Digital Actors meeting

The future of co-operation under the Second Additional Protocol: the role of private partners within cybercrime cases

Presentation prepared by Cybercrime Division

Strasbourg, France, 15 May 2025

Co-funded by the European Union
EUROPEAN UNION
COUNCIL OF EUROPE
CONSEIL DE L'EUROPE
Co-funded and implemented by the Council of Europe

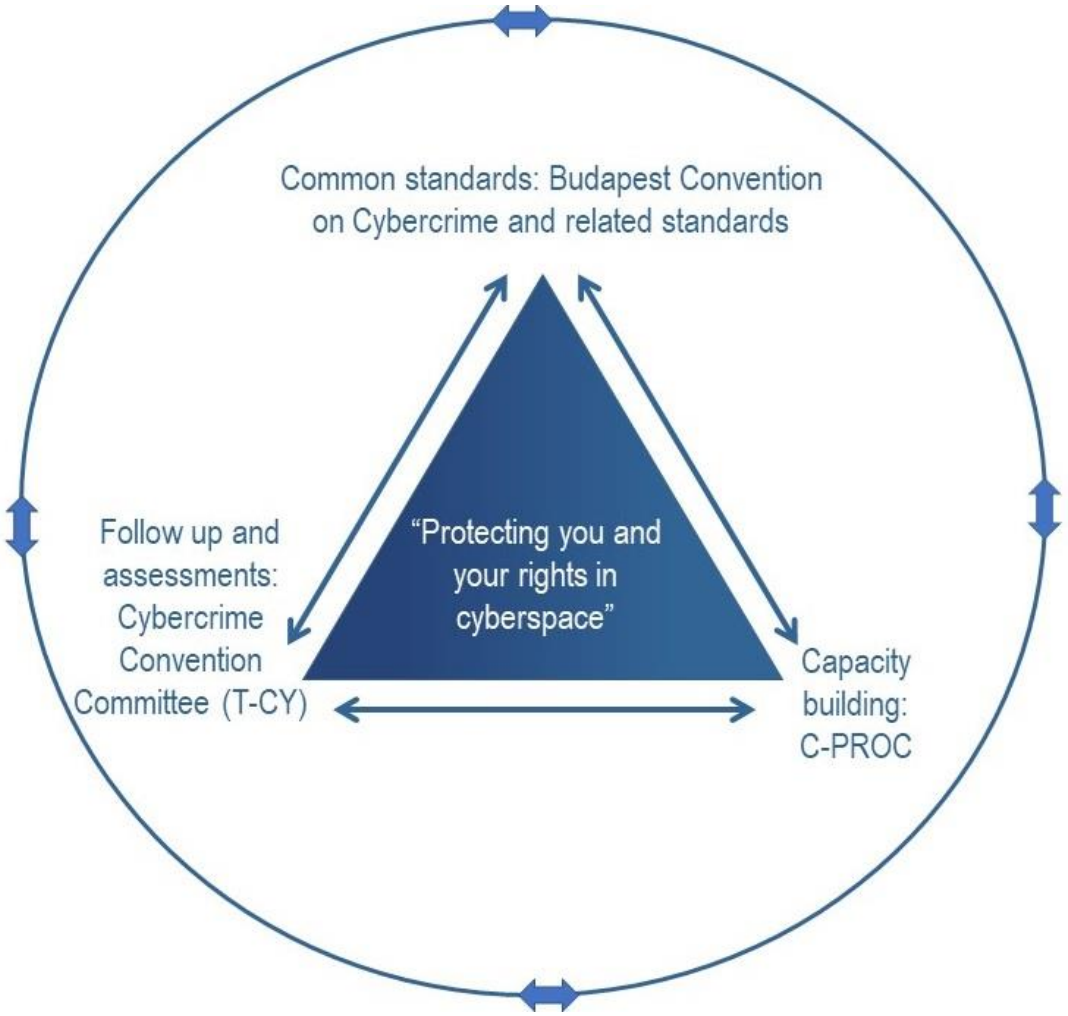
The framework of the Convention on Cybercrime (Budapest Convention)

- Budapest Convention on Cybercrime (2001)

  1. Specific offences
  2. Procedural powers
  3. International cooperation

- 1st Protocol on Xenophobia and Racism via Computer Systems (2003)
- 2nd Protocol on enhanced cooperation and disclosure of electronic evidence (2022)
- Guidance Notes

By March 2025: **78 Parties and 17 "Observer States"**



Rationale: Why the Second Protocol?

Cybercrime: Threat to

- Human rights
- Democracy
- Rule of law

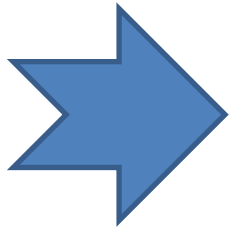
Positive obligations:

- Provide the means to protect the rights of individuals, also against crime

Problem:

- Proliferation of cybercrime
- Any type of crime now involving e-evidence
- Evidence somewhere in foreign, multiple, shifting or unknown jurisdictions
- Effective means not available to obtain the disclosure of e-evidence

- Less than 0.1% of offences in cyberspace lead to prosecutions and convictions
- Do victims obtain justice?



2nd Protocol to help address these challenges

Rationale: Why the Second Protocol?

Specific issues:

- How to obtain subscriber information efficiently?
- How to cooperate directly with a service provider in another Party?
- How to obtain WHOIS data (domain name registration information) from registrars?
- How to obtain stored data, including content, in an emergency situation?
- How to make mutual assistance more effective?
- How to reconcile efficient and effective measures with rule of law and data protection requirements?

Example subscriber information

"Subscriber information" is data most often needed in a criminal investigation (to identify the owner of a webmail account, user of an IP address)

►How to obtain it from a provider in another Party?

Content of the Second Protocol

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

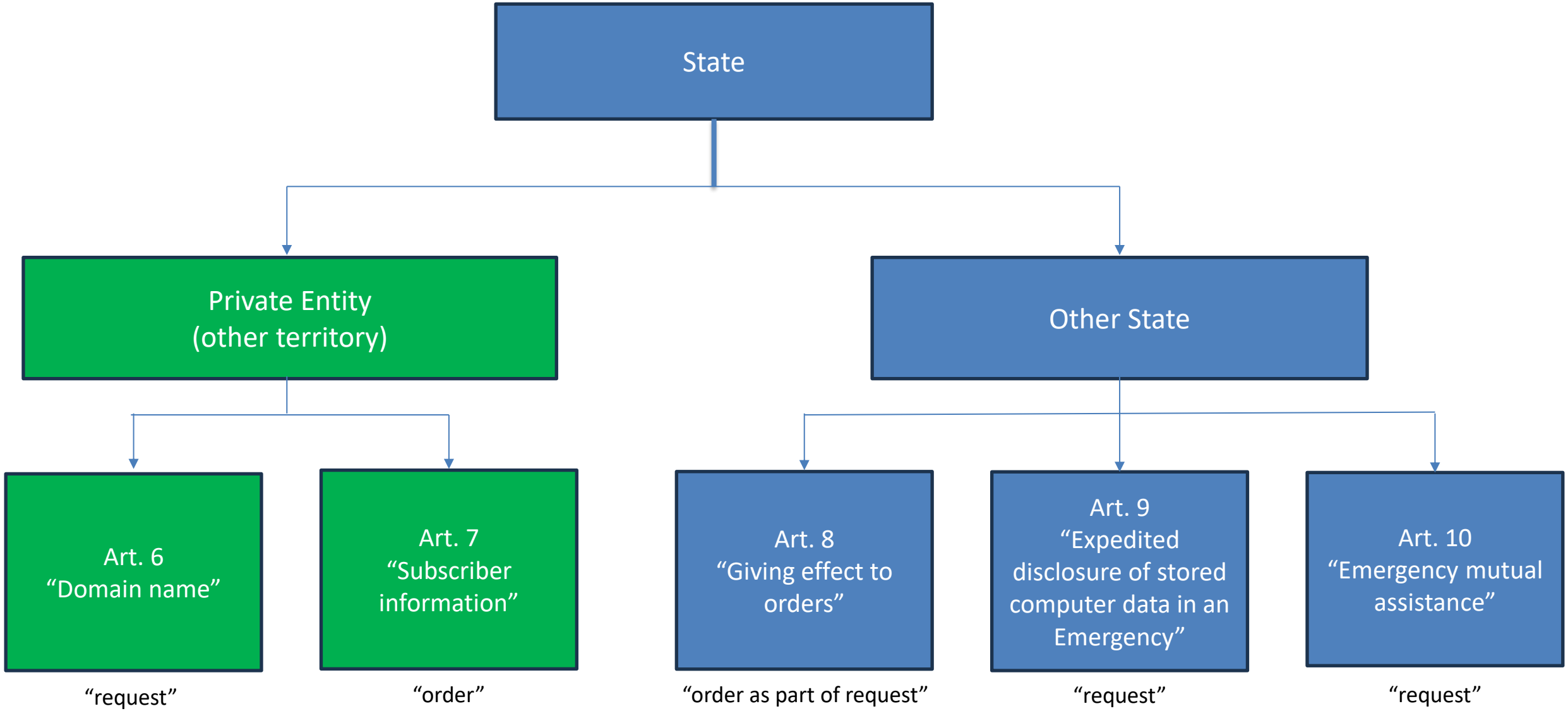
Article 25 Notification

Measures of the Second Protocol

Chapter II: Measures for enhanced cooperation

Article 6	Request for domain name registration information	→ Public-2-Private
Article 7	Disclosure of subscriber information	→ Public-2-Private
Article 8	Giving effect to orders from another party for expedited production of subscriber information and traffic data	→ Public-2-Public
Article 9	Expedited disclosure of stored computer data in an emergency	→ Public-2-Public
Article 10	Emergency mutual assistance	→ Public-2-Public
Article 11	Video conferencing	→ Public-2-Public
Article 12	Joint investigation teams and joint investigations	→ Public-2-Public

Content of the Second Protocol



Second Protocol: What next?

Second Protocol on electronic evidence: Status May 2025		
Parties	2	Serbia (February 2023), Japan (May 2023)
+ Signatories	47	Most recent: Czechia, Georgia, Latvia, Paraguay, Peru, Sierra Leone

Note:

- 5 ratifications needed for entry into force
- 30 Parties to the Convention on Cybercrime have not yet signed it

Second Protocol: What next?

- Signature and ratification of the Second Protocol ▶ PRIORITY for 2025
- C-PROC capacity building projects available to support and share experience
- EU member States to implement alongside the E-evidence Regulation

CyberSPEX

CyberSPEX – Overview

- Duration: 24 months (1 March 2024 – 28 February 2026)
- Budget and Funding: 2.23 million EUR. European Union (90%)/Council of Europe (10%)
- Implemented by the Council of Europe's Cybercrime Programme Office (C-PROC)
- Close cooperation with EUROJUST and EUROPOL, including the EJCN and SIRIUS project, as well as CEPOL
- all EU m/S are invited to participate in CyberSPEX, offer activities tailored to their need

CyberSPEX – Purpose and main objectives

Purpose

- the project supports EU m/S in the development of the relevant domestic legislation and of other measures to operationalise the provisions of the Second Protocol
- focus on EU m/S cooperation with non-EU countries (EU m/S will cooperate with each other primarily on the basis of EU law)

Main objectives

- Increased alignment of domestic legislation of EU m/S with the Second Protocol
- EU m/S to become signatories and Parties to the Second Protocol
- Improved capacities of criminal justice practitioners in EU m/S to apply the tools of the Protocol

Solutions proposed by CyberSPEX project

A. Support to national authorities through regional meetings and workshops in order to exchange and cooperate with different stakeholders from countries with a similar legislative framework. Already 3 different meetings (Nordic and Scandinavian countries, Mediterranean countries and Central and Eastern European countries)
B. Providing expertise and logistical arrangements (venue, catering, travel) to support internal assessment, progress and discussions within EU countries
C. Organise meetings and exchanges between national authorities and industry/service providers to enhance direct public/private cooperation (especially related to article 6 and 7)
D. Possibility for exchange between national authorities and service providers within the same country to facilitate a better understanding of procedures and to erase potential challenges

To participate to the Octopus Conference, please register on this webpage:

Thank you for your participation!

Contact CyberSPEX team:

Jutta DINCA
Programme Manager
CyberSPEX Project
Council of Europe (C-PROC)
jutta.dinca@coe.int

Iolanda VASILE
Senior Project Officer
CyberSPEX Project
Council of Europe (C-PROC)
iolanda.vasile@coe.int

Floriane SPIELMANN
Project Assistant
CyberSPEX Project
Council of Europe
floriane.spielmann@coe.int

Contact Cybercrime team:

Jan KRALIK
Programme Manager
Cybercrime Division
Council of Europe
jan.kralik@coe.int