



C-PROC

**Cybercrime Programme Office
Council of Europe, Bucharest, Romania**

C-PROC

**Cybercrime Programme Office of the Council of Europe
iPROCEEDS-2 PROJECT**

www.coe.int/cybercrime

COUNCIL OF EUROPE



CONSEIL DE L'EUROPE



C-PROC

Cybercrime Programme Office

Council of Europe, Bucharest, Romania



Council of Europe - leading human rights organization

- **46 states parties**, 27 members of the EU
- signed the European Convention on human rights, a treaty designed to protect:
 - **Human rights**
 - **Democracy**
 - **Rule of law**

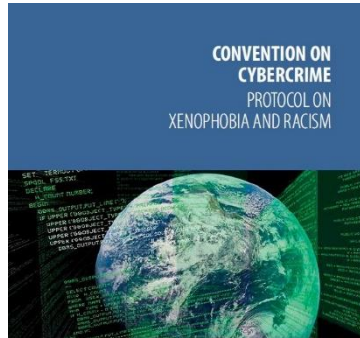
Cybercrime - a threat to fundamental rights

- Affects the **right to private life, dignity and integrity** of individuals
- Causes **financial loss**, affects **critical services** and **public security**
- Threatens **the freedom of expression** media, civil society organizations
- Threatens the **democratic stability**, radicalization terrorism, interfering with elections

C-PROC

Cybercrime Programme Office

Council of Europe, Bucharest, Romania



Explanatory Reports
and Guidance Notes

www.coe.int/t/cybercrime

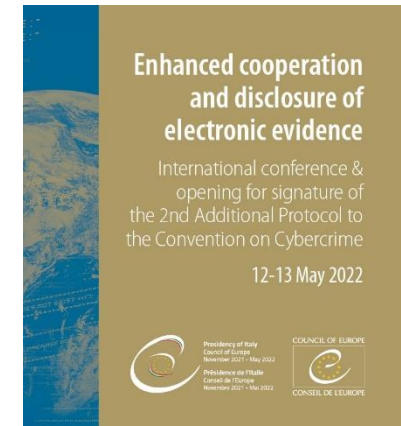


1 Common standards: Budapest Convention on Cybercrime and relates standards

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



3 Capacity building: C-PROC ► Technical cooperation programmes





C-PROC

Cybercrime Programme Office

Council of Europe, Bucharest, Romania

Project specific objective:	To further strengthen the capacity of authorities in project countries and areas to search, seize and confiscate cybercrime proceeds and prevent money laundering on the Internet and to secure electronic evidence.
Project area:	Albania, Bosnia and Herzegovina, Montenegro, Serbia, North Macedonia, Turkey and Kosovo*
Duration:	48 months (January 2020 – December 2023)
Budget:	EURO 4,945,000
Funding:	European Union and Council of Europe
Implementation:	Cybercrime Programme Office (C-PROC) of the Council of Europe

**This designation is without prejudice to positions on status and is in line with UNSC 1244 and the ICJ Opinion on the Kosovo Declaration of Independence.*



C-PROC

Cybercrime Programme Office

Council of Europe, Bucharest, Romania

Project specific objective:	To further strengthen the capacity of authorities in project countries and areas to search, seize and confiscate cybercrime proceeds and prevent money laundering on the Internet and to secure electronic evidence.
RESULT 1	Legislation strengthened regarding securing electronic evidence and access to data
RESULT 2	Coordinated cybercrime and cybersecurity Policies and Strategies
RESULT 3	Specialised online public Reporting Systems on cybercrime offences
RESULT 4	Capacities of specialised Investigative Units and inter-agency co-operation between cybercrime investigators, prosecutors, FIUs and cybersecurity experts on online crime proceeds, cybercrime and electronic evidence
RESULT 5	Public/Private information sharing and co-operation between service providers and criminal justice authorities
RESULT 6	Judicial training on cybercrime, electronic evidence, financial investigations and anti-money laundering measures
RESULT 6	International cooperation between cybercrime units, FIUs, authorities for judicial cooperation



C-PROC

Cybercrime Programme Office

Council of Europe, Bucharest, Romania

TARGET GROUPS	<ul style="list-style-type: none">• Specialized Cybercrime Units, Financial Investigation Units, FIUs• Digital forensics experts, Prosecution, Judiciary• Cybersecurity community – CERTS/CIRTS• Data protection community, Private sector
GUIDES	<ul style="list-style-type: none">• Guide on virtual currencies• Electronic evidence guide• Guide on ransomware
HIGHLIGHTS	<p>Strengthened capacities of Cybercrime Investigation Units</p> <ul style="list-style-type: none">-Training on Financial Investigations, Virtual Currencies, Darknet and Digital Forensics-Regional exercise on investigation Ransomware (in collaboration with US DoJ)-Regional workshop on investigation cyber-attacks (in collaboration with CEPOL)-Guide on Ransomware investigation and Electronic Evidence Guide v.3 <p>Stronger Public/Private cooperation</p> <ul style="list-style-type: none">-6 domestic public/private meetings on cooperation between criminal justice and ISPs-Underground Economy Conference-Promoting the role of women in fighting cybercrime <p>Closer International cooperation</p> <ul style="list-style-type: none">-24/7 NETWORK, EUROPOL, EUROJUST, CEPOL, INTERPOL, Americas Forum, regional meetings



CROSS-CUTTING DEVELOPMENTS

LEGISLATION

- Country **wikis**
- Country **legal profiles**
- Global report on cybercrime legislation

JUDICIAL TRAININGS

- Specialised judicial training on **cybercrime** and **EE (introductory)**
- Specialised judicial training on cybercrime and EE (**advanced**)
- Specialised judicial training on **international cooperation**
- Specialised judicial training on **training skills**

ONLINE TRAINING PLATFORMS

- HELP
- Octopus


GUIDES AND TOOLS

- Electronic evidence **guide** (updated v 3.0)
- SOPs on **electronic evidence**
- Guide for **first responders** to cybercrime investigations
- Guide on LEA **training strategy**
- Guide on seizing **cryptocurrencies**
- Guide on conducting criminal investigations in **ransomware** attacks

LEA TRAININGS

- **Financial investigations** training material (CyberEast)
- **Ransomware** investigation training (CyberSouth)
- Training **exercises**/scenarios (LEA/Financial Unit/ISP)
- Exercise on **Public – Private cooperation** (LEA/ISP)

ELECTRONIC EVIDENCE

- Invisible to the untrained eye, highly volatile
 - Can be altered or destroyed by normal use
 - Can be copied without degradation
- 
- Any information, generated, stored or transmitted by the use of electronic equipment
 - Capable to ascertain the existence or non-existence of an offence, to identify the person who committed such an offence and to determine the circumstances necessary for the settlement of a case
 - Any information generated, stored or transmitted in digital form that may later be needed to prove or disprove a fact disputed in legal proceedings
-
- The collection, analysis and usage of e-evidence is increasingly relevant in criminal proceedings, not only in relation to cybercrime, but also in relation to any other offence that may involve e-evidence.
 - **Subscriber** information: user of an IP address, the owner of an email, social network account, technical information on the location or equipment used; means of payment, communication.
 - **Traffic data**: data relating to communication, generated by a computer system, indicating origin, destination, route, time, date, size, duration, or type of service.
 - **Content data**: the content, the message or information (content of emails, social networks accounts and chat messages or similar, illegal content such as child abuse materials)

ELECTRONIC EVIDENCE

- **Guide on Electronic Evidence** - Provides guidance and good practice on the handling of electronic evidence
- **Guide on Seizing Cryptocurrencies**
- **Guide for First Responders to Cybercrime Investigations**
- **Guide of investigating Ransomware attacks**
- **Standard Operating Procedures** for the Collection, Analysis and Presentation of Electronic Evidence

Octopus Community

Platform for information sharing and cooperation on cybercrime and electronic evidence



Second Additional Protocol (ETS 224) at glance

- **ISSUES:** increasing use of servers in foreign jurisdictions and LEAs limited by territorial borders
- **SOLUTION:** Second Additional Protocol to the Convention on Cybercrime on enhanced co-operation and disclosure of electronic evidence
- **OPENING OF THE TREATY:** Strasbourg
 - 12/05/2022 - Treaty open for signature
 - by the States Parties to Treaty ETS 185
- **30 COUNTRIES SIGNED:** including Romania, Serbia, Bulgaria, Montenegro, North Macedonia, Croatia and Slovenia





Second Additional Protocol (ETS 224) at glance

ARTICLE 7 – DISCLOSURE OF SUBSCRIBER INFORMATION

- The competent authorities can issue an **order** and submit it **directly** to a **service provider** in the territory of another Party, in order to obtain the disclosure of specified, stored **subscriber information** in that service provider's possession or control, where the information is needed for criminal investigations or proceedings.

ARTICLE 9 – EXPEDITED DISCLOSURE OF STORED COMPUTER DATA IN AN EMERGENCY

- In an emergency, **the 24/7 Network point of contact** can transmit/receive a request to/from a point of contact in another Party seeking immediate assistance in obtaining from a service provider in the territory of that Party the expedited disclosure of specified, stored **computer data** in that service provider's possession or control, **without a request for mutual assistance**.

ARTICLE 10 – EMERGENCY MUTUAL ASSISTANCE

- Each Party may seek mutual assistance on a **rapidly expedited basis** where it is of the view that an emergency exists. The request shall include a description of the facts that demonstrate the emergency and how the assistance sought relates to it.
- Each Party shall ensure that a person from its **central authority** or other authorities responsible for responding to mutual assistance requests is **available 24/7** for the purpose of responding to a request under this article.
- Each Party may, declare that requests may also be sent **directly** to its **judicial authorities**, or through **INTERPOL** or **24/7 Point of Contact**. In any such cases, a copy shall be sent at the same time to the central authority of the requested Party through the central authority of the requesting Party.



Second Additional Protocol (ETS 224) at glance

FURTHER CYBERCRIME AND E-EVIDENCE CAPACITY BUILDING IN THE REGION

- Cyberattacks, ransomware attacks, attacks against critical infrastructure
- Tools and capacities to address challenges related to virtual currencies
- Implementation of the SAP to the BC in the region, with new tools for enhanced cross-border cooperation and disclosure of e-evidence
- Strengthen ownership by national stakeholders and project impact
- Involvement of additional stakeholders

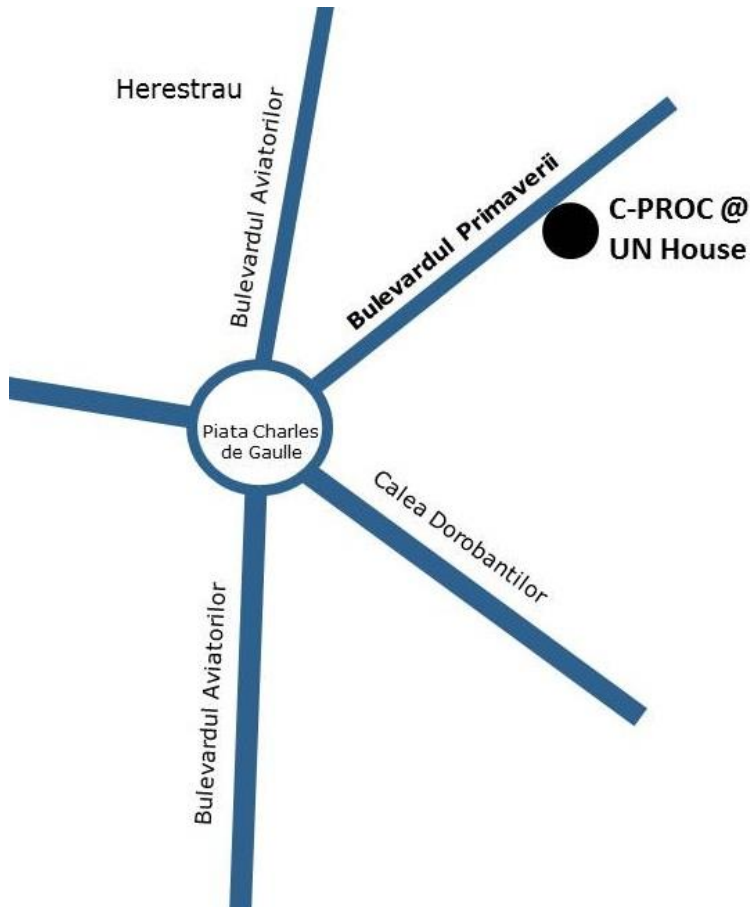


C-PROC

Cybercrime Programme Office

Council of Europe, Bucharest, Romania

Thank you!



COUNCIL OF EUROPE



CONSEIL DE L'EUROPE

Daniel CUCIURIANU

Programme Manager

Cybercrime Programme Office (C-PROC)

Council of Europe – Conseil de l'Europe

Blvd Primaverii 48A, 011975, Bucharest, Romania

T + 40212017882 / M + 40722686064

www.coe.int/cybercrime

daniel.cuciurianu@coe.int