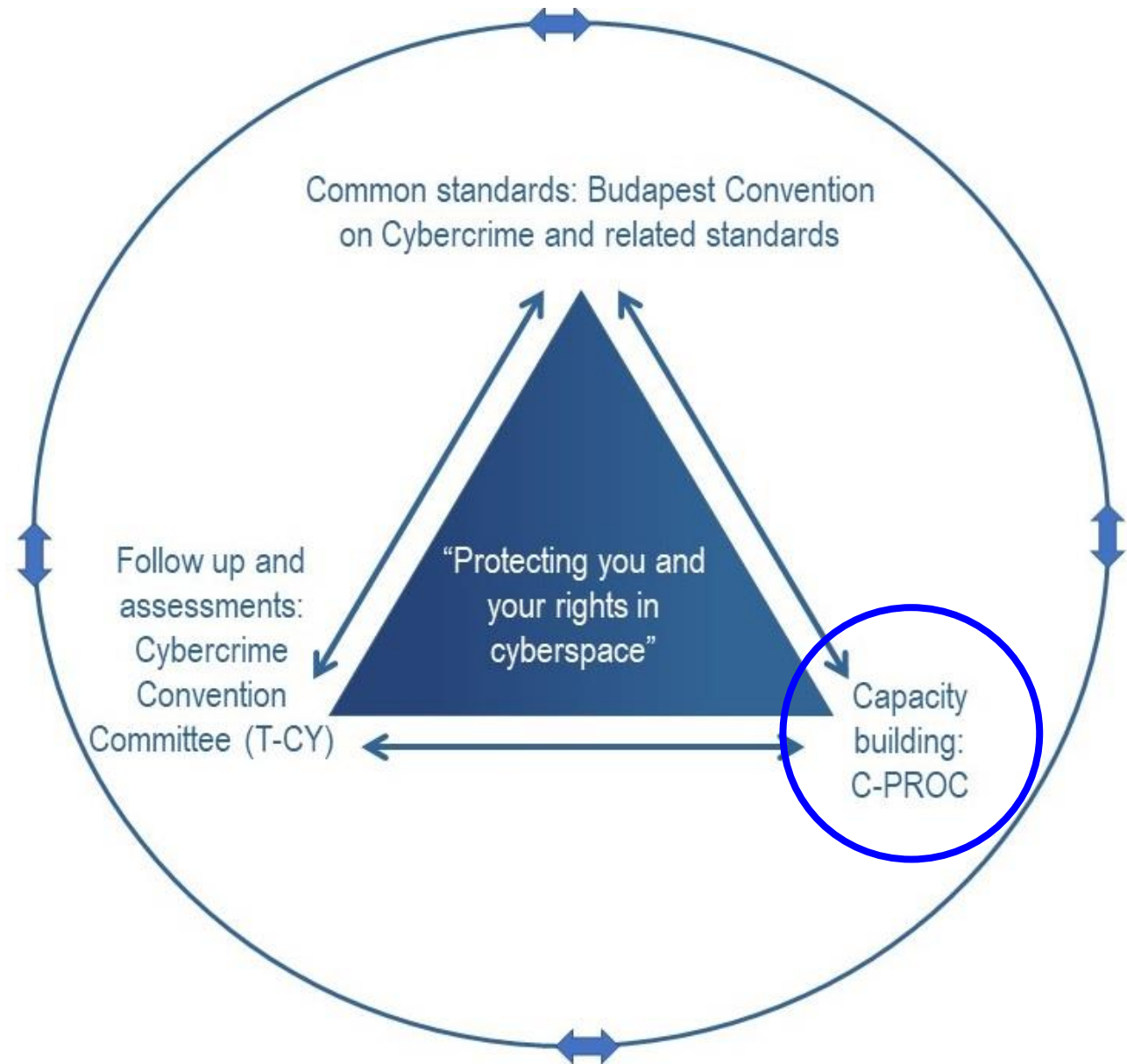


Update on capacity building activities by the Cybercrime Programme Office of the Council of Europe (C-PROC)



The framework of the Convention on Cybercrime

- ▶ Budapest Convention on Cybercrime (2001)
- ▶ 1st Protocol on Xenophobia and Racism via Computer Systems (2003)
- ▶ 2nd Protocol on enhanced cooperation and disclosure of electronic evidence (2022)
- ▶ Guidance Notes



The Convention on Cybercrime: Backed up by capacity building



GLACY-e: Training of Trainers for justice and law enforcement officials

10-12 SEPTEMBER 2024 | BOGOTA, COLOMBIA

A three-day training activity on cybercrime and electronic evidence in Colombia, between 10-12 September. With the support of GLACY-e, the event was jointly organised by the Ministry of Foreign Affairs, Superior Council of the Judiciary, and the Office of the Attorney General. ...



Philippines showcased a self-developed electronic evidence course for prosecutors and frontline police officers

23 - 26 SEPTEMBER 2024 | PANGASINAN, PHILIPPINES

The Department of Justice (DOJ) and the Philippine National Police (PNP) organised the Electronic Evidence First Responder's Training course from 23 to 26 September, in Pangasinan, Philippines for 30 police officers, 16 prosecutors, and 4 investigative agents of the National Bureau of Investigation. ...



CyberSPEX: Online Workshop on international co-operation tools (Art 9 and 10) provided by the Second Additional Protocol to the Convention on Cybercrime (Budapest Convention)

23 SEPTEMBER 2024 | ONLINE

On 23 of September 2024, the CyberSPEX project, a joint initiative of the European Commission and the Council of Europe, held an online workshop aimed at enriching the knowledge of the representatives of the EU Member States on the tools provided for enhanced co-operation on cybercrime and electronic evidence. ...



Underground Economy Conference 2024

2-5 SEPTEMBER | STRASBOURG, FRANCE

From 2 to 5 September 2024, the Council of Europe, alongside the European Commission, organised the fourth time the Underground Economy Conference at the Palais de l'Europe, in Strasbourg, France. This year's event gathered around 500 experts representing various countries. ...



Panama updates its cybercrime legislation to align with the Convention on Cybercrime

10 OCTOBER 2024 | PANAMA CITY, PANAMA

On 10 October 2024, the National Assembly of Panama approved several provisions on cybercrime and electronic evidence, including for amending the Criminal Code, the Code of Criminal Procedure and Law 11 of 2015 on international legal assistance in criminal matters. The Council of Europe. ...



Octopus project – CYBERKOP action: Domestic workshop on public-private cooperation on assessing and mitigating security risks and incidents in the 5G era

17 SEPTEMBER 2024 | PRISTINA, KOSOVO

The CYBERKOP Action of the Octopus Project is supporting the National Cyber Security Unit (KOS-CERT) to organise a workshop in Pristina, Kosovo* aimed at strengthening the public-private cooperation in managing 5G security risks and incidents. The workshop brings together 20 representatives from various sectors. ...



GLACY-e & ID4D projects lead a legislative drafting workshop in Nigeria

4-5 SEPTEMBER 2024 | LAGOS, NIGERIA

On 4-5 September, GLACY-e project, a joint initiative of the European Union and the Council of Europe, partnered with the ID4D project in facilitating the organisation of a legislative drafting workshop for representatives of the national task force in charge of drafting the new cybercrime law. ...



Eurojust – Council of Europe workshop sparks thriving discussions on spontaneous information sharing

25-26 SEPTEMBER 2024 | THE HAGUE, NETHERLANDS

Eurojust and the Cybercrime Programme Office of the Council of Europe (C-PROC) brought together more than 70 participants from some 40 countries to discuss key aspects related to the spontaneous sharing of information obtained in criminal investigations. The relevance of spontaneous information sharing. ...



CyberSouth+: Regional training exercise on live data forensics and cryptocurrency for law enforcement agencies

16-19 SEPTEMBER 2024 | ISTANBUL, TÜRKİYE

The joint European Union and Council of Europe project CyberSouth+ organised together with all its partners – Algeria, Egypt, Jordan, Lebanon, Libya, Morocco, Palestine[1] and Tunisia a regional training exercise on live data forensics and cryptocurrency for law enforcement agencies, between 16-19 September 2024. ...



GLACY-e: First pool of national trainers set up in Brazil

26-27 AUGUST 2024 | ONLINE

19 prosecutors have finalised the Training of Trainers Programme supported by the GLACY-e project, a joint initiative of the European Union – Council of Europe, with the last session concluded online, between 26-27 August 2024, on training skills – adult training methodology. The aim of the programme is to build a pool of national trainers. ...



Guatemala working on national legislation on cybercrime, in view of acceding to the Budapest Convention

GUATEMALA CITY | 22-23 OCTOBER 2024

Strengthening the country's capacities to combat cybercrime and facilitating accession to the Convention on Cybercrime.

Octopus Project: Judicial Training Programme on cybercrime and e-evidence kick starts in Indonesia

BOGOR, INDONESIA | 29 OCTOBER - 1 NOVEMBER 2024



CyberSEE: Judges, Prosecutors and Judicial Trainers from South-East Europe, Türkiye and Kazakhstan attended the Regional workshop on strategies and practices of judicial training on cybercrime and electronic evidence

ISTANBUL, TÜRKİYE | 22-23 OCTOBER 2024



The eighth Annual Meeting of the 24/7 Network of Contact Points

THE HAGUE, NETHERLANDS | 18 OCTOBER 2024

On 18 October 2024, the Cybercrime Programme Office of the Council of Europe (C-PROC) organised the eighth Annual Meeting of the 24/7 Network of Contact Points. ...

C-PROC (2014 – 2024): 2300+ activities for 130+ countries

Cybercrime Programme Office of the Council of Europe (C-PROC)

in Romania:

- Support processes of change towards stronger criminal justice capacities on cybercrime and e-evidence in line with the Budapest Convention and with rule of law safeguards
- 7 ongoing projects with a cumulative budget of EUR 34+ million
- 45 staff
- Some 400 activities per year
- Capacity for virtual capacity building
- Cooperation with 120+ countries in 2024
- Joint projects with the European Union
- Voluntary contributions by France, Japan, UK, USA and others
- Support to T-CY

ional delivery of an introductory course
ronic evidence in Benin

group of judges and prosecutors from Benin, who had
hop earlier in August, delivered for the first time an
pe

Current projects:

- ▶ Octopus Project
- ▶ GLACY-e
- ▶ CyberEast+
- ▶ CyberSouth+
- ▶ CyberSEE
- ▶ CyberUA
- ▶ CyberSPEX

Africa Working Group on
da

he GLACY+ Project, organised the 9th Africa Working
om 18 to 22 July 2022. The AF-WGM is an annual

event that aims to facilitate sharing of information and best practices in the region. This...



Workshop



detective
(male) in



This is t



Union, held a hybrid workshop with the authorities of Panama in view of further harmonising national legislation on cybercrime and electronic evidence with the provisions of the Budapest Convention on...

C-PROC guides, tools, resources

Octopus Project

Discussion paper: Freedom of expression within the context of action on cybercrime – Practical considerations

Strasbourg, 10 December 2023 / Provisional version

Octopus Community
Platform for information sharing and cooperation on cybercrime and electronic evidence

The online tools – Country Wiki profiles on cybercrime legislation and policies, training materials and many more to come – bring together experts, counterparts, academics and professionals in the cybercrime field.

- Country Wiki**: Cybercrime legislation & policy
- Public / Private Cooperation**: Tools for cooperation
- Materials**: Training materials & templates

WHAT'S NEW?

- Country Wikis now available for more than **100 States!**
- New updates are in the pipeline – stay tuned!

USEFUL LINKS

- Cybercrime website
- Template: Mutual Legal Assistance Request for subscriber information (Art. 31 Budapest Convention). English and bilingual versions available.
- Template: Data Preservation Request (Articles 29 and 30 Budapest Convention). English and bilingual versions available.

Welcome to the new Octopus Community!
BUCHAREST, 10 JUNE 2023
We are happy to announce the opening for public access of our specialised resource on cybercrime.

You are here: Octopus Cybercrime Community > Materials

Training materials, guides, templates

You have access to all the training and other materials on cybercrime and electronic evidence developed by the Council of Europe within its capacity building programmes. Training materials are provided for **educational non-commercial purposes**.

- You can expect new / updated courses to be available soon
- The **HELP course** on cybercrime has been launched and you can find more information [here](#). The course is available in ENG, ARA, AZE, BUL, CES, FRA, HUN, HYE, KAT, POR, RON, SLK, SPA, UKR. Soon available: TUR.

TRAININGS

- Introductory Training Module on Cybercrime, Electronic Evidence and Online Crime Proceeds
- Introductory Judicial Training UPDATED (2020/2021)
Introductory level of knowledge for judges/prosecutors on cybercrime/electronic evidence
- Advanced Judicial Training UPDATED (2018)
Additional level of knowledge on cybercrime/electronic evidence for judges/prosecutors.
- First Responder Training Pack (2020)
Training course for "1st responders" on how to handle electronic evidence on crime scenes
- Basic Course on the Search, Seizure and Confiscation of Online Crime Proceeds (2017)
Training Course for Judges and Prosecutors

You are here: Cyberviolence > News

Cyberviolence against women addressed by Council and European Parliament in first EU-wide law

BRUSSELS, 12 FEBRUARY 2023
A first-ever EU-wide instrument agreed upon by the Council and European Parliament addresses all...

View all news

What is cyberviolence?

Cyberviolence being a relatively new phenomenon that encompasses a wide variety of crimes, the term is still difficult to define precisely. The T-CY Working Group on cyberbullying and other forms of violence, in its Mapping Study on Cyberviolence, settled on defining cyberviolence as:

"The use of computer systems to cause, facilitate, or threaten violence against individuals, that results in (or is likely to result in) physical, sexual, psychological or economic harm or suffering and may include the exploitation of the individual's circumstance, characteristics or vulnerabilities."

Why is addressing it important?

Cyberviolence is often misunderstood and not taken as seriously as it should be. Yes, it is important to remember that cyberviolence may start online, but it often ends offline with devastating consequences for the victims and their families. Threats of violence, stalking, incitement to suicide, solicitation of children for sexual purposes... may all result in the victim self-harming or being physically attacked by the initial perpetrator. It is important to act in order to prevent cyberviolence from happening, and to protect and bring justice to the victims.

However, most countries are struggling to recognize the different faces of the problem and to address them in domestic law. Some types of cyberviolence are addressed fully or in part in international agreements, but many remain unaddressed.

The Council of Europe is working across sectors (through, for instance, the mechanisms related to the Budapest Convention, the Istanbul Convention and the Lanzarote Convention) to ensure human rights are upheld in cyberspace as well, for all.

READ MORE
Read the T-CY's Mapping Study on Cyberviolence

Octopus Project

Implementing the First Protocol to the Convention on Cybercrime on Xenophobia and Racism: Good practice study

Strasbourg, 1 December 2023 (provisional)

Country Wiki



The wiki profiles provide an overview of a country's policy on cybercrime and electronic evidence. Every fiche includes a description of cybercrime policies/strategies, the state of cybercrime legislation, the channels of cooperation, international cooperation and case law.

For more information on a country's legislation, click on the **legal profile** in each country wiki.

Type your search here

Afghanistan	Albania	Algeria
Andorra	Angola	Antigua and Barbuda
Argentina	Armenia	Australia
Azerbaijan	Bahamas	Bahrain
Bangladesh	Barbados	Belarus
Belgium	Belize	Benin
Bolivia (Plurinational State of)	Bosnia and Herzegovina	Botswana
Brazil	Brunei	Bulgaria
Burkina Faso	Burundi	Cabo Verde
Cambodia	Cameroon	Canada
Central African Republic	Chad	Chile

CYBOX CYBERCRIME & E-EVIDENCE COUNCIL OF EUROPE

The CYBOX journey ahead: a glimpse at our timeline

The future of CYBOX is bright, and we can't wait to embark on this journey with you! In...

ABOUT CYBOX

Welcome to **CYBOX** - your online platform for exchange, training, and resource sharing on cybercrime and electronic evidence.

With the rise of cybercrime and the increasing reliance on electronic evidence, it is essential for professionals in the criminal justice sector to stay ahead of the criminals. **CYBOX** is designed to meet the evolving training needs of judges, prosecutors, law enforcement agencies, and other key stakeholders in the criminal justice system worldwide.

CYBOX creates an environment in which countries cooperating with *Cybercrime Research Office of the Council of Europe* can...

- A repository of cybercrime and e-evidence related reference and training materials
- Highly customizable learning management system for C-PROC and criminal justice

C-PROC



Bucharest, 8 December 2023 / Provisional version

- Thousands of criminal justice practitioners trained + capacities for training
- Contribution to human rights and rule of law in cyberspace
- Legislation:
 - ▶ 2013: 70 States with offences in line with Budapest Convention
 - ▶ 2023: 130 States
- Partnerships, synergies, trusted cooperation
- Membership in Convention on Cybercrime:
 - ▶ By 2013: 53 States were parties (41) or had signed it (2) or been invited to accede (10)
 - ▶ By 2024: 96 States were parties (76), or had signed it (2) or been invited to accede (17)
- ▶ Successful investigations, prosecutions and international operations all over the world

OCTOPUS Project	Jan 2021 – Dec 2027	EUR 10 million	Voluntary contributions (USA, Japan, France , UK and others) [funding not fully secured]
GLACY-e project on Global Action on Cybercrime Enhanced	Aug 2023 – Jan 2026	EUR 5.55 million	EU/CoE joint project (including Council of Europe 10% OB/JPP)
CyberUA project on strengthening capacities on electronic evidence of war crimes and gross human rights violations in Ukraine	Feb 2024 – July 2026	EUR 3.5 million	Voluntary contributions to the Ukraine Action Plan and Ordinary Budget [funding not fully secured]
CyberEast+ on enhanced action on cybercrime for cyber resilience in Eastern Partnership States	Mar 2024 – Feb 2027	EUR 3.89 million	EU/CoE joint project (including Council of Europe 10% OB/JPP)
CyberSouth+ project on enhanced co-operation on cybercrime and electronic evidence in the Southern Neighbourhood Region	Jan 2024 – Dec 2026	EUR 3.89 million	EU/CoE joint project (including Council of Europe 10% OB/JPP)
CyberSEE project on enhanced action on cybercrime and electronic evidence in South-East Europe and Türkiye	Jan 2024 – Jun 2027	EUR 5.55 million	EU/CoE joint project (including Council of Europe 10% OB/JPP)
CyberSPEX project on enhanced co-operation on e-evidence by EU Member States through the Second Additional Protocol to the Convention on Cybercrime	Mar 2024 – Feb 2026	EUR 2.23 million	EU/CoE joint project (including Council of Europe 10% OB/JPP)

C-PROC: priorities 2025+

- To support the implementation of the Second Additional Protocol to the Convention on Cybercrime through all projects
- To assist countries – in particular those already invited to accede to the Convention on Cybercrime – to meet their requirements and become parties
- To help criminal justice authorities address challenges related to ransomware, virtual currencies, and artificial intelligence, and to enhance their co-operation with bodies responsible for cybersecurity
- To further strengthen capacities for the collection and use of e-evidence for the prosecution of war crimes and gross violations of human rights in Ukraine
- To support the strengthening of human rights and rule of law safeguards in project countries
- To promote further synergies of the Convention on Cybercrime and its Protocols with other organisations (UNODC ► UN treaty), initiatives and relevant Council of Europe instruments.
- To make use of the CYBOX online platform for training and exchange – developed under the Octopus Project – in order to permit the scaling up of online training on cybercrime and e-evidence

