Budapest Convention on Cybercrime:

Content, impact, benefits and process of accession
IBM finds phishing threat to covid-19 vaccine ‘cold chain’

The problem of cybercrime …

The Week in Ransomware - November 27th 2020 - Attacks continue

Comment les acteurs du cybercrimes se professionnalisent

Warning: Domestic cyber terrorism on the rise in 2021

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

Covid-19 lockdowns drive spike in online child abuse

Pfizer/BioNTech vaccine docs hacked from European Medicines Agency
... and e-evidence re all types of crime

- Online sexual violence against children
- Violence against women
- Election interference
- Terrorism
- Drug trafficking
- Money laundering
- Fraud
- Corruption
- COVID-19 related crime
- War crime
- Any crime
- Medicrime
- Hate crime
- Kidnapping
- Murder
- Hate crime
Budapest Convention on Cybercrime (2001):

1. Specific offences against and by means of computer systems
2. Procedural powers with safeguards to investigate cybercrime and collect electronic evidence in relation to any crime
3. International cooperation on cybercrime and e-evidence

+ 1st Protocol on Xenophobia and Racism via Computer Systems

+ 2nd Protocol on enhanced cooperation on cybercrime and electronic evidence (Strasbourg, 12 May 2022)

+ Guidance Notes

By 30 June 2023: 68 Parties and 21 Observer States
Content of the Budapest Convention

Criminalising conduct
- Illegal access
- Illegal interception
- Data interference
- System interference
- Misuse of devices
- Fraud and forgery
- Child pornography
- IPR-offences

Procedural tools
- Expedited preservation
- Production orders
- Search and seizure
- Interception of computer data
  Limited by safeguards

International cooperation
- Extradition
- MLA
- Spontaneous information
- Expedited preservation
- MLA for accessing computer data
- MLA for interception
- 24/7 points of contact

Procedural powers and international cooperation for any criminal offence involving evidence on a computer system!
WannaCry, Petya, NotPetya: how ransomware hit the big time in 2017

Most first encountered ransomware after an outbreak shut down hospital computers and diverted ambulances this year. Is it here to stay?
### Content of the Budapest Convention: example ransomware

<table>
<thead>
<tr>
<th>Article</th>
<th>Budapest Convention on Cybercrime</th>
</tr>
</thead>
<tbody>
<tr>
<td>Art. 2</td>
<td>Illegal access</td>
</tr>
<tr>
<td>Art. 3</td>
<td>Illegal interception</td>
</tr>
<tr>
<td>Art. 4</td>
<td>Data interference</td>
</tr>
<tr>
<td>Art. 5</td>
<td>System interference</td>
</tr>
<tr>
<td>Art. 6</td>
<td>Misuse of devices</td>
</tr>
<tr>
<td>Art. 7</td>
<td>Computer-related forgery</td>
</tr>
<tr>
<td>Art. 8</td>
<td>Computer-related fraud</td>
</tr>
<tr>
<td>Art. 11</td>
<td>Attempt, aiding, abetting</td>
</tr>
<tr>
<td>Art. 12</td>
<td>Corporate liability</td>
</tr>
<tr>
<td>Art. 13</td>
<td>Sanctions and measures</td>
</tr>
<tr>
<td>Art. 14-21</td>
<td>Procedural powers</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Article</th>
<th>2nd Additional Protocol to Convention on Cybercrime</th>
</tr>
</thead>
<tbody>
<tr>
<td>Art. 7</td>
<td>(Direct) Disclosure of subscriber information</td>
</tr>
<tr>
<td>Art. 8</td>
<td>Giving effect to orders from another party for expedited production of subscriber information and traffic data</td>
</tr>
<tr>
<td>Art. 9</td>
<td>Expedited disclosure of stored computer data in an emergency</td>
</tr>
<tr>
<td>Art. 10</td>
<td>Emergency mutual assistance</td>
</tr>
<tr>
<td>Art. 11</td>
<td>Video conferencing</td>
</tr>
<tr>
<td>Art. 12</td>
<td>Joint investigation teams and joint investigations</td>
</tr>
</tbody>
</table>

### Ransomware Offences

- Article 2
- Article 3
- Article 4
- Article 5
- Article 6
- Article 7
- Article 8
- Article 11
- Article 12
- Article 13
Reach of the Convention on Cybercrime

Parties: 68
Signed: 2
Invited to accede: 19
Other States with substantive laws broadly in line with Budapest Convention: 45+
Further States drawing on Budapest Convention for legislation: 30+

= 89
= 75+
Treaty open for accession  (article 37)

**Phase 1:**
- A country with legislation in place
- Letter from Government to CoE expressing interest in accession
- Consultations (CoE/Parties) in view of decision to invite
- Invitation to accede

**Phase 2:**
- 5 years for the completion of the process
- Domestic procedure (e.g. decision by national Parliament)
- Deposit of the instrument of accession
Protocol concerning the criminalisation of acts of a racist and xenophobic nature committed through computer systems

Formal adoption 7 November 2002
Opening for signature 28 January 2003
Entry into force 01 March 2006
Currently 35 State Parties

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)
The first Protocol on Xenophobia and Racism: implementation

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

Status as at 30 June 2023

- **35 Parties + 11 Signatories**
The first Protocol on Xenophobia and Racism: resources

First additional protocol dedicated page:

- The official text of the protocol in official and non-official languages
- Conference
- Webinars
- Cyberviolence webpage
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?

- Transnational nature of cybercrime and e-evidence
- Crime and jurisdiction in cyberspace
- Need for public/private and international cooperation
Cybercrime: Threat to
► Human rights
► Democracy
► Rule of law

Positive obligations:
► Provide the means to protect the rights of individuals, also against crime

Problem:
► Proliferation of cybercrime
► Any type of crime now involving e-evidence
► Evidence somewhere in foreign, multiple, shifting or unknown jurisdictions
► Effective means not available to obtain the disclosure of e-evidence
► Less than [0.1%] of offences in cyberspace lead to prosecutions and convictions
► Do victims obtain justice?

2\textsuperscript{nd} Protocol to help address these challenges
Rationale: Why a 2nd Additional Protocol to the Budapest Convention?

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

Chapter I: Common provisions
  Article 1 Purpose
  Article 2 Scope of application
  Article 3 Definitions
  Article 4 Language

Chapter II: Measures for enhanced cooperation
  Article 5 General principles applicable to Chapter II
  Article 6 Request for domain name registration information
  Article 7 Disclosure of subscriber information
  Article 8 Giving effect to orders from another party for expedited production of subscriber information and traffic data
  Article 9 Expedited disclosure of stored computer data in an emergency
  Article 10 Emergency mutual assistance
  Article 11 Video conferencing
  Article 12 Joint investigation teams and joint investigations

Chapter III – Conditions and safeguards
  Article 13 Conditions and safeguards
  Article 14 Protection of personal data

Chapter IV: Final provisions
  Article 15 Effects of this Protocol
  Article 16 Signature and entry into force
  Article 17 Federal clause
  Article 18 Territorial application
  Article 19 Reservations and declarations
  Article 20 Status and withdrawal of reservations
  Article 21 Amendments
  Article 22 Settlement of disputes
  Article 23 Consultations of the Parties and assessment of implementation
  Article 24 Denunciation
  Article 25 Notification
Protocol on enhanced cooperation and disclosure of electronic evidence

Negotiated 2017 – 2021 by Parties to the Budapest Convention

Formal adoption 17 November 2021

Opening for signature 12 May 2022

Key provisions:

- Direct requests to registrars for data to identify registrants of domains (Article 6) or and orders to service providers to obtain subscriber information (Article 7)
- Giving effect to production orders from another Party (Article 8)
- Expedited cooperation in emergencies (Art. 9 and 10)
- Tools for mutual assistance (Article 11 - video conferencing and Article 12 – joint investigation teams and joint investigations)
- Rule of law and data protection safeguards (Articles 13 and 14)
**Scope**

**Criminal Justice Treaty**
- Related to an investigation or proceeding (relevance-proportionality)
- Not to gather intelligence or mass surveillance

- Related to cybercrimes
- Related to any crime including electronic evidence

**Electronic transmission**

**Related to electronic evidence**
Scope – electronic transmission
2⁰ Additional Protocol to the Convention on Cybercrime: efficiency with safeguards

Efficiency with safeguards

Means for a more effective criminal justice response:

▪ Direct cooperation with service providers in other jurisdictions to obtain subscriber information
▪ Direct requests to registrars to obtain domain name registration information
▪ More effective means to obtain subscriber information and traffic data through government-to-government cooperation
▪ Expeditious cooperation in emergency situations
▪ Joint investigations and video-conferencing

Subject to a strong system of safeguards:

▪ Article 2 – scope of Protocol: specific criminal investigations or proceedings related to cybercrime and e-evidence
▪ Article 13 incorporates Article 15 of the Convention to ensure the adequate protection of human rights and liberties and that provides for the principle of proportionality
▪ Article 14 provides for detailed data protection safeguards that are unique for a criminal justice treaty
▪ Articles specify types of data to be disclosed
▪ Articles specify information to be included to permit application of domestic safeguards
▪ Reservations and declarations to permit domestic safeguards and limit information to be provided
2nd Additional Protocol to the Convention on Cybercrime on enhanced cooperation and disclosure of electronic evidence (CETS 224)

Signatories (status 30 June 2023):

1. Andorra 18. Ghana 35. Slovenia
4. Austria 21. Iceland 38. Sweden
5. Belgium 22. Italy 39. Ukraine
7. Cabo Verde 24. Lithuania 41. USA
8. Canada 25. Luxembourg
9. Chile 26. Malta
10. Colombia 27. Mauritius
12. Croatia 29. Moldova
15. Finland 32. North Macedonia
16. France 33. Portugal
17. Germany 34. Romania

Ratification: (status 30 June 2023): 1. Serbia

Next:

► Signature by other Parties
► Ratification (5 needed for entry into force)
► Capacity building
Benefits of the Protocol

Operational value:

- Basis for direct cooperation with service providers for subscriber information ("direct disclosure")
- Effective means to obtain subscriber information and traffic data ("giving effect")
- 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
- Efficient cooperation with rule of law and data protection safeguards is feasible
- Respect for free Internet with limited restrictions in case of criminal misuse (specific criminal investigations, specified data)
The Convention on Cybercrime: Backed up by capacity building

Budapest Convention on Cybercrime and related standards

"Protecting you and your rights in cyberspace"

Cybercrime Convention Committee (T-CY)

Cybercrime Programme Office (C-PROC) for capacity building
The Convention on Cybercrime: Backed up by capacity building

CyberSouth: Study visit to Multinational Service Providers
6-7 JUNE 2023 | DUBLIN, IRELAND
The CyberSouth project, a joint endeavour of the Council of Europe and European Union, organised a study visit to Multinational Service Providers, to enhance public-private partnership to address cybercrime, during 6 and 7 June 2023, in Dublin, Ireland. Finance, Google, META, Microsoft, and...

GLACY+: First part of the ToT on Cybercrime and Electronic Evidence for judges and prosecutors in Peru
22-26 MAY 2023 | LIMA, PERU
Between 22-26 May 2023, was organised in Lima the first Introductory training on Cybercrime and Electronic Evidence for judges and prosecutors, since Peru’s onboarding as GLACY+ priority country in 2022. The activity is part of the broader Training of Trainers (ToT) programme aimed at creating a...

GLACY+: Co-operation with Timor-Leste on the legislative reform on cybercrime and electronic evidence
17 MAY 2023 | DILI, TIMOR-LESTE
On 17 May 2023, the GLACY+ Project, a joint action of the European Union and the Council of Europe, in co-operation with the Ministry of Justice of Timor-Leste, organised a one-day workshop to discuss the draft law currently being prepared by the national authorities in view of implementing the...

CyberEast: Trainings on the handling of cyber incident and cybercrime taxonomy take place in the Eastern Partnership countries
25 MAY – 6 JUNE 2023 | EASTERN PARTNERSHIP REGION
Thanks to the vital contributions of project partners from Armenia, Azerbaijan, Georgia, the Republic of Moldova and Ukraine, the CyberEast Joint Project of the European Union and of the Council of Europe has completed a series of Training

Octopus and GLACY+ Projects: Training on Child Protection System for countering online child sexual exploitation and abuse in Mauritius
15-19 MAY 2023 | MAURITIUS
The increasing use of children and communication technologies (ICTs) has created new opportunities for sexual offenders to target and harm children. As a continuation of the support to the authorities of Mauritius in fighting online child sexual exploitation and abuse (OCSEA)...

GLACY+: Introductory and Advanced training course on cybercrime and electronic evidence for 20 Ukrainian judges
24 MAY 2023 | BUCURESTI, ROMANIA
Between 2-6 May 2023, the National School of Judges of Ukraine, with the support of CyberEast, a joint project of the Council of Europe and of the European Union, held an introductory training course, followed by an advanced session on cybercrime and electronic evidence, designed for judges...

CyberEast: 25 Ukrainian investigators and prosecutors attend a training course on cybercrime and e-evidence in Suceava
25-28 APRIL 2023 | SUCEAVA, ROMANIA
CyberEast, a joint project of the European Union and of the Council of Europe, in co-operation with Police, Security services and the Prosecutor’s Office training institution of Ukraine, organised a four-day exercise on cybercrime and electronic evidence in Suceava, Romania. This course was...
The Convention on Cybercrime: Backed up by capacity building

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
- 5 ongoing projects with a cumulative budget of EUR 40 million
- 40 staff
- Some 400 activities per year = 1500+ since 2014
- Capacity for virtual capacity building
- Cooperation with 120+ countries in 2022
- Joint projects with the European Union
- Voluntary contributions by Canada, Hungary, Iceland, Italy, Japan, Netherlands, UK and USA in 2020-23
- Support to T-CY

Current projects:
- GLACY+
- CyberEast
- CyberSouth
- iPROCEEDS-2
- Octopus
The Convention on Cybercrime: Backed up by capacity building

Projects managed by C-PROC support:

- 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

Rationale:

Support countries in the implementation of the Convention on Cybercrime

- Priority given to countries that are Parties to or that have requested accession to the Convention on Cybercrime
Benefits

✓ Stronger and more consistent legislation
✓ More efficient international cooperation between Parties
✓ More investigation, prosecution, adjudication of cybercrime and e-evidence cases
✓ Trusted partnerships and public/private cooperation
✓ Catalyst for capacity building
✓ Better cybersecurity performance
✓ Participation in the Cybercrime Convention Committee (T-CY)
✓ Participation in future standard setting (Guidance Notes, Protocols and other additions to Budapest Convention)
✓ Contribution to human rights/rule of law in cyberspace

“Cost”: Commitment to cooperate

Disadvantages?
www.coe.int/cybercrime