



www.coe.int/cybercrime

International standards on cybercrime: Council of Europe Convention on cybercrime

The advantages for Georgia to become Party to the Convention

Cristina Schulman
Council of Europe
Strasbourg, France
Tel +33-3-8841-2103
cristina.schulman@coe.int



Global trends

- Cybercrime - form of **economic crime** for illicit proceeds through: identity theft and related fraud and other types of scams
- Offenders are **increasingly organising** to commit cybercrime
- **Spam** is spreading not only as a nuisance but as a vector for malware
- A **proliferation of child abuse materials** and offenders is noted and with it the commercial sexual exploitation of children
- **Terrorists use ICT**, including
 - for propaganda, fund raising, recruitment and training
 - for logistical purposes such as target identification, communication or money laundering
 - the possible risk of terrorist attacks against critical infrastructure



Challenges

- **Electronic evidence** (related to cybercrime or any crime) is volatile evidence and needs to be preserved in an urgent and efficient manner
- Cybercrime is **transnational crime**; evidence (e.g. traffic data, subscriber information, content data) may be stored in multiple jurisdictions.
- The investigation of cybercrimes requires the **cooperation between LEA and ISPs** that have to consider the different roles of LEA (to uphold the law) and ISPs (to provide services to their clients) and the need for both to protect privacy, freedom of expression and other fundamental rights of internet users
- In 2008 the German Constitutional Court: *as people rely on ICT to communicate, express themselves and store their private information, the confidentiality, integrity and availability of computer data and systems is a fundamental right.*



The approach against cybercrime

Standards:

Convention on Cybercrime
Protocol on Xenophobia and Racism
Convention on the Protection of Children against Sexual Exploitation and Sexual Abuse

Council of Europe action against cybercrime

Future development:
Cybercrime Convention Committee (T-CY)

Implementation:
Project on Cybercrime (Phase 1)
Project on cybercrime (Phase 2)



The Council of Europe Convention on Cybercrime

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

2001 - Convention was adopted and opened for signature
entered into force on 1.07.2004

Costa Rica, the Dominican Republic, Mexico, Philippines, and soon Chile have been invited to accede

Total number of signatures not followed by ratifications:	20
Total number of ratifications/accessions:	26

- 
- 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)
-
- 

Why Council of Europe Convention?

- The only multilateral treaty dealing with cybercrime matters already implemented in many countries while others are taking into consideration to become Party
- A guideline for drafting the 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 avoid conflicts with national legislations and proceedings

Major global trend towards better cybercrime legislation



Convention provides a global standard

The aims of the Convention



Harmonize the domestic criminal substantive law elements of offences



Provide procedural law powers necessary for the investigation and prosecution of such offences as well as other offences committed by means of a computer system



Establish a framework for an effective and fast international cooperation



Structure and content of the Convention

- **Chapter I: Definitions**

- **Chapter II: Measures at national level**
 - Section 1 - Substantive criminal law**
 - Section 2 - Procedural law**
 - Section 3 - Jurisdiction**

- **Chapter III: International cooperation**
 - Section 1 - General principles**
 - Section 2 - Specific provisions**

- **Chapter IV: Final provisions**



Chapter II – Measures at national level

Section 1 – Substantive criminal law

Title 1 - Offences against the confidentiality, integrity and availability of computer data and systems:

- **illegal access**
- **illegal interception**
- **data interference**
- **system interference**
- **misuse of devices**

Title 2 – Computer-related offences:

- **Computer - related forgery**
- **Computer - related fraud**

Title 3 – Content-related offences (child pornography)

Title 4 – Infringements of copyright and related rights

Title 5 – Ancillary liability and sanctions (attempt and aiding or abetting, corporate liability, sanctions and measures)



Chapter II – Measures at national level

Section 2 – Procedural law

- Title 1 – Common provisions (scope of procedural provisions, conditions and safeguards)
 - Title 2 – Expedited preservation of stored computer data (expedited preservation of stored computer data/traffic data and partial disclosure of traffic data)
 - Title 3 – Production order
 - Title 4 – Search and seizure of stored computer data
 - Title 5 – Real-time collection of computer data (traffic data, interception of content data)
-
- Scope of procedural provisions: apply to:
 - *criminal offences provided by Art. 2 - 11 of the Convention;*
 - *other criminal offences committed by means of a computer system; and*
 - *collection of evidence in electronic form of a criminal offence*

Chapter III – International co-operation

Section 1 – General principles

- Art.23 - General principles on international cooperation
- Art .24 - Principles related to extradition
- Art. 25 - Principles related to mutual legal assistance
- Art. 26 - Spontaneous information
- Art.27 - MLA in the absence of applicable international instruments
- Art.28 - Confidentiality and limitation on use

Section 2 - Specific provisions

- Art.29 - Expedited preservation of stored computer data
- Art.30 - Expedited disclosure of preserved traffic data
- Art.31 - Mutual assistance regarding accessing of stored computer data
- Art.32 -Trans-border access to stored computer data with consent or where publicly available
- Art.33 - Mutual assistance in the real-time collection of traffic data
- Art.34 - Mutual assistance regarding the interception of content data



Model law function of the Convention

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

Provision of Convention	Provision in national law
Art 4 System interference	?
Art 6 Misuse of devices	?
Art 9 Child pornography	?
Art 16 Expedited preservation	?
Art 18 Production order	?

Cybercrime Legislation - Country profiles

www.coe.int/cybercrime

[Albania](#)

[Argentina](#)

[Armenia](#)

[Austria](#)

[Belgium](#)

[Brazil](#)

[Bulgaria](#)

[China, People's Republic:
Country Profile and
Analytical Study](#)

[Croatia](#)

[Cyprus](#)

[Czech Republic](#)

[Dominican Republic](#)

[Estonia](#)

[France](#)

[Germany](#)

[Finland](#)

[Hungary](#)

[Indonesia](#)

[Italy](#)

[Lithuania](#)

[Mexico](#)

[Moldova](#)

[Morocco](#)

[Philippines](#)

[Portugal](#)

[Romania](#)

[Russian Federation](#)

[Slovak Republic](#)

["the former Yugoslav
Republic of Macedonia"](#)

[Turkey](#)

[Ukraine](#)

[United States of America](#)



Project on cybercrime (phase 1)

September 2006 - February 2009

Project objective:	To promote broad implementation of the Convention on Cybercrime (ETS 185) and its Protocol on Xenophobia and Racism (ETS 189)
Output 1:	Legislation - Draft laws meeting the standards of ETS 185 and 189
Output 2:	Capacities of criminal justice systems strengthened to investigate, prosecute and adjudicate cybercrime
Output 3:	Capacities of criminal justice bodies to cooperate internationally re-enforced

Funding: CoE, Microsoft, Estonia

Final Report



www.coe.int/cybercrime



Activities (September 2006 – February 2009)

- **Africa:** activities in *Benin, Egypt, Niger, Nigeria, South Africa*,
Contribute to regional activities: *2 regional workshops organized in Benin and Nairobi; Kenya and a Pan-African conference in Yamoussoukro (Ivory Coast)*
- **Arab region:** *workshop on cybercrime for prosecutors of the Arab region (Casablanca, Morocco); Conference on Combating Cybercrime in countries of the Gulf Cooperation Council in Abu Dhabi; first regional conference on cybercrime (Cairo)*
- **Asia:** activities in *India, Indonesia, Japan, Pakistan, Philippines, Sri Lanka; ASEAN Secretariat, the European Commission funded APRIS II Project and the CoE Project on Cybercrime - joint workshop on cybercrime legislation for ASEAN countries (Brunei Darussalam, Cambodia, Indonesia, Laos, Malaysia, Philippines, Singapore, Vietnam)*
- **Australia:** AUSCERT conference in Brisbane
- **Europe:** *Belarus, Georgia, Romania, Russian Federation, Serbia, Ukraine*
- **Regional and other activities in South-eastern Europe:** Project on Cybercrime; PACO Serbia; PROSECO project on networking among prosecutors helped: legislation passed in Serbia, draft law prepared in Montenegro in view of future ratification, Albania passed amendments to implement the Convention and its Protocol, preparation of further amendments in FYROM, support for creation of 24/7 contact points in BiH and Serbia, regional conference on cybercrime in Belgrade, regional workshop on cybercrime legislation and the training of judges in Plovdiv, Bulgaria, legislative workshops in Kosovo, BiH and Montenegro
- **Latin America and Caribbean:** *Argentina, Brazil, Colombia, Costa Rica, Dominican Republic; Cybercrime Legislation Drafting Workshop” for countries of the Caribbean; Cybercrime Legislation Drafting Workshop for countries of Latin America*
- **Global events and cooperation with other organisations**
- **Discussion papers and studies were launched under the Project on Cybercrime**

Results - Output 1: Legislation

- Convention presented to representatives from more than 150 countries around the world through different types of meetings
- “Legislative profiles” have been prepared for more than 90 countries that served as bases for regional and country-specific workshops on cybercrime legislation and helped share good practices
- More than 100 countries around the world either have cybercrime legislation in place or are in process of preparing legislation using the Convention on Cybercrime as a guideline or “model law”
- The legislative processes that the project was able to support and initiate since its launching in 2006 exceeded expectations

Ratifications/accessions to the Convention (September 2006 – July 2009)

- The **call for ratification of the EU Justice and Home Affairs Council of November 2007** and again in November 2008 may help accelerate this process among EU Members states.
- 5 member States of the CoE (Andorra, Monaco, Russia, San Marino and Turkey) had not yet signed the Convention.
- Germany, Serbia and Moldova ratified in 2009.

Ratification of the Convention on Cybercrime since November 2001

Year	Year 1	Year 2	Year 3	Year 4	Year 5	Year 6	Year 7	Year 8
	2002	2003	2004	2005	2006	2007	2008	2009
Add. Ratif.	+ 2	+2	+4	+3	+7	+3	+2	+3
Total	2	4	8	11	18	21	23	26

Status of signatures and ratifications of the Convention on Cybercrime

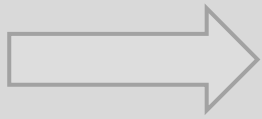
Ratified (26):	Signed (20):	Not signed (5 CoE member States):	Invited to accede (4):	Request for accession (1):
Albania Armenia Bosnia and Herzegovina Bulgaria Croatia Cyprus Denmark Estonia Finland France Germany (2009) Hungary Iceland Italy Latvia Lithuania Moldova (2009) Netherlands Norway Romania Serbia (2009) Slovakia Slovenia FYROM Ukraine United States of America	Azerbaijan Austria Belgium Canada Czech Rep Georgia Greece Ireland Japan Liechtenstein Luxembourg Malta Montenegro Poland Portugal South Africa Spain Sweden Switzerland United Kingdom	Andorra Monaco Russian Federation San Marino Turkey	Costa Rica Dominican Republic Mexico Philippines	Chile

Results - Output 2: Criminal justice capacities

- **Implementation of the procedural law tools of the Convention**
 - Several hundred police officers and prosecutors participated in activities around the world where the procedural provisions of the Convention were explained
 - Training events specifically aimed at forensic investigators and others at prosecutors.
- **Law enforcement – ISP cooperation**
- **Training:**
 - contributed to efforts for the harmonisation of law enforcement training (working group led by Europol) and creation of centres of excellence for training in cybercrime investigations and forensics (2Centre initiative supported by the public and private sector).
 - draft training manual for judges
 - ground has thus been prepared to move towards institutionalising cybercrime training for judges and prosecutors in the future.

Results - Output 3: International cooperation

- ▶ **By February 2009, 50 countries signed/ratified/invited to accede the treaty**
- ▶ **Once they are all full parties, the value of the Convention as a framework for international cooperation will be greatly enhanced**
- ▶ **Project promoted the creation of 24/7 points of contact in a number of countries**
- ▶ **October 2007, a study was launched to document good practices in the implementation of the international cooperation provisions of the Convention**
- ▶ **Report on the effectiveness of the network of 24/7 contact points was prepared between September 2008 and February 2009**



Project on cybercrime (phase 2)

www.coe.int/cybercrime

Project objective	To promote broad implementation of the Convention on Cybercrime (ETS 185) and its Protocol on Xenophobia and Racism (ETS 189) and related international standards
Output 1	Legislation and policies: Cybercrime policies and legislation strengthened in accordance with the Convention on Cybercrime and its Protocol
Output 2	International cooperation: Capacities of 24/7 points of contact, prosecutors and of authorities for mutual legal assistance strengthened
Output 3	Investigation: Law enforcement – service provider cooperation in the investigation of cybercrime improved on the basis of the guidelines adopted in April 2008
Output 4	Financial investigations: enhanced knowledge among high tech crime units and FIUs to follow money flows on the internet
Output 5	Training: Judges and prosecutors trained in the adjudication and prosecution of cybercrime
Output 6	Data protection and privacy: Data protection and privacy regulations in connection with cybercrime investigations improved in line with CoE and other relevant international standards
Output 7	Exploitation of children and trafficking in human beings: Enhanced knowledge of standards against the sexual exploitation and abuse of children and trafficking in human beings on the internet

Funding: Romania, Microsoft, McAfee

Investigation: Law enforcement – service provider cooperation in the investigation of cybercrime improved on the basis of the guidelines adopted in April 2008

Approach



1. Guidelines for LEA – ISP cooperation (adopted on 2 April 2008, Strasbourg)



2. What should be the responsibility or liability of service providers for child abuse materials that are made available through their systems?

▪How far ISP have the obligation to prevent crimes or support investigations?

▪How far the failure of the ISP to act in accordance with its obligations leads to consequences and what these consequences are?




Improving public-private (in particular law enforcement – ISP) cooperation in the investigation of cybercrime




CoE instruments:

Provide the foundation for LEA- ISP cooperation



The Guideline was drafted (October 2007 and March 2008) by a WG consisting of industry (Microsoft, eBay, EuroISPA, service provider associations of France and Germany and others) and LEA representatives (from France and Germany).



To be **disseminated all over the world** in order to help law enforcement and ISPs structure their cooperation:

✓ **EC event** (Brussels, 25-26 September 2008); participants agreed on a set of recommendations on law enforcement – ISP cooperation based on the COE guidelines (adopted by the 2987th Justice and Home Affairs Council meeting (Brussels, 27-28 November 2008).

✓ **round table discussion in Washington DC** on 30 January 2009 to present the law enforcement – ISP cooperation guidelines and other relevant tools of COE ensuring the rule of law in cybercrime investigations involving service providers

✓ guidelines served as a basis for the draft agreement between the French service provider association and the Ministry of Interior

✓ Romania, Ukraine, India etc



Provisions addressing criminalization of sexual exploitation of children on Internet

Convention on Cybercrime, Budapest, 23.11.2001

Article 9 – Offences related to child pornography

Procedural law + International cooperation provisions

Convention on the Protection of Children against Sexual Exploitation and Sexual Abuse (2007)

- ▶ Article 23 – Solicitation of children for sexual purposes
- ▶ Article 18 a) – Sexual abuse
- ▶ Article 20 a) f) – Offences concerning child pornography

- ✓ preventive and protective measures;
- ✓ assistance to child victims and their families;
- ✓ intervention programmes or measures for child sex offenders;
- ✓ criminal offences, including several entirely new offences, such as child grooming;
- ✓ child-friendly procedures for investigation and prosecution;
- ✓ recording and storing of data on convicted sex offenders;
- ✓ international co-operation;
- ✓ a monitoring mechanism.



what offences should be addressed by the different countries:

Convention on Cybercrime					Convention on the Protection of Children against Sexual Exploitation and Sexual Abuse		
Producing child porn for the purpose of its distribution through a computer system	Offering or making available child porn through a computer system	Distributing or transmitting child porn through a computer system	Procuring child porn through a computer system for oneself or for another person	Possessing child porn in a computer system or on a computer-data storage medium	Knowingly obtaining access, through information and communication technologie, to child porn	Intentional proposal, through information and communication technologies, of an adult to meet a child for the purpose of engaging in sexual activities with a child who, according to the relevant provisions of national law, has not reached the legal age for sexual activities	Intentional proposal, through information and communication technologies, of an adult to meet a child for the purpose of producing child porn



definition of “child pornography” within the framework provided by CC and CPC:

Legal provisions determine that "child pornography" comprises pornographic material that visually depicts:

Convention on Cybercrime		Convention on the Protection of Children against Sexual Exploitation and Sexual Abuse	
A minor engaged in sexually explicit conduct	A person appearing to be a minor engaged in sexually explicit conduct	Realistic images representing a minor engaged in sexually explicit conduct	Any depiction of a child's sexual organs for primarily sexual purposes





Project on cybercrime in Georgia

www.coe.int/cybercrime

1 June 2009 - 31 May 2010

Project objective	<p>The overall objective of the project is to contribute to the security of and confidence in information and communication technologies in Georgia.</p> <p>The purpose of the project is to help Georgia develop a consistent policy on cybercrime in view of implementing the Convention on Cybercrime (ETS 185).</p>
Output 1	<p>Legislation: Legislative proposals will be available to bring Georgian legislation fully in line with the Convention on Cybercrime and related European standards on data protection</p>
Output 2:	<p>Training: Training policies and modules are available for standard training courses for law enforcement authorities, prosecutors and judges regarding the investigation, prosecution and adjudication of cybercrime</p>
Output 3:	<p>Institution building: Proposals available for the creation of a 24/7 point of contact for international police cooperation, the establishment of a high-tech crime unit within the police and competent authorities for international judicial cooperation in cybercrime cases</p>
Output 4	<p>Law enforcement/internet service provider cooperation: Policy available regarding law enforcement authorities and Internet service provider cooperation in the investigation of cybercrime in line with Georgian legislation and the guidelines adopted at the Council of Europe in April 2008</p>

Funding: European Commission and Council of Europe

**Counterpart
institutions**

**Ministry of Justice of Georgia
Ministry of Internal Affairs of Georgia**

Issues

➤ FACTORS THAT PREVENT RATIFICATION

- Complex legislative reforms of criminal law in order to comply with the Convention and to ensure the protection of fundamental human rights
- Cybercrime not always a priority of governments/parliaments and the seriousness of this threat is often ignored

➤ TRAINING FOR POLICE, JUDGES AND PROSECUTORS

➤ COOPERATION BETWEEN LEA AND ISP (clear standards for public/private sector cooperation)

➤ INTERNATIONAL COOPERATION

- Need to enhance the number of countries that are party to the Convention
- Need to make 24/7 points of contact more effective
- Preliminary measures (e.g. expedited preservation) need to be followed up by efficient MLA process
- Speed up judicial cooperation

➤ FUTURE DEVELOPMENT

- Cybercrime keep evolving: need continues review of the international response

Ratification of the Convention: benefits for Georgia and other countries

- **Coherent national approach to legislation on cybercrime**
- **Facilitates the gathering of electronic evidence**
- **Facilitates the investigation of cyberlaundering, cyberterrorism and other serious crime**
- **Harmonisation and compatibility of criminal law provisions on cybercrime with those of other countries**
- **Legal and institutional basis for international law enforcement and judicial cooperation with other parties to the Convention**
- **Participation in the Consultations of the Parties**
- **The treaty as a platform facilitating public-private cooperation**

*THANK YOU FOR YOUR
ATTENTION*

crisrina.schulman@coe.int

