts of a racist and xenophobic nature committed through computer systems) in force since 2006
- the Convention is still a **valid and updated legal framework**
- the evolution of information and communication technologies requires the adoption of some **new specific solutions**

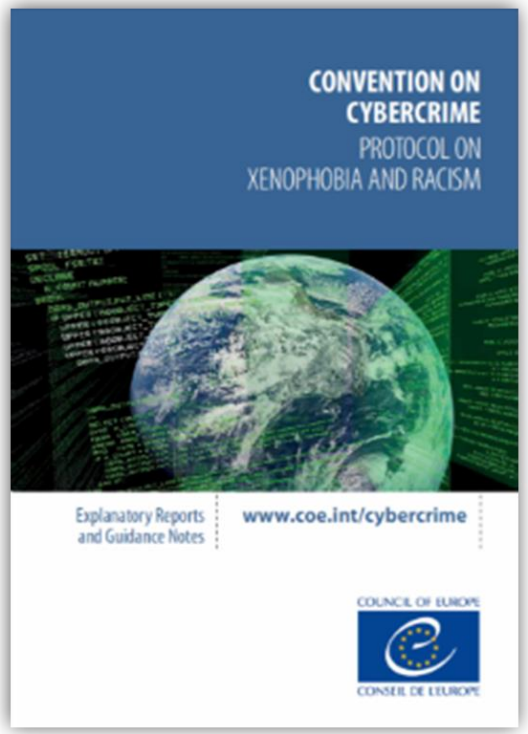


a new landscape

- information and communication **technologies constantly evolve**
- mankind benefits from many **positive outcomes** from that permanent process
- but also, **several challenges**
- regarding criminal justice, a number of them respect **rule of law** and gathering electronic evidence

a new environment

- traditional **mutual legal assistance tools** and channels have **limited effectiveness**
- a number of **national laws** already allow their national authorities to **transborder access to data**
- **unilaterally**
- **without the knowledge and formal consent of the other country**



- **20 years** have gone after the drafting of the Budapest Convention
- regarding the penal substantive aspects, **the Convention remains fully valid and updated**, as a reference
- **with respect to the operational side**, in view of the new introduced technologies, **some specific solutions are needed**

the famous *cloud*

- **evidence in remote** servers
- in **other** countries
- **multiple or unknown** locations

new difficulties (territoriality and jurisdiction)

- **where is the evidence** (both physically and legally)?
- which **legal framework** applies?
- **which entity or service provider** controls the sought information, in case?

Jurisdiction in cyberspace: Amsterdam conference concludes

AMSTERDAM, NETHERLANDS | 7-8 MARCH 2016

Effective criminal justice access to data in the cloud is a priority of the Netherlands presidency of the European Union. The conference "Crossing borders: jurisdiction in cyberspace" was held on 7-8 March 2016 in Amsterdam. The aim was to move towards solutions in terms of more efficient mutual legal assistance, public/private sharing of data and situations where the location of data or data controllers is unknown. The conference drew, among other things, on the work of the Cloud

the Amsterdam Conference

- March 2016
- on **jurisdiction in cyberspace**
- effective criminal justice **access to data in the cloud**
- priority of the European Union

- objective: to explore possible concrete solutions in terms of **more efficient MLA**
- **public/private** sharing of data
- identifying situations where the **location of data is unknown** – in view of finding new approaches to this new reality

Transborder Group

- the landscape: each day **more crime takes place online** – thus **more evidence is online**
- most of it is stored in **foreign or unknown jurisdictions** – that is, not in the State that investigates
- in practice, these crimes **violate human rights**, privacy and other individual rights
- and **cannot be effectively investigated** – thus, criminals are not punished

- 2011 – sub-group (of the T-CY), on **jurisdiction and transborder access** to data
- objective: to examine the possible use of **transborder investigative measures** on the Internet
- explore the **challenges to transborder investigations** (jurisdiction and sovereignty)
- **develop and instrument to further regulate** the transborder access to data

Cloud Evidence Group

- **consider differently subscriber information from traffic and content data**, regarding the respective process of obtaining
- recognize that in some situations it is **impossible, in practice, to know the location** of the physical storage of certain computer data.
- no international rules at this respect – thus, States are increasingly introducing the **practice of unilateral transborder access to data**
- need to consider expedited disclosure of data in **emergency situations**
- MLA process is not able to **fulfil the needs** of gathering electronic evidence

some recommendations for consideration by the T-CY

Octopus Conference 2016

Cybercrime@Octopus: News

Octopus Conference key messages

STRASBOURG | 18/11/2016

Some 300 cybercrime experts from 90 countries, 12 international and 40 private sector, civil society organisations and academia met at the Council of Europe in Strasbourg, France, from 16 to 18 November 2016 for the Octopus 2016 Conference on cooperation against cybercrime.

The Conference was opened by Thorbjørn Jagland, Secretary General of the Council of Europe, and commenced with a special session on the occasion of the 15th anniversary of the Budapest Convention on Cybercrime. Andorra deposited the instrument of ratification of the Convention during this session to become the 50th Party to this treaty.

OCTOPUS 2016 messages

- there is a **general obligation of States** of **protecting** society and individuals against crime
- in view of that, **access to evidence on servers in the cloud** (in foreign, unknown or multiple jurisdictions) is increasingly more **necessary** for the purposes of regular criminal investigations
- **voluntary cooperation by international service providers** (namely regarding subscriber information and in emergency situations) is most valuable but also raises concerns
- a Protocol to the Budapest Convention **is necessary**

the challenge

In June 2017, the T-CY Committee agreed on the **Terms of Reference** for the preparation of the Second Additional Protocol to the Budapest Convention.
The negotiation process **started in September 2017**, and it was originally expected to be completed by December 2019.
It was postponed and just ended in **May 2021.**

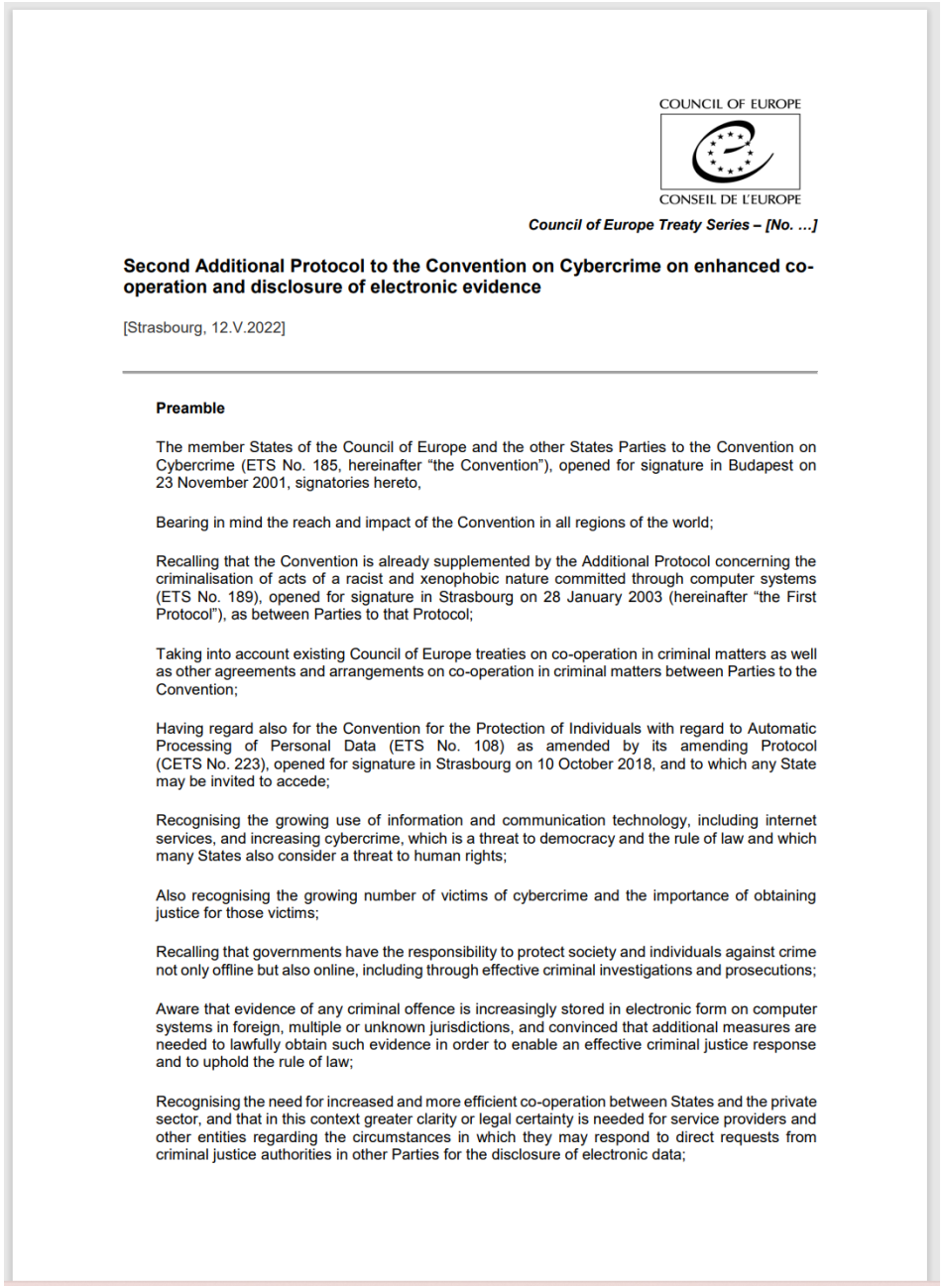
- the T-CY established the "**Protocol Drafting Plenary**" (national experts appointed by the Parties to the Budapest Convention)
- task: **drafting a proposal** of a protocol
- besides, the "**Protocol Drafting Group**", a smaller working group, in charge of working on the concrete text of the protocol, in between plenary sessions
- In practice, **discussions** about the protocol **aimed to answer** questions such as
  - how to get **information from subscribers efficiently**
  - how to obtain data (evidence) in **emergency situations**
  - how to draw **more effective** forms of **mutual legal assistance**

19 and 20 September 2017
The **first meeting** of the *Protocol Drafting Group* was held in Strasbourg

The **draft Protocol** was **concluded in May 2021** by more than **100 experts of 66 countries**

Opened for signature:
12 May 2022

(December 2023)
43 States Signed
2 States Ratified



COUNCIL OF EUROPE

CONSEIL DE L'EUROPE

Council of Europe Treaty Series – [No. …]

Second Additional Protocol to the Convention on Cybercrime on enhanced co-operation and disclosure of electronic evidence

[Strasbourg, 12.V.2022]

Preamble

The member States of the Council of Europe and the other States Parties to the Convention on Cybercrime (ETS No. 185, hereinafter "the Convention"), opened for signature in Budapest on 23 November 2001, signatories hereto,

Bearing in mind the reach and impact of the Convention in all regions of the world;

Recalling that the Convention is already supplemented by the Additional Protocol concerning the criminalisation of acts of a racist and xenophobic nature committed through computer systems (ETS No. 189), opened for signature in Strasbourg on 28 January 2003 (hereinafter "the First Protocol"), as between Parties to that Protocol;

Taking into account existing Council of Europe treaties on co-operation in criminal matters as well as other agreements and arrangements on co-operation in criminal matters between Parties to the Convention;

Having regard also for the Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data (ETS No. 108) as amended by its amending Protocol (CETS No. 223), opened for signature in Strasbourg on 10 October 2018, and to which any State may be invited to accede;

Recognising the growing use of information and communication technology, including internet services, and increasing cybercrime, which is a threat to democracy and the rule of law and which many States also consider a threat to human rights;

Also recognising the growing number of victims of cybercrime and the importance of obtaining justice for those victims;

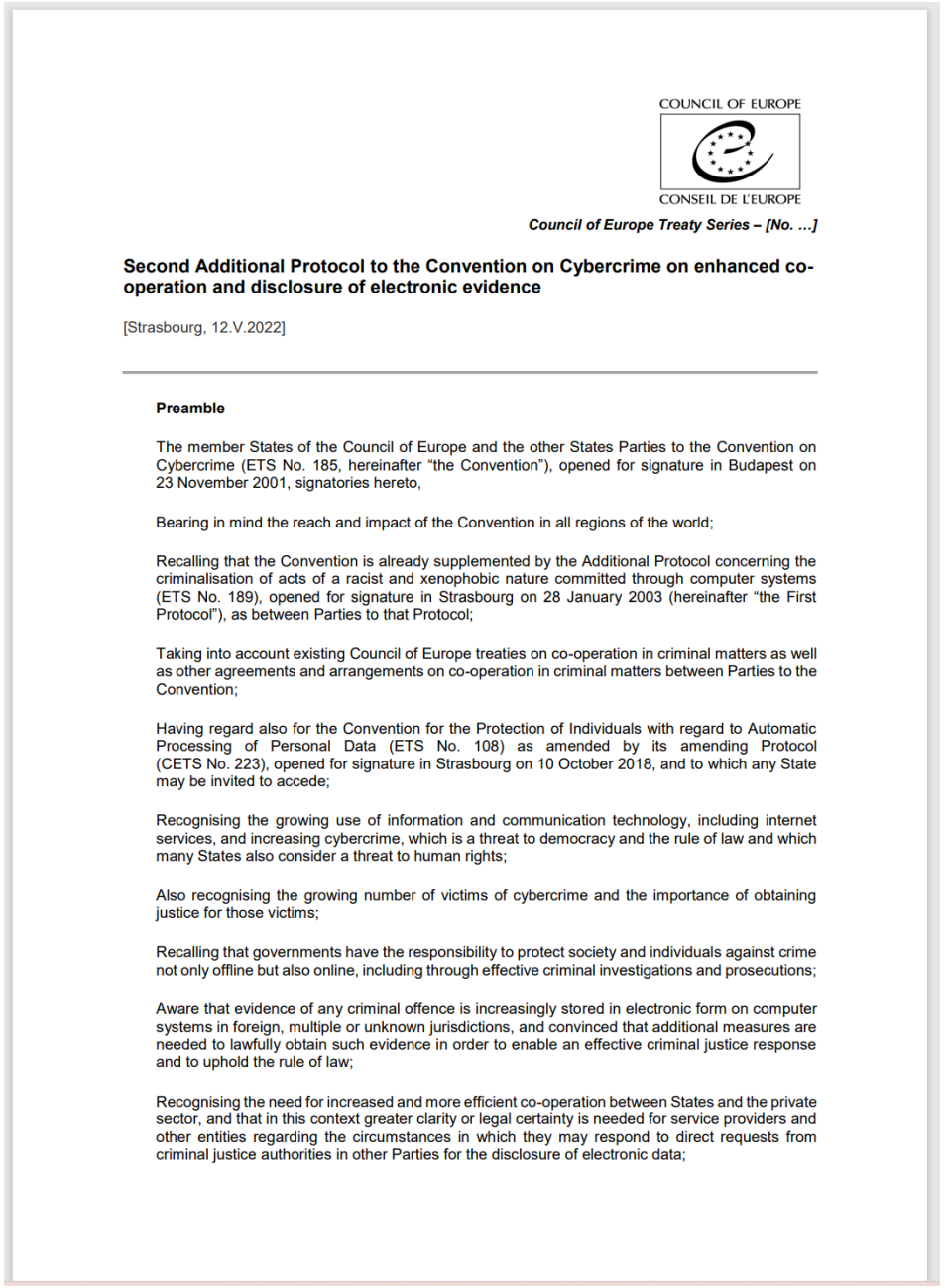
Recalling that governments have the responsibility to protect society and individuals against crime not only offline but also online, including through effective criminal investigations and prosecutions;

Aware that evidence of any criminal offence is increasingly stored in electronic form on computer systems in foreign, multiple or unknown jurisdictions, and convinced that additional measures are needed to lawfully obtain such evidence in order to enable an effective criminal justice response and to uphold the rule of law;

Recognising the need for increased and more efficient co-operation between States and the private sector, and that in this context greater clarity or legal certainty is needed for service providers and other entities regarding the circumstances in which they may respond to direct requests from criminal justice authorities in other Parties for the disclosure of electronic data;

The Protocol includes

- formal **standard provisions** (such as on its purpose, scope of application, effects, or territorial application, among many other)
- **conditions and safeguards** and a very detailed regime on **protection of personal data**
- from a substantive point of view
  - some **very innovative** provisions
  - provisions similar to **provisions also existent in other treaties** (transpose into the cyber environment measures already applicable to other forms of criminality)



COUNCIL OF EUROPE

CONSEIL DE L'EUROPE

Council of Europe Treaty Series – [No. …]

Second Additional Protocol to the Convention on Cybercrime on enhanced co-operation and disclosure of electronic evidence

[Strasbourg, 12.V.2022]

Preamble

The member States of the Council of Europe and the other States Parties to the Convention on Cybercrime (ETS No. 185, hereinafter "the Convention"), opened for signature in Budapest on 23 November 2001, signatories hereto,

Bearing in mind the reach and impact of the Convention in all regions of the world;

Recalling that the Convention is already supplemented by the Additional Protocol concerning the criminalisation of acts of a racist and xenophobic nature committed through computer systems (ETS No. 189), opened for signature in Strasbourg on 28 January 2003 (hereinafter "the First Protocol"), as between Parties to that Protocol;

Taking into account existing Council of Europe treaties on co-operation in criminal matters as well as other agreements and arrangements on co-operation in criminal matters between Parties to the Convention;

Having regard also for the Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data (ETS No. 108) as amended by its amending Protocol (CETS No. 223), opened for signature in Strasbourg on 10 October 2018, and to which any State may be invited to accede;

Recognising the growing use of information and communication technology, including internet services, and increasing cybercrime, which is a threat to democracy and the rule of law and which many States also consider a threat to human rights;

Also recognising the growing number of victims of cybercrime and the importance of obtaining justice for those victims;

Recalling that governments have the responsibility to protect society and individuals against crime not only offline but also online, including through effective criminal investigations and prosecutions;

Aware that evidence of any criminal offence is increasingly stored in electronic form on computer systems in foreign, multiple or unknown jurisdictions, and convinced that additional measures are needed to lawfully obtain such evidence in order to enable an effective criminal justice response and to uphold the rule of law;

Recognising the need for increased and more efficient co-operation between States and the private sector, and that in this context greater clarity or legal certainty is needed for service providers and other entities regarding the circumstances in which they may respond to direct requests from criminal justice authorities in other Parties for the disclosure of electronic data;

More relevant provisions of the Protocol, in substance

- Languages of requests
- Request for domain name registration information
- Direct disclosure of subscriber information
- Giving effect to orders from another Party for expedited production of data
- Request for domain name registration information
- Expedited disclosure of stored computer data in an emergency
- Emergency MLA
- Video conferencing
- Joint investigation teams and joint investigations

Languages of requests

- when requesting assistance from other States in a criminal investigation, one of the **more important practical obstacles is language**
- currently, most of the requests must be sent in the **language of the requested** State
- This provision allows one State to submit a request in **any other language** (for example English), if such language is acceptable to the requested State
- It **encourages flexibility**, allowing States to communicate in most effective manners (regarding the language)

Request for domain name registration information

- **Direct cooperation procedure** between the **authorities of a Party** and an entity that provides domain name registration services in the territory of another Party
- for information on Internet domain name registrations
- these data are usually indispensable, as a **first step in many investigations**
- and to determine **where to direct requests for international cooperation**

Disclosure of Subscriber Information

- legal framework to an investigative procedure of **direct cooperation** between the competent authorities for criminal investigation of one State and a **service provider in the territory of another State**
- only applies to specific criminal investigations or proceedings
- limited to obtain stored **subscriber information**

Giving effect to orders from another Party for expedited production of data

- procedural mechanism to **give effectiveness to orders issued by the authorities from on State**, to service providers in another State
- **compelling mechanism** to produce data
- limited to **subscriber information and traffic data**
- only in the context of a specific **criminal investigations** or proceedings

Expedited disclosure of stored computer data in an emergency

- this provision focuses **emergency situations related to a criminal investigation**.
- national authorities from one State may request and **obtain immediate assistance** from a provider in another State
- expedited disclosure of computer data, **without a request for mutual assistance**

Emergency Mutual Legal Assistance

- when during a criminal investigation, there is the need to **obtain immediate assistance**
- used when, for formal reasons, namely because of the **nature of the sought information**, the procedure cannot be simplified, and the process must follow the rules of mutual legal assistance
- introduces a legal framework of an **expedited procedure for mutual assistance requests**, in emergency situations
- emergency situations are defined as situations in which there is a **significant and imminent risk to the life or safety** of any natural person

Video conferencing

- along **similar provisions in other international instruments**, regarding other types of criminality
- in general, it allows **testimony and other statements to be taken by video conference** of witnesses or experts, or even suspects

Joint investigation teams and joint investigations

- another provision **already included in other international instruments**, regarding other types of criminality
- in this case, the provision is **specifically drafted to envisage investigations and prosecutions related to cybercrime** and electronic evidence

Thank you

Questions?

https://www.coe.int/en/web/cybercrime