

Council of Europe  
Conseil de l'Europe



European Union  
Union européenne

---

## Project on Cybercrime in Georgia

# Convention on Cybercrime: a framework for comprehensive legislation and joint action against cybercrime

---

***Regional Workshop on Cybercrime, Tbilisi, Georgia 13 May 2010***

---

Cristina Schulman  
Council of Europe  
Strasbourg, France  
Tel +33-3-8841-2103  
[cristina.schulman@coe.int](mailto:cristina.schulman@coe.int)

[www.coe.int/cybercrime](http://www.coe.int/cybercrime)



# Fighting Cybercrime – what approach?

---

High-tech crime units

Judicial training

LEA-ISP cooperation  
(guidelines 2008)

## **Budapest Convention**

- Criminalising conduct
- Investigative tools  
(procedural law)
- Legal framework for  
international  
cooperation

Efficient MLA

24/7 points of contact

Guideline on legislation for more  
100 countries

Other treaties,  
laws and  
instruments

Online protection of children against  
sexual exploitation



# The Convention on Cybercrime: status

Elaborated by the Council of Europe with the participation of Canada, Japan, South Africa and the USA

In 2001 the Convention was adopted/opened for signature and entered into force on 1.07.2004

5 countries (Costa Rica, the Dominican Republic, Mexico, Philippines and Chile) have been invited to accede

2 more countries requested accession

Total number of signatures not followed by ratifications:	17
Total number of ratifications/accessions:	29

- Art 36 - Signature and entry into force (open to member States and non-members which have participated in its elaboration)
- Art 37 - Accession (any State may accede following majority vote in Committee of Ministers and unanimous vote by the parties entitled to sit on the Committee of Ministers)



## Status of signatures and ratifications of the Convention on Cybercrime

Ratified (29):		Signed (17):	Not signed (5 CoE member States):	Invited to accede (4):
<b>Albania</b> <b>Armenia</b> <b>Azerbaijan (2010)</b> <b>Bosnia and Herzegovina</b> <b>Bulgaria</b> <b>Croatia</b> <b>Cyprus</b> <b>Denmark</b> <b>Estonia</b> <b>Finland</b> <b>France</b> <b>Germany (2009)</b> <b>Hungary</b> <b>Iceland</b> <b>Italy</b> <b>Latvia</b> <b>Lithuania</b> <b>Moldova (2009)</b> <b>Montenegro (2010)</b>	<b>Netherlands</b> <b>Norway</b> <b>Portugal (2010)</b> <b>Romania</b> <b>Serbia (2009)</b> <b>Slovakia</b> <b>Slovenia</b> <b>FYROM</b> <b>Ukraine</b> <b>United States of America</b>	<b>Austria</b> <b>Belgium</b> <b>Canada</b> <b>Czech Rep</b> <b>Georgia</b> <b>Greece</b> <b>Ireland</b> <b>Japan</b> <b>Liechtenstein</b> <b>Luxembourg</b> <b>Malta</b> <b>Poland</b> <b>South Africa</b> <b>Spain</b> <b>Sweden</b> <b>Switzerland</b> <b>United Kingdom</b>	<b>Andorra</b> <b>Monaco</b> <b>Russian Federation</b> <b>San Marino</b> <b>Turkey</b>	<b>Costa Rica</b> <b>Dominican Republic</b> <b>Mexico</b> <b>Philippines</b> <b>Chile</b>

## **Budapest Convention on Cybercrime: a comprehensive legal instrument**

- Harmonize the domestic criminal substantive law elements of offences and
- Provide procedural law powers necessary for the investigation and prosecution of such offences as well as of other offences committed by means of a computer system

### **Model law function of the Convention**

- Use as a checklist
- Compare provisions
- Use wording

**Country profiles on cybercrime legislation as a tool for analysis and sharing of good practices**

**Art 9 - Child pornography**

**Art 6 - Misuse of devices**

 **Art 4 - System interference**

**Art 16- Expedited preservation**

**Art 18 - Production order**

 [www.coe.int/cybercrime](http://www.coe.int/cybercrime)

# The Convention serves as a framework for international cooperation against cybercrime

- Harmonisation of legislation
- Chapter 3 of the Convention provides the legal and institutional basis for international law enforcement and judicial cooperation with other parties to the Convention
- Tools and obligations to cooperate
- Participation in the Consultations of the Parties (Cybercrime Convention Committee, T-CY) = participation in future work on the Convention

By becoming a party to this treaty, any country can make use of this framework and cooperate with:

- Europe
- Asia
- Africa
- Australia
- South and North America

# **Budapest Convention on cybercrime**

- The only multilateral treaty dealing with cybercrime matters already implemented in many countries while others are taking into consideration to become Party
- Proven value as a guideline for drafting legislation on cybercrime
- Provides important tools for law enforcement to investigate cybercrime
- Ensure adequate protection of human rights and liberties according to the relevant international documents
- Flexible mechanisms to adapt its provisions to different legal systems

## **CC provides for countries:**

- Coherent national approach to legislation on cybercrime
- Harmonisation of criminal law provisions on cybercrime with those of other countries
- Legal and institutional basis for international LE and judicial cooperation
- Participation in the Consultations of the Parties
- The treaty as a platform facilitating public-private cooperation



**Convention provides global standards and a framework for an effective fast international cooperation**

## Global Project on Cybercrime (Phase 2)

21-22 Jan 10	Washington D.C	Sixth Meeting of the REMJA Working Group on Cyber-Crime
26-28 Jan 10	Manila, Philippines	ASEAN/APRIS workshop on cybercrime legislation
2-3 Feb 10	Abuja, Nigeria	1st West African Internet Fraud
10 Feb 10	Buenos Aires	Meeting on Convention on Cybercrime
16-18 Feb 10	Malta	MENA Cybercrime Legislation Workshop
17-18 Feb 10	Brussels	EastWest Institute - the 7th Worldwide Security Conference
23-24 Feb 10	Pakistan	Cybercrime training for law enforcement and judge
16-17 Mar 10	Barcelona, Spain	SecureCloud 2010 -- ENISA joint Conference on Cloud Computing
23-25 Mar 10	Strasbourg	Octopus Interface conference
31 Mar – 1 Apr10	Lille	French National Gendarmerie: International Forum on Cybercrime
12-19 Apr 10	Salvador, Brazil	The 12th United Nations Congress on Crime Prevention and Criminal Justice
29-30 Apr 10	Madrid	EuroDIG 2010
12-13 May 10	Burbank, California, USA	POLCYB International Conference 2010
June (tbc)	Colombia	Meeting with LA countries on accession to the Convention on Cybercrime
9-11 June 10	Izmir, Turkey	International Informatics Law Assembly
7- 12 June 10	Malta	Legal Frameworks for ICTs
24-25 of June	Paris	Cybercrime Convention Committee (T-CY) plenary meeting
5-7 July 10	Rabat	Atelier de formation sur l'harmonisation du cadre légal pour la cybersécurité en Afrique du Nord
6-8 July 10	Odessa, Ukraine	Regional workshop: Protecting children against sexual exploitation and sexual abuse
August (tbc)	Mexico	Workshop on cybercrime legislation



## **Legislation and policies: Cybercrime policies and legislation strengthened in accordance with the Convention on Cybercrime and its Protocol**

---

### **2009 (March)– 2010 (April)**

- Germany, Moldova, Serbia, Montenegro, Azerbaijan and Portugal ratified the Convention on Cybercrime
- Chile was invited to accede to the Convention
- Australia and Argentina requested accession
- Montenegro, Portugal Romania and Serbia ratified the Protocol on Xenophobia and Racism committed through Computer Systems
- In Portugal, the laws on the implementing the Convention and the Protocol were adopted
- Reforms in Bosnia and Herzegovina and “the former Yugoslav Republic of Macedonia” have been initiated. Both are parties to the Convention on Cybercrime but legislation does yet not comply fully with the treaty
- Cooperation with Morocco was taken up again and Morocco could seek accession to the Convention
- Legislative advice was provided to Senegal. Given the law on cybercrime adopted in 2008, Senegal could seek accession to the Convention on Cybercrime
- Legislative advice was also provided to Nigeria and Uganda. Unless support to reform efforts in Africa is intensified, Africa will become a major source of cybercrime given the expansion of fibre optic networks on this continent
- Legislative advice was also provided to Montenegro, Vietnam, Korea, Cambodia, Laos, Indonesia, Philippines, Singapore, Thailand, Malaysia
- Contribute to regional legislative workshops in Asia, Africa and Latin America



# **The EU/COE Joint Project on Cybercrime in Georgia**

---

## **Objectives:**

- Legislative proposals to bring Georgian legislation fully in line with the Convention on Cybercrime and related European standards on data protection;
- Training policies and modules;
- Proposals for institution building;
- Law enforcement/internet service provider cooperation.

## **Results:**

- Legislation
  - Draft amendments in line with the Convention on Cybercrime and related European standards on data protection to be submitted to the Government;
- Training policies and modules
  - train the trainers course
  - training materials available
  - involve Georgia in developing the concept cybercrime training for judges and prosecutors
  - implement the concept paper in Georgia
- Proposals for institution building
  - expert report: assessment and making proposals
  - MoAI decision on HTC unit
  - formally to be established once the new legislation enters into force
- LEA/ISPs cooperation
  - workshop on LEA/ISP
  - legislation in place needed to allow such cooperation
  - memorandum to be concluded

# COE/UE cooperation on Cybercrime

- ▶ **Stockholm Programme for 2010-2014** adopted in December 2009: *“As soon as possible, Member States should ratify the 2001 Council of Europe Cyber-crime Convention. This Convention should become the legal framework of reference for fighting cyber-crime at global level – section 4.4.4)*
- ▶ **Council Conclusions Concerning an Action Plan** to Implement the Concerted Strategy to Combat Cybercrime (3010th General Affairs Council Meeting, Luxembourg, 26 April 2010): *“The European Council's call on Member States, as laid down in the Stockholm Programme, to ratify the 2001 Council of Europe Cybercrime Convention as soon as possible, to give their full support to the national alert platforms in charge of the fight against cybercrime and the Council's emphasis on the need for cooperation with countries outside the European Union, and also its invitation to:*
  - ▶ *· the Commission to take measures for enhancing/improving public private partnerships,*
  - ▶ *· and Europol to step up strategic analysis on cyber crime”.*
- ▶ **12th UN Congress on Crime Prevention and Criminal Justice** (Salvador, Brazil, 12-19 April 2010): *Need for a global capacity building effort to strengthen the full implementation of existing treaties and standards*

# Need for a global capacity building effort

1. Global review of needs (UNODC, COE, US, European Union, etc) to carry out a global review of needs and propose an action plan to address those needs.
  2. This should be accompanied by a global effort to mobilise donor funding for technical assistance against cybercrime.
  3. Based on the needs analysis, international and bi-lateral organisations to provide specific support to countries to:
    - ✓ Strengthen legislation and its implementation
    - ✓ Train law enforcement, prosecutors and judges
    - ✓ Establish high-tech crime units
    - ✓ Make international cooperation more efficient
    - ✓ Join 24/7 network of contact points
    - ✓ Improve public/private cooperation
    - ✓ Enhance the protection of children
- **Review needs**
  - **Provide support**
  - **Assess progress**



---

*THANK YOU FOR YOUR  
ATTENTION*

*cristina.schulman@coe.int*

