

BUDAPEST CONVENTION AND THE COUNCIL OF EUROPE APPROACH

GLACY - Launching conference & workshops (Senegal, 24-27 March 2014)



COUNCIL OF EUROPE APPROACH

Follow up and Assessment:

**Cybercrime Convention
Committee (T-CY)**

Standards:

- **Budapest Convention
Cybercrime**
- **and related standards**

**Fighting
against
cybercrime**

Capacity building

A dynamic framework



COUNCIL OF EUROPE: STANDARDS, CAPACITY BUILDING, ASSESSMENT

1. Adoption of the Budapest Convention on Cybercrime in 2001

2. Cybercrime Convention Committee (T-CY)

3. Capacity Building Programme

- **Global Project on Cybercrime (Phase 1)**
- **Global Project on Cybercrime (Phase 2)**
- **Joint Project on Cybercrime in Georgia**
- **Cybercrime@IPA Joint Project on Cybercrime in South-eastern Europe**
- **Cybercrime@EAP Joint Project on Cybercrime in Eastern Partnership Countries**
- **Global Project on Cybercrime (Phase 3)**
- **GLACY – Joint Project on Global Action on Cybercrime**

BUDAPEST CONVENTION: CRIMINAL JUSTICE TREATY

- **Criminalising conduct**
- **CyberCRIME**
- **Rule of Law + Human Rights Principles**

**A framework for an effective international criminal justice
response to cybercrime**

Contents 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**
- **Search and seizure**
- **Interception of computer data**

+

International cooperation

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

Harmonisation

ELECTRONIC EVIDENCE

- **Any crime may entail electronic evidence - on a laptop, smart phone, tablet, server or any other computer or storage device.**
- **Examples:** location data proving that a suspected offender was at the crime scene, traffic data in a corruption case proving that two persons communicated, communications proving membership in a criminal organisation, etc.
- **Cybercrime is thus not only a specific form of crime, but also – in particular when considering the question of electronic evidence – a horizontal issue and can be an element in almost any type of crime.**
- **Electronic evidence brings major challenges for criminal justice authorities.**

BUDAPEST CONVENTION: STATUS

Opened for signature November 2001 in Budapest

As at March 2014:

- **42 parties (36 European, Australia, Dominican Republic, Japan , Mauritius, Panama and USA)**
- **11 signatories (European, Canada, South Africa)**
- **9 States invited to accede (Argentina, Chile, Colombia, Costa Rica, Israel, Mexico, Morocco, Philippines, Senegal)**
- = **62 States are parties/are committed to become parties/participate in Cybercrime Convention Committee at present**

- **Additional invitations to accede are in process**

- **Many more have used Budapest Convention as a guideline for domestic legislation**

Art 37: Open to any country to become Party

Cybercrime Convention Committee (T-CY) – Article 46

Membership (status March 2014:

- **42 Members (State Parties)**
- **Observer States**
- **10 International organisations (African Union Commission, ENISA, European Union, Europol, INTERPOL, ITU, OAS, OECD, OSCE, UNODC)**

Activities (examples):

- **Assessment in 2012 of expedited preservation provisions (Articles 16, 17, 29 and 30)**
- **Assessment in 2013 and 2014 of efficiency of international cooperation (Article 31 etc.)**
- **Guidance Notes (“botnets”, “spam”, “ID-fraud” etc.)**
- **Transborder access to data (Analysis of Article 32)**
- **Functioning of network of 24/7 contact points**

CAPACITY BUILDING

BROAD INTERNATIONAL SUPPORT

- **Enable criminal justice authorities to meet the challenge of cybercrime and electronic evidence**
- **Entails strengthening the knowledge and skills and enhancing the performance of criminal justice organisations**
- **Help protect individuals and society against crime and protect the rights of individuals**
- **Promote security, confidence and trust in ICT**

ELEMENTS OF CAPACITY BUILDING PROGRAMMES

- **CYBERCRIME POLICIES AND STRATEGIES**
- **LEGISLATION**
- **CYBERCRIME REPORTING**
- **PREVENTION**
- **SPECIALISED UNITS**
- **LAW ENFORCEMENT TRAINING**
- **JUDICIAL TRAINING**
- **PUBLIC/PRIVATE COOPERATION**
- **INTERNATIONAL COOPERATION**
- **PROTECTION OF CHILDREN**
- **FINANCIAL INVESTIGATIONS AND PREVENTION OF FRAUD AND MONEY LAUNDERING**
- **PREVENTION AND CONTROL OF TERRORIST USE OF ICT**

COUNCIL OF EUROPE PROJECTS: EXAMPLE OF SEQUENCING



C-PROC: CYBERCRIME PROGRAMME OFFICE OF THE COUNCIL OF EUROPE

- **Offer by the prime minister of Romania the Council of Europe**
- **Decision in October 2013 to establish a cybercrime Programme Office in Bucharest, Romania.**
- **The C-PROC will be responsible for the implementation of the capacity building projects of the Council of Europe on cybercrime and electronic evidence worldwide.**
- **The added value includes specialisation, cost-effective project management, competitiveness and thus increased resource mobilisation.**

Impact of the Council of Europe approach

- **Stronger and more harmonised legislation**
- **More efficient international cooperation between Parties**
- **Increase the number of investigation, prosecution and adjudication of cybercrime and e-evidence cases**
- **Trusted partnerships and public/private cooperation**
- **Contribution to human rights/rule of law in cyberspace**

The Budapest Convention is in place and functioning.

Obstacles:

- 1. Limited criminal justice capacities**
- 2. Political disagreements**

THANK YOU FOR YOUR

ATTENTION

cschulman@just.ro