Cybercrime

I. In brief

With the increasing reliance on information and communication technologies, societies worldwide have become vulnerable to threats such as cybercrime. Cybercrime is a transnational crime. Attacks may be launched from anywhere and affect victims in Europe.

Cybercrime is about offences against, as well as by, means of computer systems. And any crime may entail electronic evidence found on computer systems.

The approach of the Council of Europe consists of a triangle of:

- Standards with the Budapest Convention on Cybercrime (www.coe.int/cybercrime) as the only binding international treaty addressing this challenge;
- Follow-up and assessment of implementation through the Cybercrime Convention Committee;
- Capacity-building through technical co-operation projects.

The Budapest Convention has a global vocation:

- Non-member States of the Council of Europe have ratified, signed or been invited to accede to this treaty.
- The Council of Europe has been co-operating with more than 120 countries worldwide.

The European Union strongly supports the implementation of the Budapest Convention not only in Europe but worldwide, as reflected in the Stockholm Programme on Justice, Freedom and Security (2010-14) and numerous other documents and decisions.

The EU has so far been funding several joint projects on cybercrime, including:

- Project on Cybercrime in Georgia;
- CyberCrime@IPA regional project on cybercrime in pre-accession countries of South-Eastern Europe;
- CyberCrime@EAP project on cybercrime under the Eastern Partnership Facility.

The EU also participates as an observer in the Cybercrime Convention Committee (T-CY).

The EU and the Council of Europe have agreed that further capacity-building is required in Europe and other regions of the world to help societies protect people and their rights and engage in international co-operation against cybercrime.

II. Background

The Budapest Convention on Cybercrime was opened for signature in 2001. Since 2006, the Cybercrime Convention Committee meets regularly: support to countries is provided through co-operation projects.

Measures against cybercrime are part of the Council of Europe's Internet governance strategy 2012 - 2015 that has been adopted by all 47 member States.

Cybercrime is thus not addressed in isolation but within the context of other Internet Governance issues and in relation to challenges such as data protection (Convention 108), online sexual violence against children (Lanzarote Convention), money-laundering and financial investigations as well as other rule of law and human rights concerns. The Budapest Convention is complemented by an additional Protocol on Xenophobia and Racism committed through Computer Systems.

The Budapest Convention on Cybercrime requires State Parties to:

- Criminalise offences against computer systems (illegal access, data and system interference and others) and by means of computer systems (fraud, child pornography and others);

- Provide criminal justice authorities with investigative tools (preservation, search, seizure, interception and others);
- Engage in efficient international co-operation (expedited preservation, mutual legal assistance, 24/7 network of contact points and others).

Any country able to implement its provisions can accede to this treaty. In addition to European countries, Japan and the USA have ratified and Canada and South Africa have signed it. Countries such as Australia, Argentina, Philippines, Senegal and others have been invited to accede.

The Cybercrime Convention Committee (T-CY) is the Committee of the Parties. Among other things, it carries out assessments and provides guidance to Parties to facilitate implementation of the treaty.

III. Comparative advantages and added value

These include:

- The Budapest Convention on Cybercrime is the only internationally-binding treaty addressing cyber-crime. It is unlikely that an international treaty of a similar scope and nature will be agreed upon and come into effect in the coming years.
- This treaty has a global vocation and has provided legislative guidance to more than 100 countries.
- Most of the Internet infrastructure and the most important service providers are located in the USA and most countries would need to co-operate with the USA in the investigation of cybercrime. The USA is a very active Party to the Budapest Convention.
- The EU supports the Budapest Convention as reflected in the Stockholm Programme and other decisions. Objectives include full implementation by all EU Member States but also implementation in other regions of the world.
- The Council of Europe and the EU have not only implemented successful joint projects on cybercrime but are closely co-operating at different levels, ranging from consultations on policies to practical matters (examples are a good practice study on specialised cybercrime units in co-operation with the EU Cybercrime Task Force in 2011 or co-operation in the assessment of data preservation and data retention provisions between the DG Home and the Cybercrime Convention Committee in 2012).
- The approach of the Council of Europe on cybercrime consists of a dynamic triangle of standards, monitoring and technical co-operation. This approach is unique and is producing results and impact.
- The Council of Europe is addressing cybercrime not in isolation but within the context of related Internet governance, rule of law and human rights challenges.
- The Council of Europe has a large network of contacts in the anti-cybercrime world in public and private sectors and is capable of assisting any country or region and co-operating with many public and private sector and international organisations.

Through technical co-operation projects, the Council of Europe can assist countries in establishing the necessary legal and operational capacities to apply the Budapest Convention in practice. For example:

- Support the adoption of cybercrime policies and strategies by governments http://www.coe.int/t/DGHL/cooperation/economiccrime/cybercrime/Documents/Reports-Presentations/2079_cy_strats_rep_V23_30march12.pdf
- Help strengthen and harmonise legislation with the Budapest Convention (including substantive and procedural law and rule of law safeguards) http://www.coe.int/t/DGHL/cooperation/economiccrime/cybercrime/Documents/CountryProfiles/default_en.asp http://www.coe.int/t/DGHL/cooperation/economiccrime/cybercrime/Documents/Reports-

Presentations/2467_SafeguardsRep_v18_29mar12.pdf

- Help establish specialised cybercrime or high-tech crime units http://www.coe.int/t/DGHL/cooperation/economiccrime/cybercrime/Documents/Reports-Presentations/Octopus2011/2467_HTCU_study_V30_9Nov11.pdf
- Introduce sustainable law enforcement training http://www.coe.int/t/DGHL/cooperation/economiccrime/cybercrime/Documents/Cyber%20IPA%20reports/2467_LEA_Training_Strategy_Fin1.pdf
- Provide guidance in the use of electronic evidence http://www.coe.int/t/dghl/cooperation/economiccrime/cybercrime/cy%20project%20balkan/Default_eeg_en.asp
- Institutionalise judicial training http://www.coe.int/t/dghl/cooperation/economiccrime/cybercrime/Documents/Training/default_en.asp
- Enhance public/private co-operation http://www.coe.int/t/dghl/cooperation/economiccrime/cybercrime/Documents/Reports-Presentations/567_prov-d-guidelines_provisional2_3April2008_en.pdf
- Promote efficient international co-operation http://www.coe.int/t/dghl/cooperation/economiccrime/cybercrime/Documents/Internationalcooperation/default_en.asp
- Help protect children against online sexual violence with Budapest and Lanzarote Conventions as criminal law benchmarks
- Promote financial investigations and the prevention and control of criminal money flows on the Internet http://www.coe.int/t/DGHL/cooperation/economiccrime/cybercrime/Documents/Reports-Presentations/MONEYVAL(2012)6_Reptyp_flows_en.pdf

Resources have been developed for all these fields.

IV. Geographic contextualisation

The EU and the CoE have been carrying out a number of joint projects addressing the question of cybercrime. For example:

- Cybercrime as a component of rule of law joint projects of the EU and CoE: The "PACO Serbia" project on economic crime (2006 – 2008) and the "PROSECO" project on a network of prosecutors in South-Eastern Europe (2008–2010), comprising of activities aimed at strengthening cybercrime legislation, the training of investigators, judges and prosecutors, and international co-operation against cybercrime.
- EU/CoE joint project on cybercrime in Georgia (2009/2010): this one-year joint project allowed Georgia to adopt legislation on cybercrime and on the protection of personal data; establish a high-tech crime unit; design training programmes for judges and prosecutors and conclude a memorandum of understanding between law enforcement authorities and Internet service providers. In June 2012, Georgia ratified the Budapest Convention.
- EU/CoE joint project on co-operation against cybercrime in EU pre-accession countries (2010 – 2013): this regional "Cybercrime@IPA" project covers eight countries and areas in South-Eastern Europe. It was launched in November 2010 and focuses on:
  - Cybercrime policies and strategies
  - Harmonisation of legislation
  - International co-operation
  - Law enforcement training
  - Financial investigations
  - Law enforcement/Internet service provider co-operation
  - Assessment of progress made.
- EU/COE Eastern Partnership regional project (2011-2013): This "Cybercrime@EAP" project was launched in April 2011 in six countries of Eastern Europe to provide advice and assess measures taken with regard to:
  - Cybercrime legislation
  - Specialised institutions
  - Judicial and law enforcement training

- Law enforcement/Internet service provider co-operation
- Financial investigations
- International co-operation.

While these Joint Projects have been limited geographically to Europe, the Council of Europe is implementing its Global Project on Cybercrime. It started in 2006 and is now in its 3rd phase.

- Results on Phase 1 (2006 – 2009) are available at:

http://www.coe.int/t/dghl/cooperation/economiccrime/cybercrime/cy%20Project/567-dinal%20report1i%20final%20_15%20june%2009_.pdf

- Results on Phase 2 (2009 – 2011) are available at:

http://www.coe.int/t/dghl/cooperation/economiccrime/cybercrime/Documents/Reports-Presentations/2079_adm_finalreport_V12_9apr12.pdf

The tools and materials developed under these projects are replicable and can be adapted to any national or regional context. Some of them have been translated into multiple languages and used in all regions of the world. Examples include the Guidelines on law enforcement/Internet service provider co-operation or the Concept for judicial training. This will also be the case for the judicial training materials or the Electronic evidence guide that are under preparation.

Given the political support of the EU to the Budapest Convention on Cybercrime; the positive experience of joint projects on cybercrime in Europe; the co-operation of the Council of Europe in this matter with countries worldwide and the standards, tools and materials already developed, both organisations are well positioned to engage in joint projects on cybercrime not only in Europe but in any country or region prepared to co-operate against cybercrime.