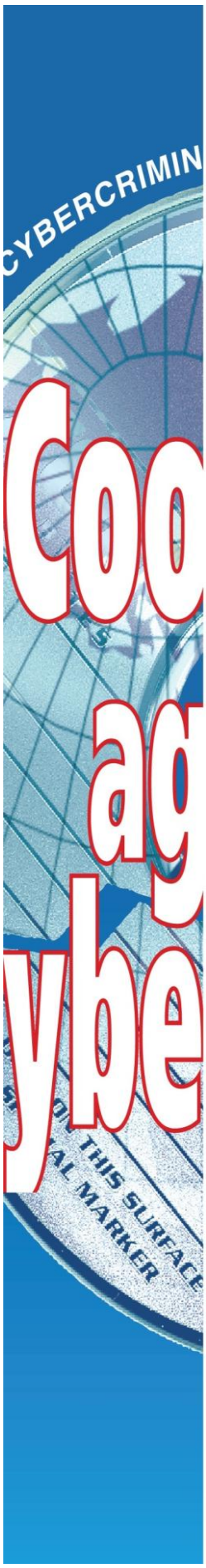


Global Project on Cybercrime

Cooperation against Cybercrime in 2012

Activities of the Council of Europe

Document prepared for information of the Cybercrime Convention Committee (T-CY)

Data Protection and
Cybercrime Division

Strasbourg, 7 December 2012
(provisional)

www.coe.int/cybercrime

COUNCIL OF EUROPE CONSEIL DE L'EUROPE

Contents

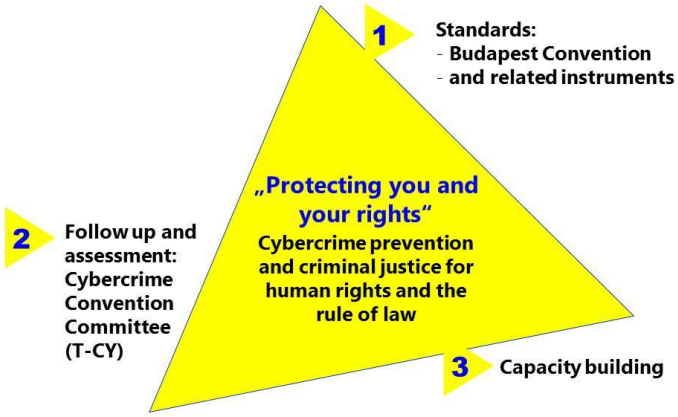
CONTACT

Data Protection and Cybercrime Division
Directorate General of Human Rights and Rule of Law
Council of Europe, F-67075 Strasbourg Cedex (France)

Tel +33 3 8841 2103
Fax +33 3 8841 3955
Email cristina.schulman@coe.int

1 Introduction

The approach of the Council of Europe on cybercrime consists of the three interrelated elements of the setting of common standards, follow up and assessment of implementation, and technical cooperation for capacity building:



This approach was confirmed at the 6th Plenary of the Cybercrime Convention Committee (T-CY) which followed the 10th anniversary of the Budapest Convention on 23 November 2011. On that occasion, the T-CY decided to launch the assessment of implementation of the Convention by the Parties. It furthermore established the "T-CY Subgroup on Transborder Access to Data and Jurisdiction" tasked to explore options for additional standard setting work in this specific area.

In January 2012, implementation of Phase 3 of the Global Project on Cybercrime was commenced while the CyberCrime@IPA and CyberCrime@EAP joint projects of the European Union and the Council of Europe continued in South-eastern and Eastern Europe.[1]

In March 2012, the Committee of Ministers of the Council of Europe adopted the "Internet Governance Strategy 2012 – 2015.[2]

Section IV covers "enhancing the rule of law and effective co-operation against cybercrime". The aims include contributing to harmonisation of legislation at the global level and promoting the Budapest Convention as reference standard for international cooperation against cybercrime.

The above approach on cybercrime thus has the political backing of its member States.

The purpose of the present is to provide an overview of activities carried out and of key achievements in 2012.

[1] For summaries of the projects see www.coe.int/cybercrime

[2] https://wcd.coe.int/ViewDoc.jsp?Ref=CM%282011%29175&Language=lanEnglish&Ver=final&BackColorInternet=C3C3C3&BackColorIntranet=EDB021&BackColorLogged=F5D383

2 Activities of the Cybercrime Convention Committee (T-CY)

2.1.1 Summary

Title	Cybercrime Convention Committee (T-CY)
T-CY Members	38 Parties to the Budapest Convention
T-CY Observers	18 Signatories and States invited to accede, 4 member States of the Council of Europe International organisations (African Union, European Union (European Commission, EU Council, Europol, ENISA), Interpol, International Telecommunication Union, Organisation of American States, OECD, OSCE, UN Office on Drugs and Crime)
Budget	Euro 80,000 (2012)
Funding	Budget of the Council of Europe Additional support through Global Project on Cybercrime (Phase 3)

Objectives 2012/13[3]	1. Support the ratification and accession to the Budapest Convention 2. Review the functioning of the accession procedure for non-member States of the Council of Europe 3. Review the effective implementation of the Budapest Convention by the Parties 4. Continue to give consideration to possible future standard-setting work, taking into account all options as regards the exact choice of instrument (amendment of the Convention, additional protocol to the Convention or a "soft law" instrument) 5. Ensure closer coordination between the Parties and ensure representation of the TCY in future discussions on cybercrime in international fora 6. Ensure close cooperation and coordination with the technical cooperation programme on cybercrime of the Council of Europe (including the Global Project on Cybercrime) developed by the Council of Europe 7. Exchange of information on significant legal, policy or technological developments pertaining to cybercrime and the collection of evidence in electronic form 8. Review the financial resourcing of the Committee

[3] http://www.coe.int/t/dghl/standardsetting/t-cy/TCY2012/TCY_2011_04E_Wayforward_V5%20_final.pdf

2.1.2 Activities 2012

Date	Place	Description
30-31 Jan 2012	Strasbourg	T-CY Bureau Meeting
31 Jan – 1 Feb 2012	Strasbourg	Meeting of the T-CY Sub-group on Transborder Access to data and jurisdiction (Transborder Group)
Feb – May 2012	Strasbourg	Assessment: circulation of questionnaire and preparation of draft report (T-CY Bureau and Secretariat)
Feb – May 2012	Strasbourg	Transborder Group: preparation of draft report (T-CY Transborder Group and Secretariat)
1 June 2012	Strasbourg	T-CY Bureau Meeting
1 – 3 June 2012	Klingenthal, France	Meeting of the Transborder Group
4-5 June 2012	Strasbourg	7th Plenary of the T-CY
6-8 June 2012	Strasbourg	Octopus Conference
June – Nov 2012	Strasbourg	Assessment: preparation of revised draft report (T-CY Bureau and Secretariat)
June – Nov 2012	Strasbourg	Transborder Group: preparation of draft report (T-CY Transborder Group and Secretariat)
4 Dec 2012	Strasbourg	T-CY Bureau Meeting
5-6 Dec 2012	Strasbourg	8th Plenary of the T-CY
Jan – Dec 2012	Multiple	Participation by T-CY Bureau members in technical cooperation activities of the Council of Europe

3 The technical cooperation programme

3.1 Global Project on Cybercrime (Phase 3)

3.1.1 Project summary

Project title	Global Project on Cybercrime, Phase 3 (DGHL/2571)
Project area	A global project aimed at supporting the implementation of the Budapest Convention on Cybercrime and related standards and practices
Budget	Up to EURO 1 million
Funding	Voluntary contributions from the Governments of Estonia, Japan, Monaco, Romania and the United Kingdom, and from Microsoft as well as the budget of the Council of Europe
Implementation	Data Protection and Cybercrime Division (Directorate General of Human Rights and Rule of Law, Council of Europe)
Duration	24 months (1 January 2012 – 31 December 2013)

Objectives and expected results

Project objective	To promote broad implementation of the Budapest Convention on Cybercrime (CETS 185) and related standards and tools
Output 1	Experience exchange: Good practices related to measures against cybercrime documented and shared
Output 2	Assistance: Countries assisted in the implementation of the Budapest Convention and related standards and good practices
Output 3	Assessment of measures against cybercrime available

3.1.2 Activities 2012

Date	**Place**	**Description**
17 Jan 2012	London, UK	Commonwealth Cybercrime Initiative: Participation in Major Partners Meeting
5-8 Feb 2012	Mexico	Participation in Kaspersky Lab Cyber Conference 2012: IT Security in the Age of Cyber Warfare
6-7 Feb 2012	Washington, USA	Organisation on American States: participation the 7th Meeting of the REMJA Working Group on Cyber-Crime
22 Feb 2012	Brussels, Belgium	Discussion of EU funding opportunities for cybercrime activities
27 Feb 2012	London, United Kingdom	Commonwealth: Cybercrime Conference
5-7 Mar 2012	Gaborone, Botswana	Participation in Commonwealth Telecommunications Organisation: 6th Annual e-Gov Africa Forum 2012 (by Chair of the T-CY)
7-9 Mar 2012	San José, Costa Rica	Organisation of international workshop on cybercrime and cybersecurity policies and legislation (in cooperation

		with OAS/CICTE)
11-16 Mar 2012	San Jose, Costa Rica	Participation in ICANN meeting
13 – 15 Mar 2012	Redmond, USA	Participation in Microsoft Worldwide Public Safety Symposium
26 Mar 2012	Jerusalem, Israel	Round Table on the Budapest Convention
28 Mar 2012	Brussels, Belgium	Participation in the European Union Cybercrime Task Force
23 April 2012	Brussels, Belgium	Contribution to European Commission: Workshop on data preservation
23-27 April 2012	Vienna, Austria	Participation in Twenty-first session of the UN Commission on Crime Prevention and Criminal Justice
25-27 April 2012	Prague, Czech Republic	Contribution to Anti-Phishing Working Group: 6th annual Counter-eCrime Operations Summit (CeCOS VI)
10 May 2012	New Delhi, India	Round Table on the Budapest Convention on Cybercrime
11 May 2012	New Delhi, India	Contribution to 5th ASSOCHAM International Cyber Security Conference
14-15 May 2012	Seoul, Korea	Meetings on the Budapest Convention on Cybercrime
16-18 May 2012	Ulaanbataar, Mongolia	Contribution to workshops on cybercrime legislation
21-24 May 2012	Bucharest, Romania	Contribution to POLCYB Summit Romania (by member of the T-CY Bureau)
24-25 May 2012	Milan, Italy	Contribution to Europäische Rechtsakademie (ERA): Fighting Cybercrime: Between Legislation and Concrete Action
4-5 June 2012	Strasbourg	Contribution to 7th Plenary of the Cybercrime Convention Committee (T-CY)
6-8 June 2012	Strasbourg	Organisation of the Octopus Conference
11 – 16 June 2012	Malta	Contribution to COMNET, Commonwealth Secretariat and Malta's Ministry of Foreign Affairs: Legal Frameworks Programme
14- 15 June 2012	Stockholm, Sweden	Contribution to EuroDIG 2012
19-22 June 2012	Tagaytay City, Philippines	Contribution to UNODC workshop on terrorist use of the Internet (by Chair of the T-CY)
21-22 June 2012	Geneva, Switzerland	Participation in Commonwealth Working Group meeting (by member of the T-CY Bureau)
22-24 Aug 2012	Miami, USA	Contribution to Workshop on Cyber Security and Cyber Crime in the Caribbean (by member of the T-CY Bureau)
5-6 Sep 2012	Ottawa, Canada	Contribution to OAS-CICTE Roundtable on cyber security
18 Sep 2012	London (vis phone)	Participation in Commonwealth Cybercrime Initiative: 2nd Steering Group meeting
18-20 Sep 2012	Dakar, Senegal	Contribution to USDOJ cybercrime workshop ECOWAS
20-21 Sep 2012	Vienna, Austria	OSCE: Annual Police Experts Meeting "Fighting the Threat of Cybercrime"
4-5 Oct 2012	Budapest, Hungary	Budapest Conference on cyberspace
15 Oct 2012	Zurich, Switzerland	Panel „Tatort Internet" at University of Zurich
16-17 Oct 2012	Dubai, UAE	Participation in cybercrime panel at ITU Telecom World

17 Oct 2012	St. Petersburg, Russian Federation	Contribution to Office of the UN High Commissioner for Human Rights: Workshop on cybercrime and human rights
25-26 Oct 2012	Stockholm, Sweden	Contribution to workshop on Cyber-related Financial Crime (by member of the T-CY Bureau)
30-31 Oct 2012	Port au Prince, Haiti	Contribution to National Cybersecurity and Cybercrime Workshop
13 Nov 2012	London, UIK	Participation and contribution to Commonwealth Working Group meeting on cybercrime
25-28 Nov 2012	Tokyo, Kyoto Japan	Meetings with authorities on the role of Japan in the Budapest Convention on Cybercrime
29-30 Nov 2012	Madrid, Spain	Contribution to ERA conference: Child pornography online
4-5 Dec 2012	Bishkek, Kyrgyzstan	Contribution to OSCE Sub-regional workshop on terrorism and crime in cyberspace
3-13 Dec 2012	Dubai	Participation in ITU World Congress on Information Technology
8 Dec 2012	Freiburg, Germany	Participation in Max-Planck Institute Workshop on Cybercrime Legislation
9-10 Dec 2012	Abu Dhabi	Contribution to Virtual Global Taskforce Board of Management meeting to provide an update on the Global Engagement Strategy
11-13 Dec 2012	Abu Dhabi	Contribution to VGT 5th biennial conference: Plenary sessions on legislative engagement
13 Dec 2012	Washington DC, USA	World Bank event on "Cybersecurity and Human Rights"
14-15 Dec 2012	Gaborone, Botswana	Organisation of workshop on Capacity building against cybercrime

3.2 CyberCrime@IPA

3.2.1 Project summary

Project title	Regional Cooperation in Criminal Justice: Strengthening capacities in the fight against cybercrime (Cyber@IPA – DGHL/201/2467)
Project area	Western Balkans: Albania, Bosnia and Herzegovina, Croatia, "the former Yugoslav Republic of Macedonia", Montenegro, Serbia as well as Kosovo[4], and Turkey
Budget	EURO 2,777,778
Funding	European Commission (IPA Regional Programme 2010) and Council of Europe
Project Partners	France (Ministry of Interior), Italy (Postal and Communication Police Service), Romania (Prosecution Service and National Police), Slovenia (Criminal Police), University College Dublin
Implementation	Council of Europe (Data Protection and Cybercrime Division, DG-I)
Duration	24 months (1 November 2010 – 30 April 2013)

[4] All reference to Kosovo, whether to the territory, institutions or population, in this text shall be understood in full compliance with United Nations Security Council Resolution 201244 and without prejudice to the status of Kosovo.

3.2.2 Activities 2012

Date	Place	Description
27 Jan 2012	Belgrade, Serbia	Specific workshop on legislation
Jan – Oct 2012	Strasbourg	Prepare a guiding paper on electronic evidence with involvement of experts from EU MS, Asia and Latin America in cooperation with the global Project on Cybercrime (draft to be discussed in the Octopus Conference 2012)
Jan –Dec 2012	All countries/areas	Support the conclusion of memoranda of understanding between law enforcement and (associations of) ISPs in each project area
Jan-Dec 2012	All countries/areas	Support the integration of basic and advanced courses into initial and in-service training curricula
Jan 2012 - March 2013	Zagreb, Croatia	Support the establishment of a Pilot Centre in Croatia
Jan-Dec 2012	all countries/areas	Support the implementation of the LEA Training Strategy
Jan-Dec 2012	Strasbourg	Preparation of a training manual on international police and judicial cooperation against cybercrime
14-15 Feb 2012	Paris, France	Expert Meeting on Electronic Evidence Guide
20-24 Feb 2012	Zagreb, Croatia	Train the trainers regional course, basic module (Judiciary and Prosecution)
27-29 Feb 2012	Kyiv, Ukraine	Joint event with CyberCrime@EAP: Regional training course for cybercrime investigators, financial investigators, intelligence units on criminal money flows on the internet
26 March 2012	Bosnia and Herzegovina	Specific workshop on legislation
28-29 March 2012	Skopje, The Former Yugoslav Republic of Macedonia"	Regional workshop to provide advice to prosecution services and ministries of justice regarding the handling of international cooperation requests
30 March 2012		3rd Steering Committee Meeting
April-May 2012	All project areas	Basic Training Course for judges and prosecutors Albania (16-18 April, 2012); BIH (9-11 May, 2012); Croatia (11-13 April, 2012); Kosovo* (19-21 April, 2012); Montenegro (23-25 April, 2012); Serbia (17-19 May, 2012); Turkey (2-4 May, 2012); "The FYR Macedonia" (26-28 April, 2012)
April – Dec 2012	Strasbourg	Develop training modules for advanced training (module 2) courses and make them available in local languages
9 May 2012	Sarajevo, Bosnia and Herzegovina	Meeting with the TEAM for tracking of implementation of criminal legislation - support of amendments to legislation
15-16 May 2012	The Hague	Participation in the ECTEG Meeting
29-31 May 2012	Germany	Expert Meeting on Electronic Evidence Guide
May-June 2012	Strasbourg	Recommendations and legal advice provided to draft legislative amendments in Bosnia and Herzegovina
4-8 June 2012	Strasbourg	Participation in the Octopus Conference and the Committee of the Convention (T-CY) International workshop on trans-border access to data

		International workshop on public-private information exchange Side event on electronic evidence
June 2012	Dublin, Ireland	MSc programme: Residential workshops at UCD
11-12 July 2012	Croatia	Regional workshop to finalise the basic judicial training pack
July-Aug 2012		Review of the new Criminal Procedure Code of "the former Yugoslav Republic of Macedonia" from the perspective of its compliance with the Cybercrime Convention
July-Sep 2012	Strasbourg	Review of the new Criminal Procedure Code of Serbia and recommendations provided for further reform of cybercrime legislation.
Aug 2012	Strasbourg	Recommendations and legal advice provided for improvement of the cybercrime legislation in Montenegro
Aug-Sep 2012	Strasbourg	Translation of the Explanatory Report of the Budapest Convention on Cybercrime into Albanian language
4-5 Sep 2012	Struga, "The Former Yugoslav Republic of Macedonia"	Workshop on electronic evidence (legal and practical aspects) for institutions of the criminal justice chain (investigators, forensic experts, prosecutors, judges) (in cooperation with CyberCrime@EAP)
6 Sep 2012	Struga, "The Former Yugoslav Republic of Macedonia"	4th Steering Committee Meeting
Sep 2012-Jan 13	Strasbourg	Drafting of an agreement on regional priorities regarding cybercrime taking into account European policies based on the results of assessment visits (September - October 2012) and adopted reports (October 2012)
20-21 Sep 2012	Vienna, Austria	Participation in OSCE Annual Police Experts Meeting
Oct/Nov 2012	All countries/areas	Carry out a cycle of regional assessments
Oct/Nov 2012	Kosovo*; "The Former Yugoslav Republic of Macedonia", Croatia, Turkey	Advanced Training Courses for judges and prosecutors Kosovo* (1-2 October, 2012); "The Former Yugoslav Republic of Macedonia" (4-5 October, 2012); Croatia (29-30 October, 2012) Turkey (1-2 November, 2012)
21-24 Oct 2012	Sofia, Bulgaria	Second South European Regional Forum on Cybersecurity and Cybercrime
5 Nov 2012	Baku, Azerbaijan	Workshop on safeguards and conditions (in cooperation with Cybercrime@EAP)
6-9 Nov 2012	Baku, Azerbaijan	Participation in the Internet Governance Forum
26-28 Nov 2012	Istanbul, Turkey	Regional workshop to support the establishment of trusted fora for regular information exchange between financial investigators, FIU and the private sector (including financial sector) (in cooperation with CyberCrime@EAP) Regional meeting for the training of LEA and ISP staff responsible for cooperation and for developing standard procedures for cooperation

3.3 CyberCrime@EAP

3.3.1 Project summary

Project title	Eastern Partnership – Cooperation against Cybercrime (Cyber@EAP – DGHL/2523)
Project area	Armenia, Azerbaijan, Belarus, Georgia, the Republic of Moldova, Ukraine
Budget	EURO 725,000
Funding	European Union (Council of Europe Facility)
Implementation	Council of Europe (Data Protection and Cybercrime Division, DG-I)
Duration	1 March 2011 – 31 August 2013 (30 months)

3.3.2 Activities 2012

Date	**Place**	**Description**
27-29 Feb 2012	Kyiv, Ukraine	Regional seminar on financial investigations
20-21 March 2012	Tbilisi, Georgia	Regional seminar on specialised cybercrime units
25-27 April 2012	Yerevan, Armenia	Roundtable Discussion on Cybercrime Legislation in Armenia Roundtable discussion on law enforcement – ISP cooperation Regional seminar on law enforcement – ISP cooperation
4-8 June 2012	Strasbourg, France	Participation in the Annual Octopus Conference and the Cybercrime Convention Committee (T-CY) Plenary meeting (one/two representative/s from each country) International workshop on transborder access to data International workshop on public-private information sharing Side event on electronic evidence
25- 29 June 2012	Tbilisi, Georgia	Regional conference on strategic priorities regarding cybercrime Regional seminar on judicial and law enforcement training 2nd Project Steering Committee meeting
4-5 Sep 2012	Struga, "The Former Yugoslav Republic of Macedonia"	Workshop on electronic evidence (legal and practical aspects) for institutions of the criminal justice chain (investigators, forensic experts, prosecutors, judges)
5 Nov 2012	Baku, Azerbaijan	Regional workshop on Article 15 of the Budapest Convention
6-9 Nov 2012	Baku, Azerbaijan	Participation in the Internet Governance Forum
26-28 Nov 2012	Istanbul, Turkey	Regional workshop to support the establishment of trusted fora for regular information exchange between financial

		investigators, FIU and the private sector (including financial sector) (in cooperation with CyberCrime@EAP) Regional meeting for the training of LEA and ISP staff responsible for cooperation and for developing standard procedures for cooperation
5-6 Dec 2012	Strasbourg	8th T-CY Plenary Session
7 Dec 2012	Strasbourg	Roundtable discussion on Article 15 of the Budapest Convention in the EAP Region

4 Key achievements in 2012

Standards

In 2012, five new States ratified the Budapest Convention (Malta, Georgia, Austria, Japan and Belgium) and Australia acceded to it. This will bring the number of Parties to 38. A number of other States are close to ratifying or acceding. Panama was invited to accede, and requests for accession from other States have been received by the Council of Europe and are now being processed.

The Convention on Cybercrime is supported by a range of other organisations and initiatives. Following the London Conference on Cyberspace (2011) it received strong backing again at the Budapest Conference on Cyberspace in October 2012.

In the absence of a consensus on the development of new international agreements on cybercrime, the pace of rolling out the Budapest Convention is accelerating.

Cybercrime and electronic evidence are increasingly understood as transversal challenges. The value of the Budapest Convention is that it not only serves as a stand-alone agreement, but may also complement other treaties. The "Typology Study on Criminal Money Flows on the Internet"[5] adopted in March 2012 and prepared jointly by the Global Project on Cybercrime and the MONEYVAL anti-money laundering evaluation mechanism of the Council of Europe, shows how the Budapest Convention and the Convention on Laundering, Search, Seizure and Confiscation of the Proceeds from Crime and on the Financing of Terrorism (CETS 198) are linked.

The same applies to the discussion paper on "Protecting children against sexual violence: the criminal law benchmarks of the Budapest and Lanzarote Conventions" that was produced by the Global Project on Cybercrime in December 2012.

The Budapest Convention is technology neutral and covers electronic evidence in relation to any crime. This framework allows addressing newly emerging challenges. T-CY Guidance Notes on specific aspects of cybercrime and representing the views of the Parties to the Budapest Convention are likely to become very valuable.

The Budapest Convention in 2003 was complemented by the "Additional Protocol to the Convention on Cybercrime, concerning the criminalisation of acts of a racist and xenophobic nature committed through computer systems (CETS 189)". The proposal of the T-CY Transborder Group, adopted by the T-CY in December 2012, to consider the negotiation of another Additional Protocol is an important signal that the Budapest Convention may be complemented when needed.

[5] http://www.coe.int/t/DGHL/cooperation/economiccrime/cybercrime/Documents/Reports-Presentations/MONEYVAL_2012_6_Reptyp_flows_en.pdf

By taking on the question of transborder access and jurisdiction in the context of cloud computing the Parties to the Convention demonstrate that they are prepared to find solutions to complex issue.

Assessments

Assessing implementation of the Budapest Convention by the Parties will enhance the quality and thus the effectiveness of the treaty. With the "expedited preservation" Articles 16, 17, 29 and 30 of the Budapest Convention, the T-CY had selected four rather difficult provisions for its first round of assessments in 2012. The exercise showed that Parties are prepared to cooperate in this process.

The assessments increase the knowledge-base and will facilitate implementation by new Parties as well as technical assistance.

Assessments were also carried out in 2012 under the CyberCrime@IPA project covering eight project areas in South-eastern Europe. The results of this assessment are to feed into strategic priorities and policies on cybercrime to be adopted by the Governments of this region in spring 2013.

Capacity building

In 2012, under the technical cooperation programme, the Council of Europe organised or contributed to some 100 activities in about 40 countries of Africa, the Americas, Asia and Europe.

The Global Project on Cybercrime, and the CyberCrime@IPA and CyberCrime@EAP joint projects of the Council of Europe and the European Union helped facilitate cooperation and experience exchange with a large number of countries and organisations. For example, the Octopus Conference 2012 gathered some 280 cybercrime experts from 80 countries as well as public and private sector stakeholders. These activities confirmed the Budapest Convention as a crucial element of multi-stakeholder cooperation.

Specific assistance was provided on:

- Cybercrime legislation
- High-tech crime and other types of specialised units for cybercrime and computer forensics
- Judicial training
- Law enforcement training
- Public/private cooperation
- International cooperation
- Financial investigations and criminal money flows on the Internet
- Protection of children against online sexual violence

Results were fed back into cybercrime strategies and policies in some countries.

The technical cooperation programme facilitated pragmatic cooperation between the Council of Europe and numerous international organisations. In 2012, the Council of Europe cooperated in particular with the European Union, the Organisation of American States and the Commonwealth.

Practical tools[6] developed under the programme in 2012 include:

- Materials for judicial training
- Electronic evidence guide

[6] Some of these tools are available at www.coe.int/cybercrime (reports).

- Typology study on criminal money flows on the Internet
- Discussion paper on cybercrime strategies
- Discussion paper on "Protecting children against sexual violence: the benchmarks of the Budapest and Lanzarote Conventions"
- Discussion paper on Article 15 – Conditions and safeguards under the Budapest Convention on Cybercrime.

These tools are to facilitate the practical application of the Budapest Convention.

Conclusion

The approach on cybercrime built on the Budapest Convention gained further momentum in 2012. The pace of ratifications and accessions is accelerating, the assessment of implementation will enhance the effectiveness of the treaty, guidance notes on existing provisions and possibly work on a protocol will help address new challenges, technical assistance projects are delivering results and are strengthening the ability of countries to cooperate against cybercrime.