

“Breakfast meeting” on cybercrime / Réunion « petit-déjeuner » sur la cybercriminalité

Thursday / jeudi, 21 November / novembre 2024, 8h30 – 9h30, Restaurant Bleu, Palais de l'Europe

Update on the framework of the Convention on Cybercrime

- The impact so far and continued relevance of the Budapest Convention ([ETS 185](#)) and its First Protocol on xenophobia and racism ([ETS 189](#))
- The added value of the Second Protocol on electronic evidence ([CETS 224](#))
- The achievements of the Cybercrime Convention Committee ([I-CY](#))
- The Council of Europe's worldwide capacity building work through its Cybercrime Programme Office ([C-PROC](#))

Information on the draft “United Nations Convention against Cybercrime”

- [Implications](#) for the Budapest Convention ?

Alexander Seger
 Head of Cybercrime Division
 Council of Europe
alexander.seger@coe.int



www.coe.int/cybercrime

1

Cybercrime ...

Cybercrime To Cost The World \$10.5 Trillion Annually

Every U.S. business is under cyberattack

November 16, 2020 11:55 ET | Source: AT&T World Intellectual Property

PLANO, Texas, Nov. 16, 2020 (GLOBE NEWSWIRE) - Cybersecurity Ventures predicts global cybercrime costs will grow by more than the next five years' combined \$10.5 trillion (USD) annually by 2024, up from \$5 trillion (USD) in 2019. This expenditure is just of a...

Indonesia arrests 88 Chinese nationals over online romance scams

Indonesian police say they've arrested 88 Chinese citizens for involvement in a cross-border telephone and online romance scam syndicate after receiving a tip from Chinese security ministry

Written by Sean Gallagher, Anna Szalay, Andrew Brandt, Chester Wisniewski

Gangs forcing hundreds of thousands of people into cybercrime in south-east Asia, says UN

Organised criminals use threats, torture and sexual violence to coerce victims to work in international scamming operations

children and combat sexual exploitation.

The Week in Ransomware - No. 10

By Lawrence Abrams

Comment les acteurs du cybercrime se professionnalisent

Par Sophie Caulier

Publié le 16 novembre 2020 à 16h00 - Mis à jour le 16 novembre 2020 à 16h00

CYBER BULLYING

DNA Exclusive: Women soft target of cyberbullying and online violence on social media

In a shocking report, about 35 per cent of the women in the world are victims of some or the other kind of cyber violence. The DNA analysis will look into the different aspects of cyber violence against women related to nearly 400 million women around the world.

ANDY GREENBERG | SECURITY | SEP 7, 2022 12:18 PM

The International Criminal Court Will Now Prosecute Cyberwar Crimes

And the first case on the docket may well be Russia's cyberattacks against civilian critical infrastructure

Costa Rica's 'War' Against Ransomware Is a Wake-Up Call for the Region

James Bosworth

Jul 18, 2023

2,700 people tricked into working for cybercrime syndicates rescued in Philippines

Ransomware claims increase by 20%

Cybercrime has developed into a real business in recent years, with offerings such as ransomware-as-a-service leading to a real “democratization” of the criminal business. Even threat actors without technical know-how can carry out attacks. At the same time, ransomware groups are becoming increasingly aggressive. Manufacturing, services, and

Category	Percentage
Trusted Relationship	3.3%
Insider Threat	2.4%
Malware	1.8%
Malicious Software Download	1.8%
Phishing	1.2%
Malicious Email	1.2%
Root Cause (Non-BEC Incidents)	3.2%
User Action	24.4%
External Exposure	70.1%
Other	0.8%

2

... and e-evidence re all types of crime

3

Cybercrime and e-evidence: the problem of territoriality and jurisdiction

Where is the crime?
 Where is the data, where is the evidence?
 Who has the evidence?
 Where is the boundary for LEA powers?
 What protections to human rights apply?

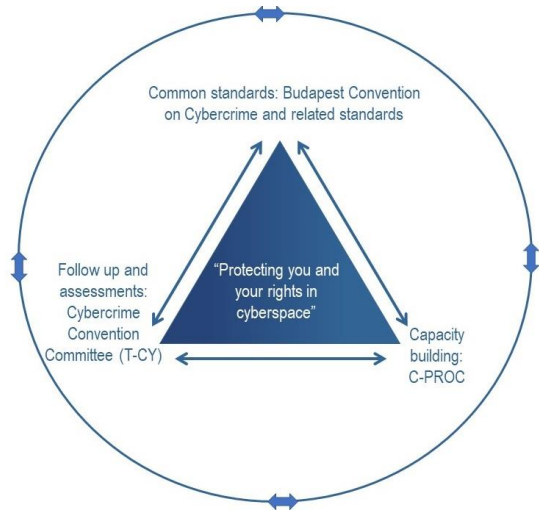
- ▶ Transnational nature of cybercrime and e-evidence
- ▶ Crime and jurisdiction in cyberspace
- ▶ Need for public/private and international cooperation

4

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 October 2024: 76 Parties and 20 "Observer States"



5

The first Protocol on Xenophobia and Racism (ETS 189)

Protocol concerning the criminalisation of acts of a racist and xenophobic nature committed through computer systems

Opening for signature 28 January 2003

Entry into force 1 March 2006

Currently 36 Parties + 10 Signatories

Key provisions

- Dissemination of racist and xenophobic material through computer systems (Article 3)
- Racist and xenophobic-motivated threat (Article 4) and insults (Article 5)
- Denial, gross minimisation, approval or justification of genocide or crimes against humanity (Article 6)
- Relation between the Convention and this Protocol (Article 8)

Need to counter increasing hate speech and hate crime online ▶ XR Protocol

6

The first Protocol on Xenophobia and Racism: implementation

Parties		Signatories
Albania	Monaco	Austria
Andorra	Morocco	Belgium
Armenia	Montenegro	Canada
Benin	Netherlands	Estonia
Bosnia and Herzegovina	North Macedonia	Italy
Croatia	Norway	Liechtenstein
Cyprus	Paraguay	Malta
Czech Republic	Poland	Switzerland
Denmark	Portugal	South Africa
Finland	Romania	Türkiye
France	San Marino	
Germany	Senegal	
Greece	Serbia	
Iceland	Slovakia	
Latvia	Slovenia	
Lithuania	Spain	
Luxembourg	Sweden	
Moldova	Ukraine	

Octopus Project



Strasbourg, 1 December 2023 (provisional)

Status as at 18 Nov 2024
 ► 36 Parties + 10 Signatories

7

Second Protocol on electronic evidence (CETS 224)

Second Protocol on enhanced cooperation and disclosure of e-evidence (2022):

- Scope: criminal investigations and proceedings related to computer systems and data and collection of e-evidence re **any** criminal offence
- **Direct cooperation** with service providers and registrars in other Parties
- Giving effect to production orders from other Parties
- Expedited **cooperation in emergencies**
- Video conferencing
- Joint investigation teams and joint investigations
- **Data protection and other safeguards**

More effective tools to obtain electronic evidence re any crime

- Crucial for criminal justice practitioners
- Relevance of Budapest Convention

Priority in 2025!

Status:

- 45 signatories + 2 ratifications (Japan and Serbia)
- 5 ratifications to enter into force
- Slow progress in (most) COE member States

► **More determination re signature and ratification required**

► **EU m/s to implement alongside EU E-evidence Regulation**

8

Cybercrime Convention Committee (T-CY)

Composition:

- 76 members (= Parties)
- 20 observers (= signatories and States invited to accede)
- International organisations as observers
- [co-funded by voluntary contributions to capacity building projects]

Tasks:


- Assessment of implementation ► 4th round: Article 19 on search and seizure of stored computer data
- Guidance Notes ► terrorism, election interference, ransomware, scope of procedural powers, etc.
- Preparation of Second Protocol

Coming up:


- Working group on artificial intelligence (mapping study)
- Work on virtual assets
- Guidance Note on Article 26 – Spontaneous information

9


The Convention on Cybercrime: Backed up by capacity building




GLACY-e: Training of Trainers for justice and law enforcement officials
19-12 SEPTEMBER 2024 | BOGOTÁ, COLOMBIA
A three-day training activity on cybercrime and electronic evidence Colombia, between 10-12 September. With the support of GLACY-e, the event was jointly organised by the 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...




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 for enhanced co-operation on cybercrime and electronic...




Underground Economy Conference 2024
2-5 SEPTEMBER | STRASBOURG, FRANCE
From 2 to 5 September 2024, the Council of Europe, alongside the fourth time the Underground Economy Conference at the Palais de l'Europe, in Strasbourg, France. This year's event gathered around 500 experts repres...




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...




GLACY-e & ID4D projects lead a legislative workshop in Nigeria
4-9 SEPTEMBER 2024 | LAGOS, NIGERIA
On 4-5 September, GLACY-e project, a joint initiative of the Europe partnered with ID4D project in facilitating the organisation of a legislative drafting work representatives of the national task force in charge of drafting the...



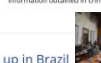
Eurojust – Council of Europe workshop sparks thriving discussions on spontaneous information sharing
20-26 SEPTEMBER 2024 | THE HAGUE, NETHERLANDS
Eurojust and the Cybercrime Programme Office of the Council of Europe (E-CYPRO) brought together more than 70 participants from some 40 countries to discuss key aspects related to the spontaneous sharing of information obtained in criminal investigations. The relevance of spontaneous information...




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



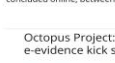
GLACY-e: First pool of national trainers set up in Brazil
26-31 AUGUST 2024 | ONLINE
19 prosecutors have finalised the Training of Trainers Programme supported by project, a joint initiative of the European Union – Council of Europe -, with the law concluded online, between 26-27 August 2024, on training skills – adult training methodology. The aim of the...




Guatemala working on national legislation on cybercrime, in view of acceding to the Budapest Convention
Strengthening the country's capacity to combat electronic and digital crimes effectively...




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



Octopus Project: Judicial Training Programme on cybercrime and e-evidence kick starts in Indonesia
INDONESIA, SEPTEMBER | 24 OCTOBER - 3 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, TURKEY | 20-23 SEPTEMBER 2024



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

10

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 2023
- 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

Current projects:

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

Africa Working Group on
Ja

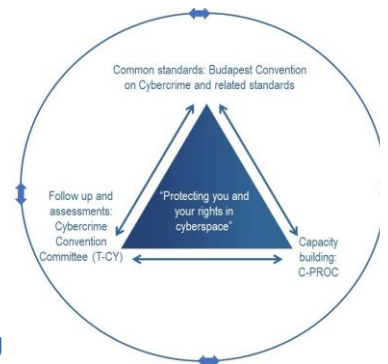
he GLACY+ Project, organised the 9th Africa Working
om 18 to 22 July 2022. The AF-WGM is an annual
event that aims to facilitate sharing of information and best practices in the region. This...

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...

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

Framework of Budapest Convention: IMPACT

- 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 (18)
- Legislation:
 - ▶ 2013: 70 States with offences in line with Budapest Convention
 - ▶ 2023: 130 States
- T-CY:
 - ▶ Maintained relevance of the Convention (2nd Protocol, Guidance Notes)
 - ▶ Increased quality of implementation (assessments)
- C-PROC
 - ▶ Legislation
 - ▶ Partnerships, synergies, trusted cooperation
 - ▶ Thousands of criminal justice practitioners trained + capacities for training



- = Successful investigations, prosecutions and international operations all over the world
- = Contribution to human rights and rule of law in cyberspace

Draft UN treaty against cybercrime: background

Background:

- UNGA initiative by Russia ► Dec 2019: UNGA Resolution 74/247
 - Decision to establish an Ad Hoc Committee (AHC) to elaborate “a comprehensive international convention on countering the use of information and communications technologies for criminal purposes”.
- Feb 2022 – Aug 2024: 7+1 formal sessions and numerous informal and intersessional meetings of the AHC
- 8 Aug 2024: Agreement by AHC on the draft text of a UN treaty and a draft resolution for submission to and adoption by UNGA
- 11 Nov 2024: Agreed by 3rd Committee of UNGA

Draft “United Nations convention against cybercrime; strengthening international cooperation for combating certain crimes committed by means of information and communications technology systems and for the sharing of evidence in electronic form of serious crimes”

Next:

- Adoption by UNGA [December 2024 TBC]
- Opening for signature in [Vietnam in 2025 TBC]

13

Draft UN treaty: Core concepts adapted from Budapest Convention


Core concepts and measures of the draft treaty

- are drawn from the BC on Cybercrime (2001)
- complemented by provisions adapted from the UN Conventions on Transnational Organised Crime (UNTOC, 2000) and Corruption (UNCAC, 2003)
- **confirms the timeless quality and relevance of the BC**

Example:

Art.	Budapest Convention		Draft UN treaty
2	Illegal access	7	Illegal access
3	Illegal interception	8	Illegal interception
4	Data interference	9	Interference with electronic data
5	System interference	10	Interference with an information and communications technology system
6	Misuse of devices	11	Misuse of devices
7	Computer-related forgery	12	Information and communications technology system-related forgery
8	Computer-related fraud	13	Information and communications technology system-related theft or fraud
9	Child pornography	14	Offences related to online child sexual abuse or child sexual exploitation material

14



In and not in the draft UN treaty

New in draft UN treaty:

- Solicitation or grooming of children for sexual offences (Article 15)
- Non-consensual dissemination of intimate images (Article 16)
- Adapted from UNTOC and UNCAC: measures on money laundering and crime proceeds

NOT in draft UN treaty:

None of the measures of the Second Protocol to the BC on enhanced cooperation and disclosure of electronic evidence (2022):

- ▶ Direct cooperation with service providers and registrars in other Parties (articles 6 and 7)
- ▶ Expedited cooperation in emergency situations (articles 9 and 10)

15



Outcome of the UN AHC process

UN AHC agreement on draft UN treaty:

- Major political success considering history and current international context.
- Largely consistent with BC.
- With minimum safeguards necessary for international cooperation.
- Maximum achievable and agreeable result.
- Will benefit cooperation between and with States that are not Parties to the BC.
- Will take some years until it be in force and operational.
- Protocol negotiations to commence two years after adoption by UNGA.
- Treaty process increased interest in Budapest Convention (more Parties, more requests for accession).

16


 Risks/concerns

Risks/concerns:

- Risk that some States will not respect human rights and rule of law conditions. Conference of States Parties (COSP) unlikely to review compliance.
- Risk of targeting assets of individuals, private sector organisations, media or civil society organisations through combination of provisions on fraud, money laundering, corporate liability, participation and attempt, and crime proceeds.
- Risk of supplementary criminalisation through a protocol (negotiations to commence two years after adoption of the convention as per draft UNGA resolution).
- ▶ Concerns raised by governments, civil society and industry stakeholders during the AHC and UNGA processes remain valid.
- ▶ Governments to decide on signature and ratification.

17


 Implications for BC

Implications for Convention on Cybercrime (Budapest Convention):

- BC with its Protocols will remain the more relevant framework in the foreseeable future.
- Synergies between both treaties feasible: capacity building, including on safeguards.
- More States will seek accession to the BC (based on experience during AHC process).
- However, a clear commitment to meeting human rights and rule of law conditions will be necessary when governments are seeking accession to the Budapest Convention on Cybercrime.

18



Discussion

Update on the framework of the Convention on Cybercrime

- The impact so far and continued relevance of the Budapest Convention ([ETS 185](#)) and its First Protocol on xenophobia and racism ([ETS 189](#))
- The added value of the Second Protocol on electronic evidence ([CETS 224](#))
- The achievements of the Cybercrime Convention Committee ([T-CY](#))
- The Council of Europe's worldwide capacity building work through its Cybercrime Programme Office ([C-PROC](#))

Information on the draft "United Nations Convention against Cybercrime"

- [Implications](#) for the Budapest Convention ?

www.coe.int/cybercrime