C-PROC at 7:

Lessons learnt from seven years of capacity building on cybercrime

Online event on the occasion of the 7th anniversary of the Cybercrime Programme Office of the Council of Europe (C-PROC) in Bucharest

Online | 9 April 2021 | 11h00-13h00 (Romania)

Agenda:

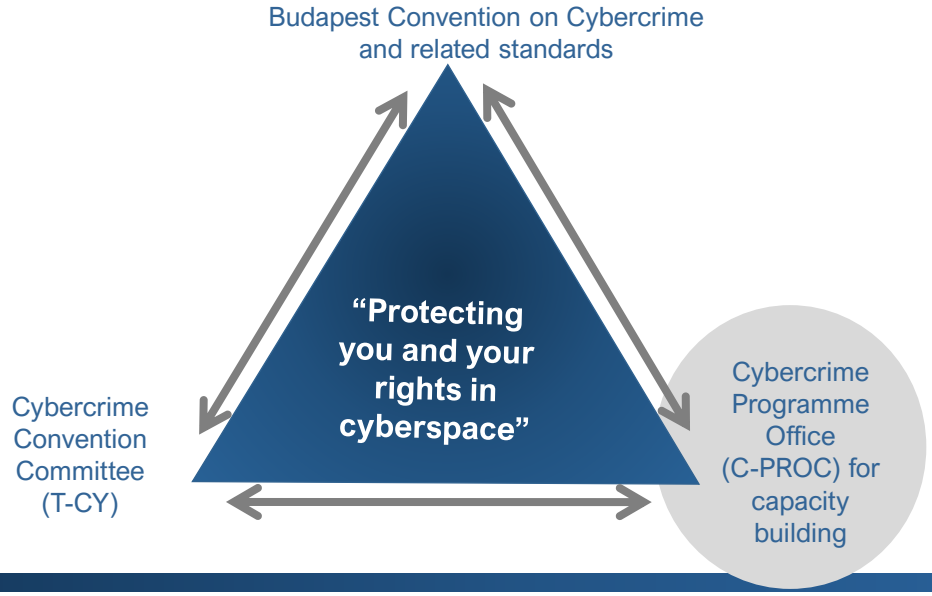
- Opening session
- C-PROC: lessons learnt from 7 years of capacity building
- Cooperation on cybercrime – the future
- Conclusions

COUNCIL OF EUROPE
CONSEIL DE L'EUROPE

www.coe.int/cybercrime

1

Cooperation on cybercrime: the approach of the Council of Europe

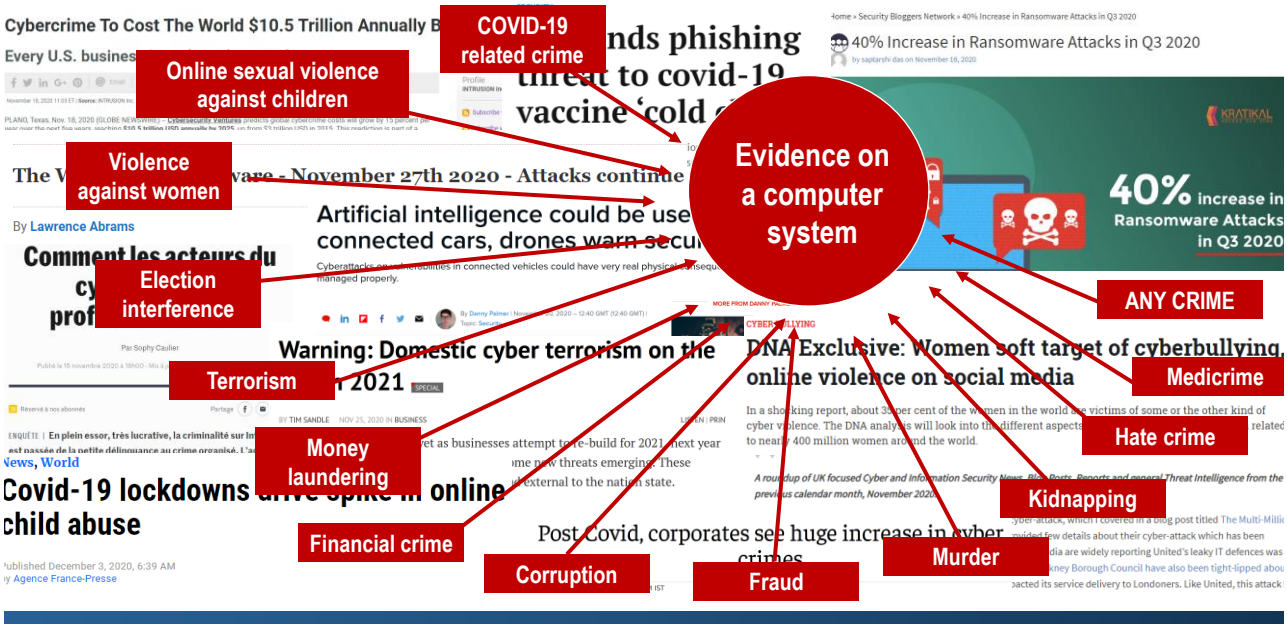


2

Why are we here?

3

And any type of crime may involve electronic evidence



4

Supporting capacity building worldwide through C-PROC: Background

- February 2013: UN Expert Group on Cybercrime – "broad agreement on capacity building", "diverse views" on other solutions*
  - Need for the Council of Europe to enhance its own capacities for capacity building on cybercrime and e-evidence
- March/April 2013: Offer by the Government of Romania to host a Council of Europe office on cybercrime in Bucharest
- October 2013: Committee of Ministers decision
- October 2013: MoU signed between Council of Europe and Government of Romania
- April 2014: C-PROC fully operational

* Confirmed by UNIEG 6-8 April 2021: most of the 61 recommendations found agreeable relate to capacity building, strengthening of legislation and sharing of experience among practitioners

5

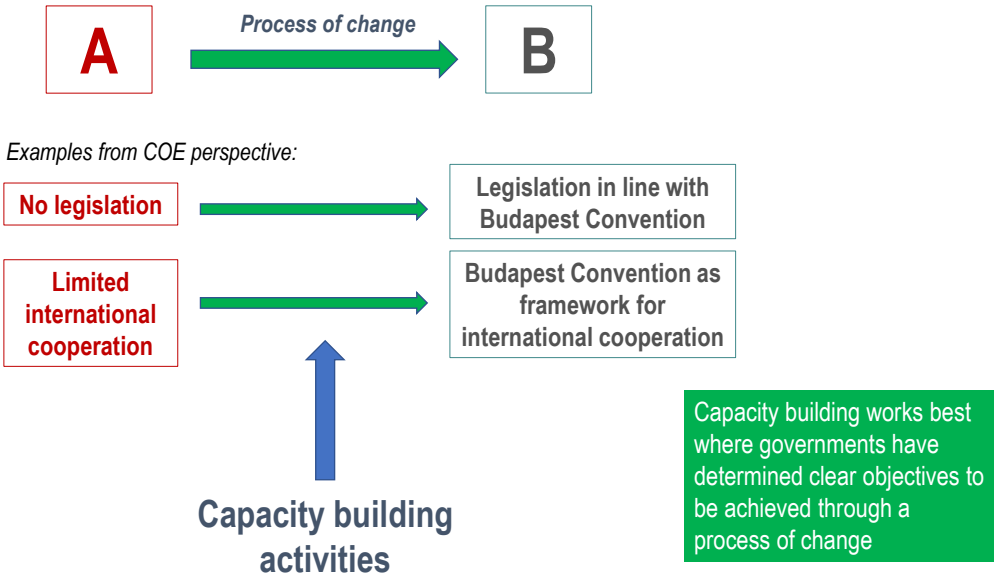
C-PROC Tasks

Task: Support to countries worldwide to strengthen criminal justice capacities on cybercrime and electronic evidence in line with the standards of the Budapest Convention

- Strengthening legislation on cybercrime and electronic evidence in line with rule of law and human rights (including data protection) standards
- Training judges, prosecutors and law enforcement officers
- Establishing specialized cybercrime and forensic units and improving interagency cooperation
- Promoting public/private cooperation
- Protecting children against sexual violence online
- Enhancing the effectiveness of international cooperation

6

About capacity building: the rationale



7

C-PROC resources

35 staff running 6 projects with a volume of EU 40 million covering all regions of the world:

- GLACY+ on Global Action on Cybercrime Extended (EU/COE Joint Project)
- iPROCEEDS-2 Targeting proceeds from online crime in South-eastern Europe (EU/COE Joint Project)
- Octopus Project resource for global capacity building (voluntary contribution funded)
- CyberSouth for the Southern Neighbourhood (EU/COE Joint Project)
- EndOCSEA@Europe on ending online child sexual exploitation and abuse (funded by WEPROTECT)
- CyberEast for the Eastern Partnership region (EU/COE Joint Project)

= 1000+ activities for 150+ countries in seven years

= 200+ virtual activities since March 2020

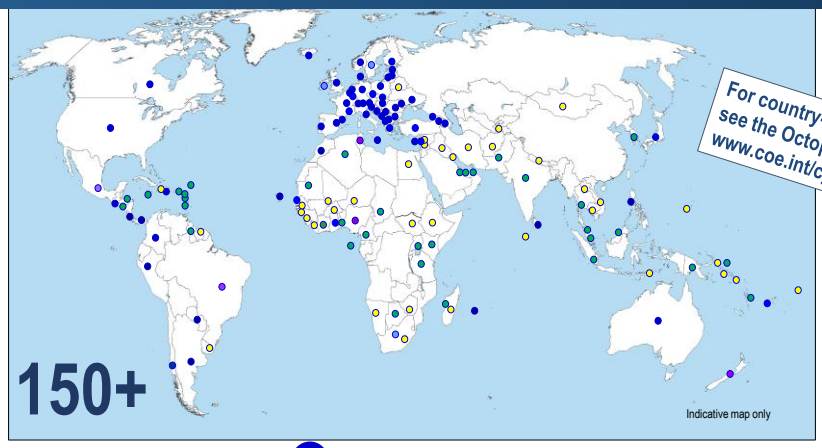
Current funding by

- European Union
- Canada
- Japan
- United Kingdom
- USA

+ the budget of the Council of Europe

8

Reach of capacity building and the Budapest Convention



For country-specific information see the Octopus Community at www.coe.int/cybercrime

Parties:	65	Other States with laws largely in line with Budapest Convention	= 20+
Signed:	3	Further States drawing on Budapest Convention for legislation	= 50+
Invited to accede:	9		
=	77		

9

C-PROC activities – recent examples

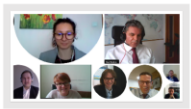
iPROCEEDS-2: Online workshop and hands-on simulation for improvement of the skills, set-up and competencies of 24/7 point of contact in Bosnia and Herzegovina

2 APRIL 2021 | ONLINE

Continuing the series of activities dedicated to the strengthening of the 24/7 Points of Contact established under the Budapest Convention on Cybercrime, the Joint Project of the European Union and the Council of Europe – iPROCEEDS-2 organized an online domestic workshop and hands-on simulation...

CyberEast: Roundtable discussion on cybercrime and cybersecurity policies and action plans with Moldovan authorities

19 MARCH 2021 | ONLINE



Cybersecurity is critical to both prosperity and security. As our daily lives and economies increasingly rely on digital technologies, we become more and more exposed to malicious cyber-attacks. These are spreading in terms of who is involved and what they seek to achieve. Harmful

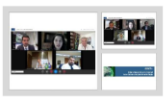
Octopus Project: Workshop on Criminal Justice Capacities on Cybercrime and Electronic Evidence and accession to the Budapest Convention organised with national authorities of Jamaica

25-26 MARCH 2021 | JAMAICA | ONLINE

"The more we educate, the less we investigate" is one of the phrases used in Jamaica that was shared from the outset by one of the 30 participants of the Workshop on Criminal Justice Capacities on Cybercrime and Electronic Evidence and accession to the Budapest Convention, held between 25-26...

GLACY+: Brazil is a new Priority Country: initial assessment of criminal justice capacities on cybercrime and e-evidence concluded

24-26 MARCH 2021 | ONLINE - BRAZIL



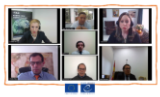
The GLACY+ Project, a joint action of the European Union and the Council of Europe, together with INTERPOL, supported the Public Ministry and the Ministry of Foreign Affairs in Brazil in organizing a three-day workshop with the scope of assessing the current state of the cybercrime legislation...

10

C-PROC activities – recent examples

GLACY+ project welcomes Colombia as priority country

24-26 MARCH 2021 | ONLINE



On 24-26 March 2021, the GLACY+ Project, a joint action of the European Union and the Council of Europe, together with INTERPOL supported the Ministry of Foreign Affairs in Colombia in organizing a three-day workshop with the scope of assessing the current state of the cybercrime legislation and...

CyberSouth: Judicial material mainstreaming, third meeting of the working group in Tunisia

12 MARCH 2021 | ONLINE ACTIVITY

Under the CyberSouth project, the third meeting for mainstreaming the judicial material in Tunisia took place, online, on the 12th of March 2021. This event was a follow-up on the second meeting of the working group focused on developing the Tunisian course on cybercrime and electronic evidence...

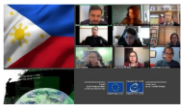
CyberSouth: Study on the conformity of personal data provisions with Convention 108+

MARCH 2021

CyberSouth, one of the capacity building projects implemented by the Cybercrime Programme Office of the Council of Europe (C-PROC), aims to strengthen the capacities to fight against cybercrime in the Southern Neighborhood Region of the following five priority countries: Algeria, Jordan, Lebanon,...

GLACY+: Designing judicial training in the Philippines – On-demand online modules and a Bench Book for judges

10 MARCH 2021 | ONLINE | PHILIPPINES



An online brainstorming session was held on the 10th of March 2021, in the framework of the GLACY+ project a joint action of the European Union and Council of Europe, aimed at defining the outline of an updated judicial training materials on cybercrime and electronic evidence,

11

C-PROC activities – recent examples

iPROCEEDS-2: Webinar cyberbullying: trends, prevention strategies and the role of law enforcement

9 MARCH 2021 | ONLINE

According to the international studies, bullying is a widespread negative phenomenon, affecting more than 20% of the school students. In the context of the COVID-19 pandemic, bullying has more and more moved from the school yard towards the internet, increasing the number of the victims of...

Cape Verdean national judicial trainers deliver introductory course on cybercrime and electronic evidence for judges and prosecutors

9-11 MARCH 2021 | HYBRID | PRAIA, CAPE VERDE

The GLACY+ Project supported the Ministry of Justice and Labour of Cape Verde in organizing a three-day Introductory Judicial Course on Cybercrime and Electronic Evidence for judges and prosecutors, using the new Council of Europe judicial training

CyberSouth: Third national meeting on the development of a domestic Standard Operating Procedures and toolkit for first responder/cybercrime investigation and e-evidence in Lebanon

8 MARCH 2021 | ONLINE ACTIVITY

Following the second meeting on the development of Standard Operating Procedures (SOPs) with Lebanon, which took place on the 9th of December 2020, the third activity for national Lebanese SOPs was implemented online on the 8th of March 2021, together with the members of the working group – law...

CyberEast: Series of Workshops on the Development of SOP for cooperation between CSIRTs and Law Enforcement in the Eastern Partnership countries finalized

AUGUST 2020 - MARCH 2021 | ONLINE

In the landscape of growing threat of cybercrime, CERTs/CSIRTs (Computer Emergency/Computer Security Incident Response Teams) have an important role in preventing cyber-attacks and in coordinating the technical response at national level. They may help in monitoring and reporting cybercrimes, in...

12

C-PROC activities – recent examples

Octopus Project: Series of online workshops on cybercrime legislation and electronic evidence in the Caribbean region kicked off with Trinidad and Tobago

2-3 MARCH 2021 | ONLINE

Countries of the Caribbean region have taken steps in recent years to equip themselves with legislation to address the growing challenge of cybercrime. While in some states such legislation has been in place for more than a decade, others are in the process of reforming their laws. The Budapest...

Crypto speaks French: rolling out the new edition of INTERPOL GLACY+ Technical Webinars

15-25 FÉVRIER 2021 | EN LIGNE

Between 15 to 25 February, INTERPOL has resumed the series of technical webinars on cryptography delivered under the GLACY+ project to Criminal Justice Authorities, this time targeting French speaking professionals from more than 30 countries. Around 100 participants per session actively engaged...

Octopus Project: Addressing COVID-19-related cybercrime in Asia with financial support from the Government of Japan

1 MARCH 2021 | ASIA REGION

COVID-19 related cybercrime may have serious consequences for the security and stability of countries. It not only compounds the social, including health, and economic impact of the pandemic, but may further weaken the ability of public authorities to respond to cyberattacks. This weakening of...

GLACY+: 4th edition of the INTERPOL Malware Analysis Training – Africa, Europe and MENA region

1-5 MARCH 2021 | ONLINE

Between 1-5 March, experienced cybercrime investigators and digital forensics experts from Benin, Cape Verde and Ghana (GLACY+ project priority countries) have participated in the 4th edition of the INTERPOL Malware Analysis Training, series dedicated to Africa, Europe and MENA region. The course...

CyberEast: Webinar on Hate Speech and Restrictive Measures

26 FEBRUARY 2021 | ONLINE

As acknowledged by the Council of Europe's Cybercrime Convention Committee (T-CY) Mapping study on cyberviolence: "Cyberviolence is the use of computer systems to cause, facilitate, or threaten violence against individuals that results in, or is likely to result in, physical, sexual,...

13

Impact of capacity building

- Works, responds to needs and makes an impact
  - Legislation with safeguards
  - Investigations and criminal proceedings
  - Public/private, interagency and international cooperation
  - Sustainable training
- Facilitates multi-stakeholder cooperation, partnerships and synergies
- Has human development benefits and feeds into Sustainable Development Goals
- Helps reduce the digital divide
- Is based on broad international agreement and may help overcome political divisions

14

Impact of capacity building – testimonies

- Jayantha FERNANDO, Chairman, Sri Lanka CERT, and Director ICTA
- Angela Marie M. DE GRACIA, State Counsel, Department of Justice, Philippines
- Branko STAMENKOVIC, Deputy General Prosecutor, Serbia
- Hania HELWEH, Judge, Ministry of Justice, Lebanon
- Albert ANTWI-BOASIAKO, T-CY Bureau Member, Ghana
- Givi BAGDAVADZE, Head of International Cooperation Unit, Office of the Prosecutor General of Georgia

15

Cooperation on cybercrime – the future

Cooperation on cybercrime – the future

- Tools for enhanced cooperation and disclosure of electronic evidence: about the 2nd Additional Protocol to the Budapest Convention
- The future of capacity building

16

The Budapest Convention tomorrow: towards a new Protocol

Why a new Protocol?

- The scale and quantity of cybercrime, devices, users and victims
- Cloud computing, territoriality and jurisdiction
  - Where is the crime?
  - Where is the data, where is the evidence?
  - Who has the evidence?
  - What legal regime applies to order / disclose data?
- The challenge of mutual legal assistance
- The 0.1% problem

- ► How to obtain subscriber information efficiently?
- ► How to cooperate directly with a service provider in another Party?
- ► How to obtain WHOIS (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?

www.coe.int/cybercrime

17

Towards a new Protocol

Benefits of the future 2nd Additional Protocol on enhanced cooperation and disclosure of electronic evidence

Operational value:

- Basis for direct cooperation with service providers in other Parties for subscriber information ("direct disclosure")
- Effective means to obtain subscriber information and traffic data ("giving effect")
- Legal basis for disclosure of WHOIS information
- Cooperation in emergencies ("expedited disclosure" + "emergency MLA")
- Mutual assistance tools ("video-conferencing", "JITs")
- Data protection safeguards to permit the flow of personal data under the Protocol.

Policy value:

- Convention on Cybercrime will remain relevant and effective
- Respect for free Internet with limited restrictions in case of criminal misuse (specific criminal investigations, specified data)

Adoption in November 2021 + 20th anniversary Budapest Convention + Octopus Conference?

18

The future of capacity building

- Much more of the same and even better
- Online/physical hybrid delivery of activities and online resources
- Priority countries and regional training centres as hubs
- Policy dialogue between criminal justice practitioners and policy makers
- Multi-stakeholder cooperation, partnerships and synergies
- Enhanced cooperation and disclosure of electronic evidence:
  - Direct cooperation with service providers and registrars
  - Expedited means of public to public cooperation
  - Cooperation in emergencies
  - Joint investigation teams and joint investigations
  - Human rights, rule of law and data protection safeguards

= Support implementation of the 2nd Additional Protocol to the Budapest Convention

19