

C-PROC

Cybercrime Programme Office

COUNCIL OF EUROPE



CONSEIL DE L'EUROPE

Be part of the global justice response to cybercrime

Between **April 2014** and **March 2026**,
C-PROC delivered more than **2,700 activities**
supporting over **140 countries**.



Who we are and what we deliver

The Council of Europe Cybercrime Programme Office (C-PROC) supports over 140 countries worldwide in strengthening their capacity to prevent and combat cybercrime. Our work is anchored in the **Convention on Cybercrime (Budapest Convention)** - the first international treaty providing a comprehensive legal framework for tackling cybercrime and securing electronic evidence.

We combine



Legal reform



Operational
capacity building



International
co-operation
mechanisms



24/7 Network*
of Points of Contact

* which enables rapid cross-border assistance in urgent cases and aims to increase meaningful partnerships between government agencies and some of the world's largest technology companies

Why this matters



Cybercrime is no longer a niche technical issue: it affects economies, trust, democracies and security of our societies.



Cyber-attacks, online fraud, ransomware, cyberviolence and online crime against children are rapidly increasing across the globe.



Criminal justice authorities face increasing challenges in accessing electronic evidence across borders while respecting human rights.



Without effective and expedited international co-operation, justice systems risk falling behind.



www.coe.int/cybercrime

www.cybox.coe.int

Turning co-operation into real-world impact

Through our programmes, countries are able to:



Access electronic evidence across borders faster

through implementation of the Second Additional Protocol on the Expedited Disclosure of Electronic Evidence*.



Investigate and prosecute cybercrime more efficiently

including cyber-attacks, online fraud, ransomware, and online crimes against children.



Engage with service providers and digital platforms

through structured, scalable and trusted public-private co-operation.



Strengthen safeguards and trust

ensuring full respect for human rights, privacy, and rule of law.



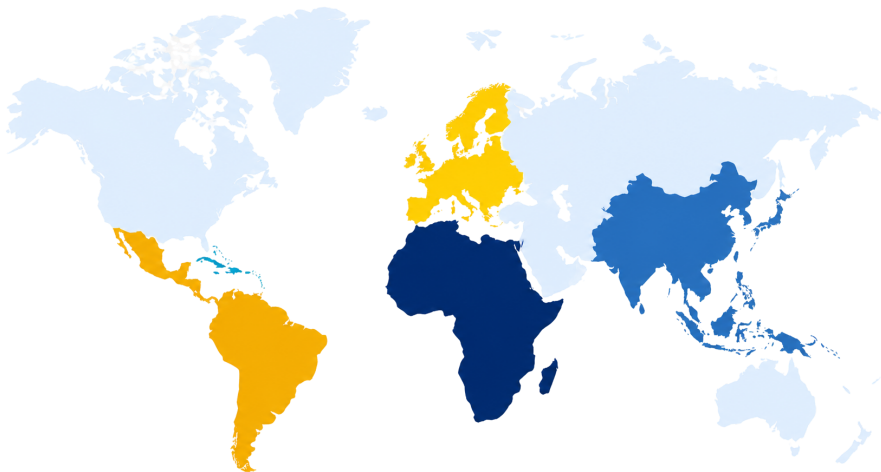
Respond to emerging threats

including AI-related crime, cyberviolence, and virtual assets.

* This provides a legal basis for private companies to disclose the data lawfully.

Where we work

Our programmes are implemented globally, with strong engagement in:



Africa

Asia Pacific

Europe

Latin America

Caribbean

Flexible partnership opportunities

We offer partners the possibility to support through funding:



Targeted interventions

Focused support to individual countries or specific challenges (e-evidence, cross-regional co-operation, interplay between cybercrime and cybersecurity)



Regional programmes

Coordinated actions addressing cross-border threats (e.g. scams, ransomware, financial investigations).



Thematic initiatives

Developing resources for addressing criminal investigations, specialized units, and judicial training.



Global co-operation platforms

Supporting international exchange, policy dialogue, operational co-operation (e.g. Octopus framework and our online training platform, CYBOX).



To explore further, please reach out to cybercrime@coe.int