COUNCIL OF EUROPE CONSEIL DE L'EUROPE

Strasbourg, 9 April 2012
Provisional

Global Project on Cybercrime (Phase 2)

1 March 2009 – 31 December 2011

Final project report

Prepared by the
Data Protection and Cybercrime Division
Information Society and Action against Crime Directorate
Directorate General of Human Rights and Rule of Law

Project funded by Estonia, Japan, Monaco, Romania, Microsoft, McAfee, Visa Europe and the Council of Europe

For further information please contact:

Data Protection and Cybercrime Division
Directorate General of Human Rights and Rule of Law
Council of Europe
Strasbourg, France

Tel: +33-3-9021-4506
Fax: +33-3-9021-5650
Email: alexander.seger@coe.int
www.coe.int/cybercrime

Disclaimer:

This technical report does not necessarily reflect official positions of the Council of Europe or of the donors funding this project or of the Parties to agreements referred to.

Contents

1 Introduction

The approach of the Council of Europe against cybercrime consists of three inter-related elements:

- Developing common standards with the Budapest Convention on Cybercrime (CETS 185) as the main instrument
- Follow up and assessment of their implementation, in particular through the Cybercrime Convention Committee (T-CY)
- Capacity building projects to support implementation.

From 2006, the main capacity building project and driver of the Council of Europe's action against cybercrime has been the Global Project on Cybercrime. Phase 1 was implemented from September 2006 to February 2009.

Phase 2 of the Global Project on Cybercrime was carried out between 1 March 2009 and 31 December 2011. The present report documents the activities supported, the results achieved and the progress made towards this objective.

Phase 2 was aimed at achieving the following objective and expected results:

Project objective	To promote global implementation of the Convention on Cybercrime (CETS 185) and its Protocol on Xenophobia and Racism (CETS 189) and related international standards on data protection (CETS 108, CETS 181) and the online sexual abuse of children (CETS 201)
Result 1	Legislation and policies: Cybercrime policies and legislation strengthened in accordance with the Convention on Cybercrime and its Protocol
Result 2	International cooperation: Capacities of 24/7 points of contact, high-tech crime units and of authorities for mutual legal assistance strengthened
Result 3	Investigation: Law enforcement – service provider cooperation in the investigation of cybercrime improved on the basis of the guidelines adopted in April 2008
Result 4	Financial investigations: enhanced knowledge among high tech crime units and FIUs to follow money flows on the internet and stronger cooperation between financial intelligence and investigation units, high-tech crime units and the private sector
Result 5	Judges and prosecutors: Training for judges and prosecutors in cybercrime and electronic evidence institutionalised
Result 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
Result 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

Phase 2 was made possible by generous contributions by the governments of Estonia, Japan, Monaco and Romania as well as by Microsoft, McAfee and Visa Europe. These contributions complemented funding from the regular budget of the Council of Europe.

2 Activities

Between March 2009 and December 2011, the project organised or contributed to some 130 activities.

Date	Place	Description	Result
9 March 2009	Strasbourg	Indonesia – Legislative review workshop	1
9 March 2009	Strasbourg	Project planning meeting	All
10-11 March 2009	Strasbourg	Octopus Interface Conference	1, 2, 4, 5, 7
12-13 March 2009	Strasbourg	Contribution to Cybercrime Convention Committee (T-CY)	All
20 March 2009	Lisbon, Portugal	Training workshop for judges and prosecutors	5
26 March 2009	New Delhi, India	Workshop on international cooperation and law enforcement/service provider cooperation	2, 3
March 2009	Strasbourg	Legislative advice to "The former Yugoslav Republic of Macedonia"	1
7 April 2009	Bosnia and Herzegovina	Workshop on cybercrime legislation (in cooperation with PROSECO project)	1
15 April 2009	Singapore	Child protection online OECD – APEC symposium	7
16-17 April 2009	Albania	Workshop for judges, prosecutors and law enforcement (in cooperation with PROSECO project)	5
27-28 April 2009	Tallinn Estonia	Presentation at EU Ministerial Conference on Critical Information Infrastructure Protection	2
29 April 2009	Ukraine	Workshop on law enforcement – ISP cooperation	3
April 2009	Strasbourg	Provide legislative advice on the new amendments to the Criminal Code and updated the country profile in "The Former Yugoslav Republic of Macedonia"	1
5 May 2009	Brussels	Public Presentation on "Protecting children using the internet" organised by the European Economic and Social Committee (EESC)	7
7 May 2009	Brussels (via teleconference)	2Centre Cybercrime Centres of Excellence Network WG Open Meeting	5
14-15 May 2009	Trier, Germany	Contribution to workshop on effective responses to cybercrime (Academy of European Law)	1
15 May 2009	Strasbourg	Legislative advice for Montenegro	1
16 May 2009	Tunis, Tunisia	Contribution to Information Society (WTISD 2009), Arab ICT Organization (AICTO) and ITU event on "Protection of children in cyberspace "	1
19 May 2009	Strasbourg	Comments on the Computer Misuse Bill of Uganda	1
19 May 2009	Strasbourg	Analysis of the legislation on cybercrime of Senegal	1
2 June 2009	Strasbourg	Comments on the amendments on cybercrime legislation in "the former Yugoslav Republic of Macedonia"	1
8-10 June 2009	Amsterdam, Netherlands	MAAWG (Messaging Anti-abuse Working Group) conference	3
30 June 2009	Berlin, Germany	International Conference "Protection of Girls and Boys against Sexual Violence in the New Media"	7
6 July 2009	Lisbon, Portugal	Working group meeting on institutionalising training on cybercrime for judges and prosecutors	5
13 July 2009	Brussels, Belgium	Meeting with the European Commission on the Instrument of Stability	1, 2
14 -15 July	Rabat, Morocco	Workshop on cybercrime legislation	1

Date	Place	Description	Result
2009			
29-30 July	Abuja, Nigeria	1st NIGERIA Workshop on the Cybercrime Convention	1, 2
3-4 September 2009	Strasbourg	Workshop on the judicial training concept	5
8-9 September 2009	Lyon, France	Meeting at Interpol	4
14-15 September 2009	Geneva, Switzerland	European Dialogue on Internet Governance	2,3
16 September 2009	Luxembourg	EC: Second meeting of Internet Focus Group "Fighting against online child abuse images"	7
21 September 2009	Strasbourg	Project Planning Group meeting (via conference call)	All
5-9 October 2009	Geneva, Switzerland	ITU Telecom World 2009. Contribution to a workshop on the cost of cybersecurity	1,2
6-7 October 2009	Vienna, Austria	UNODC: Expert Group Meeting on Cybercrime	1,2
8-9 October 2009	Bucharest, Romania	ERA - TAIEX seminar on Fight against cybercrime	1,2
12-14 October	Paris, France	OECD Working Party on Information Security and Privacy (WPISP)	7
14 October 2009	Paris, France	OECD: cloud computing workshop	1,6
13-15 October 2009	Asunción, Paraguay	Contribution to US DOJ workshop on cybercrime legislation for countries of Latin America	1
16 October 2009	Buenos Aires, Argentina	Bilateral meetings to promote accession by Argentina to the Convention on Cybercrime	1, 2
1-3 November 2009	Vancouver, Canada	Information Security Forum 20th Anniversary Annual World Congress	1,2
5-6 November 2009	Brussels, Belgium	EC: Annual cybercrime conference: EU-US cooperation	2
15-18 November 2009	Sharm el Sheikh, Egypt	The fourth annual IGF Meeting	All
18-19 November 2009	Hanoi, Vietnam	Séminaire francophone Droit des technologies de l'Information	1,2
27 November 2009	Brussels, Belgium	EC: Conference on Public-Private Sector dialogue on tackling online illegal activities	7
6-10 December 2009	Cairo, Egypt	Training workshops for judges on cybercrime and child abuse and Round table discussion on a concept for the training of judges in cybercrime/electronic evidence, including online child abuse	5
11-13 December 2009	Courmayeur Mont Blanc, Italy	International Conference on Protecting Children from Sexual Offenders in the Information Technology Era	7
September/ December 2009	Strasbourg	Study on the criminalisation of child pornography and related measures	7
12 January 2010	Ankara, Turkey	Ankara Bar Association International Law Congress 2010 – Cyber Crimes Convention Workshop	1
21-22 January 2010	Ifraine, Morocco	Building Cyber security and Cyber confidence: Strategies, Awareness and Capacity Building	1,2
21-22 January 2010	Washington D.C	Sixth Meeting of the REMJA Working Group on Cyber-Crime	1,2
26-28 January 2010	Manila, Philippines	ASEAN/APRIS workshop on cybercrime legislation and capacity building	1
25–26 January 2010	Ebene, Mauritius	The African Network Information Center (AfriNIC), the Regional Internet Registry (RIR) for Africa: First AfriNIC – Government Working Group (AfGWG) &	1

Date	Place	Description	Result
		Law Enforcement Meeting	
2-3 February 2010	Abuja, Nigeria	1st West African Internet Fraud Summit	1
10 February 2010	Buenos Aires	Meeting on Convention on Cybercrime	1
16-18 February 2010	Malta	MENA Cybercrime Legislation Workshop	1
17-18 Feb 2010	Brussels, Belgium	EastWest Institute – the 7th Worldwide Security Conference	4
23-24 February 2010	Islamabad, Pakistan	Cybercrime training for law enforcement and judges	5
16-17 March 2010	Barcelona, Spain	SecureCloud 2010 – ENISA joint Conference on Cloud Computing	1,6
23- 25 March 2010	Strasbourg	Octopus Interface conference	All
26 March 2010	Strasbourg	Working meeting on the typology study on criminal money on the Internet	4
31 March – 1 April 10	Lille, France	French National Gendarmerie: International Forum on Cybercrime	3
12-19 Apr 2010	Salvador, Brazil	The 12th United Nations Congress on Crime Prevention and Criminal Justice	All
29-30 April 2010	Madrid, Spain	EuroDIG 2010	2
6 May 2010	Brussels, Belgium	Brainstorming session on the EU Internal Security Strategy	1
17 – 21 May 2010	Vienna, Austria	Session of the United Nations Commission on Crime Prevention and Criminal Justice	1
18 May 2010	Como, Italy	International Automobile Federation (FIA): Legal and Consumer Commission's workshop held on May 18th in Como	1
9-11 June 2010	Izmir, Turkey	International Informatics Law Assembly	1
7- 12 June 2010	Malta	Legal Frameworks for ICTs	1
16-18 June 2010	Strasbourg	Meeting of ICT ministers from Pacific Islands (written submission)	1
22 June 2010	Rome, Italy	UNICRI Symposium on the state of Online Trust in Europe	1
23 June 2010	Geneva, Switzerland	The Cyber Security Course: Meeting the Cybersecurity Challenge	1
24-25 June	Paris, France	Cybercrime Convention Committee (T-CY) plenary meeting	All
1 July 2010	Brussels, Belgium	Participation in the EU cybercrime experts group on statistics	1
2 July 2010	Paris, France	Contribution to the training course for judges at the Ecole National de la Magistrature	5
12 - 13 July 2010	Phnom Penh, Cambodia	Workshops on cybercrime legislation	1
27-29 July 2010	Rabat, Morocco	UNECA Atelier de formation sur l'harmonisation du cadre légal pour la cybersécurité en Afrique du Nord	1
25-27 August 2010	Mexico City, Mexico	Regional workshop on cybercrime (for 7 countries of Latin America)	1, 2
7-8 September 2010	Baku, Azerbaijan	National Expert Workshop on a Comprehensive Approach to Cyber Security	1
8-9 September 2010	London, UK	SANS European Digital Forensics and Incident Response Summit	2
12-15 September	Bucharest,	International Forum of Prosecutors	2

Date	Place	Description	Result
2010	Romania		
14-17 Sep 2010	Vilnius, Lithuania	Internet Governance Forum	All
20 September 2010	Yogyakarta City, Indonesia	International Seminar on cybercrime	1
4-5 October 2010 2010	Moscow, Russian Federation	Meeting of the working group on criminal money flows (in cooperation with MONEYVAL and the MOLI-Russia project)	4
11-16 October 2010	Montreal, Canada	Digital Crime Consortium	All
13-15 October 2010	Sibiu, Romania	International Conference on Cybercrime	1,4
14 – 15 October 2010	Buenos Aires, Argentina	National Conference on Cybercrime	1, 2, 3
18-19 October 2010	Santiago de Chile	Bilateral meetings to promote accession to the Convention on Cybercrime	1, 2
25-29 October 2010	Kuala Lumpur, Malaysia	ASEAN: Cybercrime Training Workshop for Judges and Prosecutors organised by the Judicial and Legal Training Institute (ILKAP)	5
25-27 October 2010	Kuala Lumpur, Malaysia	Regional seminar on money laundering, trafficking and cybercrime (organised by France)	4
2-4 November 2010	Moscow, Russian Federation	Meeting of the working group on criminal money flows (in cooperation with MONEYVAL and the MOLI-Russia project)	4
9-10 November 2010	Moscow, Russian Federation	Contribution to the MONEYVAL/Euro-Asia Group meeting on money laundering typologies	4
30 November - 2 December 2010	Abuja, Nigeria	1st West Africa Cybercrime Summit	1
30 November 2010	Brussels, Belgium	Workshop on the impact of cloud computing	1
7-8 December 2010	Kiev, Ukraine	Regional workshop: Protecting children against sexual exploitation and sexual abuse	1
13-16 December 2010	UAE (Abu Dhabi and Dubai), Bahrain and Qatar	Workshops on cybercrime in the Gulf Region	1
20 December 2010	Beirut, Lebanon	Cyber Security Conference in Lebanon	1
17-21 January 2011	Vienna, Austria	Open-ended intergovernmental expert group	All
25 January 2011	Brussels, Belgium	European Commission: Expert group on cybercrime meeting	1
28-29 January 2011	Milano, Italy	OLAF Symposium 2011	4
16-18 February 2011	The Hague, Netherlands	11th IAP European Regional Conference	5
21- 24 February 2011	Kuala Lumpur Malaysia	Participation in POLCYB Summit on Cyber Security	1
February 2011	Strasbourg	Philippines - Legislative advice on the "Cybercrime Prevention Act of 2010"	1
February 2011	Strasbourg	Azerbaijan - Provide legislative advice on Draft Law on the amendment and completion to the Criminal Code of the Republic of Azerbaijan	1
10-11 March 2011	Paris, France	T-CY Bureau meeting	All
17-18 March 2011	Lisbon, Portugal	ERA-CSJ seminar on child pornography	7

Date	Place	Description	Result
1 April 2011	New Delhi, India	4th ASSOCHAM International Conference on Cyber and Network Security	1
5-6 April 2011	Colombo, Sri Lanka	Regional workshop on cybercrime	1
11-15 April 2011	Vienna, Austria,	Twentieth session of the Commission on Crime Prevention and Criminal Justice	7
12-13 April 2011	Budapest, Hungary	EU Presidency conference: The 10th anniversary of the Budapest Convention	All
27-29 April 2011	Tonga, Pacific Islands	Pacific Islands – Workshop on cybercrime legislation	1
9-10 May 2011	Vienna, Austria	OSCE Conference on a Comprehensive Approach to Cyber Security: Exploring the Future OSCE Role	1,2
19 May 2011	London, UK	Meeting on Commonwealth Cybercrime Initiative	1
30-31 May 2011	Belgrade, Serbia	EuroDIG	All
30 May – 4 June 2011	Malta	COMNET Foundation for ICT Development: Workshop on Legal Frameworks for ICT	1
6 June 2011	Santiago, Chile	University of Chile School of Law, Public Ministry, Microsoft: Workshop on cybercrime	1
28 June 2011	Paris, France	Colloque Cybercriminalité	5
28/29 June 2011	Brussels, Belgium	EU/US working group	2
1 July 2011	Paris, France	Judicial training course at the Ecole nationale de magistrature (ENM)	5
4 – 8 July 2011	Kuala Lumpur, Malaysia	Judicial training workshop	5
22-25 Aug 2011	Apia, Samoa	ITU: Workshop on Concepts and Techniques for developing Cyber Crime Policy and Legislation	1
8- 9 September 2011	Lyon, France	Virtual Global Task Force, Board of Management meeting	7
20-21 September 2011	Strasbourg	T-CY Bureau Meeting	All
27-30 September 2011	Nairobi, Kenya	The annual IGF Meeting	All
25 October 2011	Iasi, Romania	National Cyber Crime Conference	All
October – December 2011	Pakistan	Legislative advice	1
1-2 November 2011	London, UK	Conference on Cyber Space	1
21-23 November 2011	Strasbourg	The Octopus Interface Conference	All
29-30 November 2011	Los Angeles, USA	POLCYB Conference	All
29-30 November 2011	Cape Town, South Africa	2nd Annual South African Cyber Crime Conference	1
2 - 4 December 2011	Courmayeur Mont Blanc, Italy	ISPAC International Conference on Cybercrime	1

3 Delivery of results

The project was structured around seven expected results:

Result 1	Legislation and policies: Cybercrime policies and legislation strengthened in accordance with the Convention on Cybercrime and its Protocol
Result 2	International cooperation: Capacities of 24/7 points of contact, high-tech crime units and of authorities for mutual legal assistance strengthened
Result 3	Investigation: Law enforcement – service provider cooperation in the investigation of cybercrime improved on the basis of the guidelines adopted in April 2008
Result 4	Financial investigations: enhanced knowledge among high tech crime units and FIUs to follow money flows on the internet and stronger cooperation between financial intelligence and investigation units, high-tech crime units and the private sector
Result 5	Judges and prosecutors: Training for judges and prosecutors in cybercrime and electronic evidence institutionalised
Result 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
Result 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

The following provides an analysis of the level of achievement of each expected result.

3.1 Result 1 – Legislation and policies

Expected Result 1: Legislation and policies: Cybercrime policies and legislation strengthened in accordance with the Convention on Cybercrime and its Protocol

Under this component the project:

- Organised or contributed to some 80 activities covering more than 100 countries in total
- Prepared or updated some 90 country profiles of which about 50 were published at www.coe.int/cybercrime
- Provided advice on the cybercrime legislation of some 40 countries in Africa (Nigeria, Senegal, Uganda), Asia and Pacific (Australia, Cambodia, Cook Islands, Federated States of Micronesia, Fiji, Indonesia, Kiribati, Laos, Malaysia, Marshall Islands, Nauru, Niue, Pakistan, Palau, Papua New Guinea, Philippines, Samoa, Singapore, Solomon Islands, Thailand, Tonga, Tuvalu, Vietnam, Vanuatu), Europe[1] (Albania, Bosnia and Herzegovina, Montenegro, "The former Yugoslav Republic of Macedonia") and Latin America (Argentina, Colombia, Costa Rica, Dominican Republic, Guatemala, Mexico, Paraguay, Peru, Uruguay).

With regard to legislation:

- The project helped sustain the process of harmonised legislative reforms worldwide on the basis of the Budapest Convention
- New laws or amendments to legislation have been completed or are underway in at least 25 of the above countries
- Azerbaijan, Germany, Moldova, Montenegro, Portugal, Serbia, Spain, Switzerland and the United Kingdom ratified the Budapest Convention
- Turkey signed the Budapest Convention
- Argentina, Australia, Chile and Senegal were invited to accede
- Based on reforms underway or completed, many other countries could now seek accession to the Budapest Convention on Cybercrime
- Germany, Finland, Montenegro, Netherlands, Portugal, Romania and Serbia ratified the Protocol on Xenophobia and Racism committed through Computer Systems
- Italy signed the Protocol.

With regard to policies and strategies:

- The project helped confirm the Budapest Convention as the global standard of reference for cybercrime legislation
- The Octopus conferences organised in 2009, 2010 and 2011 – each with some 230-300 participants – help shape global cybercrime policies. Among other things, the 2009 conference[2] contributed to the debate on law enforcement, jurisdiction and data protection in the context of cloud computing. This contributed to the decision of the Cybercrime Convention Committee in November 2011 to launch work on an additional

[1] Note: This covers only activities to October 2010. With the launch of the CyberCrime@IPA Project in November 2010, assistance to South-eastern Europe was subsequently provided under this project and not under the Global Project on Cybercrime. From April 2011, the same applied to Eastern Partnership countries (Armenia, Azerbaijan, Belarus, Georgia, Moldova and Ukraine) through the CyberCrime@EAP Project.

[2] http://www.coe.int/t/dghl/cooperation/economiccrime/cybercrime/cy%20activity%20interface%202009/Interface2009_en.asp

instrument. The 2010 conference[3] underlined the need for a global capacity building effort which was subsequently taken up by the United Nations Congress on Crime Prevention and Criminal Justice (Salvador, Brazil, April 2010) and the United Nations Commission for Crime Prevention and Criminal Justice.[4] More organisations and countries and more development cooperation organisations are now providing technical assistance to strengthen capacities against cybercrime. The 2011 conference was combined with the 10th anniversary of the Budapest Convention and confirmed political support to this treaty.[5] These conferences furthermore helped build bridges between different initiatives and stakeholders and triggered specific action ranging from legislative reviews, to judicial training, law enforcement, criminal money flows, technical and legal measures to protect children against sexual exploitation and abuse, international cooperation and others

- The project helped inform and shape the policy of the Council of Europe. It contributed to the Secretariat position at the United Nations Crime Congress (Brazil 2010)[6] and the Internet Governance Strategy of the Council of Europe 2012-2015 with respect to cybercrime[7]
- The project helped inform the policies and strategies of other organisations, including the European Union, but also the Organisation of American States, the Secretariat of the Pacific Community and others as well as initiatives such as the London Conference on Cyberspace
- Through the Octopus conference, Internet Governance Fora and discussion papers, the project fed into discussions on the concept of cybercrime versus cybersecurity strategies[8]
- The project supported multi-stakeholder approaches and contributed to the meetings of the Internet Governance Forum in Egypt (2009), Lithuania (2010) and Kenya (2011) as well as the European Dialogue on Internet Governance.

Assessment:

- This result was fully achieved. Major impact was made regarding legislative reforms. The global reform process can be considered sustainable. However, political objections to the Budapest Convention and discussions on a new international treaty may slow down or disrupt this process in some countries.

- The number of Parties remained below expectations during the lifetime of the project although it is likely to increase in 2012/13 (see section on achievement of objective).

[3] http://www.coe.int/t/dghl/cooperation/economiccrime/cybercrime/cy-activity-Interface-2010/Presentations/default_en.asp

[4] http://www.coe.int/t/dghl/cooperation/economiccrime/cybercrime/cy_Octopus_Interface_2011/Interface2011_en.asp

[5] http://www.coe.int/t/dghl/cooperation/economiccrime/cybercrime/cy_Octopus_Interface_2011/Interface2011_en.asp

[6] http://www.coe.int/t/DGHL/cooperation/economiccrime/cybercrime/Documents/Reports-Presentations/SG%20Inf%20_2010_4%20-%20UN%20Crime%20congress_ENGLISH.pdf

[7] http://www.coe.int/t/DGHL/cooperation/economiccrime/cybercrime/Documents/Internet%20Governance%20Strategy/Internet%20Governance%20Strategy%202012%20-%202015.pdf

[8] http://www.coe.int/t/DGHL/cooperation/economiccrime/cybercrime/Documents/Reports-Presentations/2079_cy_strats_rep_V23_30march12.pdf

The following activities contributed to the achievement of this result:

9 March 2009	Strasbourg	Indonesia – Legislative review workshop
9 March 2009	Strasbourg	Project planning meeting
10-11 March 2009	Strasbourg	Octopus Interface conference
12-13 March 2009	Strasbourg	Contribution to Cybercrime Convention Committee
March 2009	Strasbourg	Legislative advice to "The former Yugoslav Republic of Macedonia"
April 2009	Strasbourg	Provide legislative advice on the new amendments to the Criminal Code and updated the country profile in "The Former Yugoslav Republic of Macedonia"
7 April 2009	Bosnia and Herzegovina	Workshop on cybercrime legislation (PROSECO)
14-15 May 2009	Trier, Germany	Contribution to workshop on effective responses to cybercrime (Academy of European Law)
15 May 2009	Strasbourg	Legislative advice for Montenegro
16 May 2009	Tunis	Contribution to Information Society (WTISD 2009), Arab ICT Organization (AICTO) and ITU event on "Protection of children in cyberspace "
19 May 2009	Strasbourg	Comments on the Computer Misuse Bill of Uganda
19 May 2009	Strasbourg	Analysis of the legislation on cybercrime of Senegal
2 June 2009	Strasbourg	Providing comments on the amendments to cybercrime legislation in "the former Yugoslav Republic of Macedonia"
13 July 2009	Brussels, Belgium	Meeting with the European Commission on the Instrument of Stability
14 -15 July 2009	Rabat, Morocco	Workshop on cybercrime legislation
29-30 July	Abuja, Nigeria	1st Nigeria Workshop on the Cybercrime Convention
5-9 October 2009	Geneva, Switzerland	ITU Telecom World 2009. Contribution to a workshop on the cost of cybersecurity
6-7 October 2009	Vienna, Austria	UNODC: Expert Group Meeting on Cybercrime
8-9 October 2009	Bucharest, Romania	ERA - TAIEX seminar on Fight against cybercrime
13-15 October 2009	Asunción, Paraguay	Contribution to US DOJ workshop on cybercrime legislation for countries from Latin America
16 October 2009	Buenos Aires, Argentina	Bilateral meetings to promote accession to the Convention on Cybercrime
1-3 November 2009	Vancouver, Canada	Information Security Forum 20th Anniversary Annual World Congress
15-18 November 2009	Sharm el Sheikh, Egypt	The fourth annual IGF Meeting
18-19 November 2009	Hanoi, Vietnam	Séminaire francophone Droit des technologies de l'Information
12 January 2010	Ankara, Turkey	Ankara Bar Association International Law Congress 2010 – Cybercrime Convention Workshop
21-22 January 2010	Ifraine, Morocco	Building Cyber security and Cyber confidence: Strategies, Awareness and Capacity Building
21-22 January 2010	Washington D.C	Sixth Meeting of the REMJA Working Group on Cyber-Crime
26-28 January 2010	Manila, Philippines	ASEAN/APRIS: Workshop on cybercrime legislation
25–26 January 2010	Ebene, Mauritius	The African Network Information Center (AfriNIC), the Regional Internet Registry (RIR) for Africa: First AfriNIC –

		Government Working Group (AfGWG) & Law Enforcement Meeting
2-3 February 2010	Abuja, Nigeria	1st West African Internet Fraud Summit
10 February 2010	Buenos Aires	Meeting on Convention on Cybercrime
16-18 February 2010	Malta	MENA Cybercrime Legislation Workshop
16-17 March 2010	Barcelona, Spain	SecureCloud 2010 – ENISA joint Conference on Cloud Computing
17-18 February 2010	Brussels, Belgium	EastWest Institute – the 7th Worldwide Security Conference
23-25 March 2010	Strasbourg	Octopus Interface Conference
12-19 April 2010	Salvador, Brazil	The 12th United Nations Congress on Crime Prevention and Criminal Justice
6 May 2010	Brussels, Belgium	Brainstorming session on the EU Internal Security Strategy
17 – 21 May 2010	Vienna, Austria	Session of the United Nations Commission on Crime Prevention and Criminal Justice
18 May 2010	Como, Italy	International Automobile Federation (FIA): Legal and Consumer Commission's workshop held on May 18th in Como
9-11 June 2010	Izmir, Turkey	International Informatics Law Assembly
7- 12 June 2010	Malta	Legal Frameworks for ICTs
16-18 June 2010	Strasbourg	Meeting of ICT ministers from Pacific Islands (written submission)
22 June 2010	Rome, Italy	UNICRI Symposium on the state of Online Trust in Europe
23 June 2010	Geneva, Switzerland	The Cyber Security Course: Meeting the Cybersecurity Challenge
1 July 2010	Brussels, Belgium	Participation in the EU cybercrime experts group on statistics
12 - 13 July 2010	Phnom Penh, Cambodia	Workshops on cybercrime legislation
27-29 July 2010	Rabat, Morocco	UNECA Atelier de formation sur l'harmonisation du cadre légal pour la cybersécurité en Afrique du Nord
7-8 September 2010	Baku, Azerbaijan	National Expert Workshop on a Comprehensive Approach to Cyber Security
20 September 2010	Yogyakarta City, Indonesia	International Seminar on cybercrime
13-15 October 2010	Sibiu, Romania	International Conference on Cybercrime
14 – 15 October 2010	Buenos Aires, Argentina	National Conference on Cybercrime
18-19 October 2010	Santiago de Chile	Bilateral meetings to promote accession to the Convention on Cybercrime
30 November - 2 December 2010	Abuja, Nigeria	1st West Africa Cybercrime Summit
30 November 2010	Brussels, Belgium	Workshop on the impact of cloud computing
7-8 December 2010	Kiev, Ukraine	Regional workshop: Protecting children against sexual exploitation and sexual abuse
13-16 December 2010	UAE (Abu Dhabi and Dubai), Bahrain and Qatar	Workshops on cybercrime in the Gulf Region
20 December 2010	Beirut, Lebanon	Cyber Security Conference in Lebanon
17-21 January 2011	Vienna, Austria	Open-ended intergovernmental expert group

21- 24 February 2011	Kuala Lumpur Malaysia	Participation in POLCYB Summit on Cyber Security
February 2011	Strasbourg	Philippines - Legislative advice on the "Cybercrime Prevention Act of 2010"
February 2011	Strasbourg	Azerbaijan - Provide legislative advice on Draft Law on the amendment and completion to the Criminal Code of the Republic of Azerbaijan
1 April 2011	New Delhi, India	4th ASSOCHAM International Conference on Cyber and Network Security
5-6 April 2011	Colombo, Sri Lanka	Regional workshop on cooperation against cybercrime in South Asia
12-13 April 2011	Budapest, Hungary	EU Presidency conference: The 10th anniversary of the Budapest Convention
27-29 April 2011	Tonga, Pacific Islands	Pacific Islands – Workshop on cybercrime legislation
9-10 May 2011	Vienna, Austria	OSCE Conference on a Comprehensive Approach to Cyber Security: Exploring the Future OSCE Role
19 May 2011	London, UK	Meeting on Commonwealth Cybercrime Initiative
30-31 May 2011	Belgrade, Serbia	EuroDIG
30 May – 4 June 2011	Malta	COMNET Foundation for ICT Development: Workshop on Legal Frameworks for ICT
6 June 2011	Santiago, Chile	University of Chile School of Law, Public Ministry, Microsoft: Workshop on cybercrime
22-25 August 2011	Apia, Samoa	ITU: Workshop on Concepts and Techniques for developing Cyber Crime Policy and Legislation
20-21 September 2011	Strasbourg	Cybercrime Convention Committee (T-CY) Bureau Meeting
27-30 September 2011	Nairobi, Kenya	The annual IGF Meeting
October – December 2011	Pakistan	Legislative advice
25 October 2011	Iasi, Romania	National Cyber Crime Conference
21-23 November 2011	Strasbourg	The Octopus Interface Conference
29-30 November 2011	Los Angeles, USA	POLCYB Conference
29-30 November 2011	Cape Town, South Africa	2nd Annual South African Cyber Crime Conference
2 - 4 December 2011	Courmayeur Mont Blanc, Italy	ISPAC International Conference on Cybercrime

3.2 Result 2 - International cooperation

Expected Result 2:
International cooperation: Capacities of 24/7 points of contact, high-tech crime units and of authorities for mutual legal assistance strengthened

Under this component the project:

- organised or contributed to some 25 activities
- prepared or contributed to a series of reports and studies.

These helped strengthen international cooperation against cybercrime:

- By December 2011, all Parties to the Budapest Convention had established 24/7 points of contact, and the Secretariat of the Cybercrime Convention Committee had began to send out an updated directory to contact points and to verify the availability of contact points on a regular basis
- A critical study on problems regarding the functioning of 24/7 points of contact[9], that had been prepared by the Project and that was discussed at the 2009 Octopus conference, proved to be instrumental for the strengthening of existing contact points and provided guidance to authorities establishing new contact points. The issues raised were followed up to by the CyberCrime@IPA and CyberCrime@EAP projects in the course of 2011. Further work in 2012/13 under these projects will be required to enhance the effectiveness of contact points of some of the Parties
- The Budapest Convention as a framework for international cooperation against cybercrime was promoted in a wide range of international fora. A considerable increase in trusted international cooperation (requests sent/received, joint investigations, exchange of information) between Parties to this treaty was noted by the 10th anniversary conference of the Budapest Convention[10]
- It was underlined that with each new Party the Convention will increase in effectiveness. The project helped increase the number of Parties and of requests for accession. However, progress in this respect is not yet satisfactory
- The project promoted international cooperation among non-members to the Budapest Convention such as in the ASEAN region, Latin America, South Asia (Bangladesh, India, Maldives, Pakistan and Sri Lanka), Pacific Island States and others
- The project supported not only intergovernmental cooperation but also public/private and multi-stakeholder cooperation through Octopus conferences, engagement in the EuroDIG, the Internet Governance Forum, and private sector initiatives
- The project helped strengthen cooperation between international organisations
- Studies prepared under the project on Internet jurisdiction, transborder access to data, data protection and cloud computing[11] feed into the work of the Cybercrime Convention

---

9 http://www.coe.int/t/dghl/cooperation/economiccrime/cybercrime/Documents/Points%20of%20Contact/567_24_7report3a%20_2%20april09.pdf

10 See documentation on the 2011 Octopus and 10th anniversary conference at: http://www.coe.int/t/dghl/cooperation/economiccrime/cybercrime/cy_Octopus_Interface_2011/Interface2011_en.asp

11 http://www.coe.int/t/DGHL/cooperation/economiccrime/cybercrime/Documents/Internationalcooperation/2079_Cloud_Computing_power_disposal_31Aug10a.pdf
http://www.coe.int/t/DGHL/cooperation/economiccrime/cybercrime/Documents/Reports-Presentations/2079_reps_IF10_yvespoullet1c.pdf

Committee which, in November 2011, established an ad-hoc group that has been tasked with the preparation of solutions (in the form of a soft-law instrument or protocol to the Budapest Convention) on transborder access to data by law enforcement.

Assessment:

- This result was achieved to a large extent. While cooperation between the Parties to the Budapest Convention improved considerably and while important progress was made regarding the 24/7 points of contact, the effectiveness of some of the contact points needs to be enhanced. Follow up by the T-CY and further assistance through CyberCrime@IPA and CyberCrime@EAP projects and Phase 3 of the Global Project is necessary. The relationship between the network of the G8 High-tech Crime Subgroup and the network established under the Budapest Convention requires further clarification. The effectiveness of mechanisms for mutual legal assistance remains a major challenge.

The following activities contributed to the achievement of this result:

10-11 March 2009	Strasbourg	Octopus Interface Conference
26 March 2009	New Delhi, India	Workshop on international cooperation and law enforcement/service providers cooperation
27-28 April 2009	Tallinn Estonia	Presentation at EU Ministerial Conference on Critical Information Infrastructure Protection
13 July 2009	Brussels, Belgium	Meeting with the European Commission on the Instrument of Stability
14-15 September 2009	Geneva, Switzerland	European Dialogue on Internet Governance
5-9 October 2009	Geneva, Switzerland	ITU Telecom World 2009. Contribution to a workshop on the cost of cybersecurity
6-7 October 2009	Vienna, Austria	UNODC: Expert Group Meeting on Cybercrime
8-9 October 2009	Bucharest, Romania	ERA - TAIEX seminar on the fight against cybercrime
16 October 2009	Buenos Aires, Argentina	Bilateral meetings to promote accession by Argentina to the Convention on Cybercrime
1-3 November 2009	Vancouver, Canada	Information Security Forum 20th Anniversary Annual World Congress
5-6 November 2009	Brussels, Belgium	EC: Annual cybercrime conference EU-US cooperation
15-18 November 2009	Sharm el Sheikh, Egypt	The fourth annual IGF Meeting
21-22 January 2010	Washington D.C	Sixth Meeting of the REMJA Working Group on Cyber-Crime
25-27 August 2010	Mexico City, Mexico	Regional workshop on cybercrime (for 7 countries of Latin America)
8-9 September 2010	London, UK	SANS European Digital Forensics and Incident Response Summit
12-15 September 2010	Bucharest, Romania	International Forum of Prosecutors
14-17 September 2010	Vilnius, Lithuania	Internet Governance Forum
16-18 February 2011	The Hague, NL	11th IAP European Regional Conference
9-10 May 2011	Vienna, Austria	OSCE Conference on a Comprehensive Approach to Cyber Security: Exploring the Future OSCE Role
20-21 September 2011	Strasbourg	Cybercrime Convention Committee (T-CY) Bureau Meeting

http://www.coe.int/t/DGHL/cooperation/economiccrime/cybercrime/Documents/Reports-Presentations/2079_reps_IF10_reps_joeschwerha1a.pdf
http://www.coe.int/t/DGHL/cooperation/economiccrime/cybercrime/Documents/Reports-Presentations/2079repInternetJurisdictionrik1a%20_Mar09.pdf

27-30 September 2011	Nairobi, Kenya	The annual IGF Meeting
25 October 2011	Iasi, Romania	National Cybercrime Conference
1-2 November 2011	London, UK	Conference on Cyber Space
21-23 November 2011	Strasbourg	The Octopus Interface Conference

3.3 Result 3 - Investigation and LEA/ISP cooperation

Expected Result 3: Investigation: Law enforcement/service provider cooperation in the investigation of cybercrime improved on the basis of the guidelines adopted in April 2008

Under this component, the project:

- Organised or contributed to twelve activities
- Mainstreamed the topic of law enforcement/service provider cooperation into different activities and additional technical cooperation projects
- Translated the LEA/ISP cooperation guidelines in multiple languages and supported its implementation in different countries.

The project helped improve the cooperation between law enforcement authorities and service providers, and more generally public/private cooperation against cybercrime:

- The LEA/ISP cooperation guidelines developed during the first phase of the project and adopted at the Octopus Conference in 2008[12] had already been taken up by the European Union's Justice and Home Affairs Council in November 2008.[13] Further action was subsequently taken by the EU to support implementation of the Council Conclusions of November 2008 in the following years
- Although developed under the Global Project and adopted by an Octopus Conference, the guidelines have been referred to in the case law of the European Court of Human Rights[14] which added to their legitimacy
- Through the Global Project on Cybercrime, the guidelines were mainstreamed into other technical cooperation projects
- The guidelines were supported by the Council of Europe/European Union joint project on Cybercrime in Georgia, and served as basis for a Memorandum of Understanding concluded between LEA and ISPs in Georgia in May 2010[15]
- The CyberCrime@IPA and CyberCrime@EAP regional projects in South-eastern and Eastern Europe also contain LEA/ISP cooperation components
- The guidelines were translated under the Global Project and these other projects into 15 different languages
- LEA/ISP cooperation was promoted furthermore in India and other countries of South-Asia, in the ASEAN region and the Pacific region
- The guidelines have served as a starting point for promoting broader public/private and interagency cooperation against cybercrime as underlined at the 2010 Octopus conference.[16] This contributed to enhanced cooperation against criminal money flows on the Internet,[17] to the discussions on the law enforcement recommendations to ICANN,

[12] http://www.coe.int/t/dghl/cooperation/economiccrime/cybercrime/cy_activity_Interface2008/Interface2008_en.asp

[13] http://www.eu2008.fr/webdav/site/PFUE/shared/import/1127_JAI/Conclusions/JHA_Council_conclusions_Cybercrime_EN.pdf

[14] http://www.coe.int/t/dghl/cooperation/economiccrime/cybercrime/Documents/LEA_ISP/1429_ECHR_CASE_OF_K.U._v%20Finland.pdf

[15] http://www.coe.int/t/dghl/cooperation/economiccrime/cybercrime/cy_project_in_georgia/projectcyber_en.asp

[16] http://www.coe.int/t/dghl/cooperation/economiccrime/cybercrime/cy-activity-Interface-2010/2079_IF10_messages_1p%20key%20prov%20_26%20mar%2010_.pdf

[17] See the section on Result 4 below.

and is expected to facilitate agreement on proposals for public/private information sharing.[18]

Assessment:

- The achievement of this result was satisfactory. The need for law enforcement/service provider cooperation is now widely acknowledged. The LEA/ISP guidelines adopted in 2008 provide guidance in many countries on how such cooperation can be organised. Support to the conclusion of specific agreements between law enforcement and service providers would have required more resources than were available.

The following activities contributed to the achievement of this result:

10-11 March 2009	Strasbourg, France	Octopus Interface Conference
26 March 2009	New Delhi, India	Workshop on international cooperation and law enforcement/service providers cooperation
8-10 June 2009	Amsterdam, Netherlands	MAAWG conference
15-18 November 2009	Sharm el Sheikh, Egypt	The fourth annual IGF Meeting
21-22 January 2010	Ifraine, Morocco	Building Cyber security and Cyber confidence: Strategies, Awareness and Capacity Building
26-28 January 2010	Manila, Philippines	ASEAN/APRIS workshop on cybercrime legislation
23-25 March 2010	Strasbourg, France	Octopus Interface Conference
31 March – 1 April 2010	Lille, France	French National Gendarmerie: International Forum on Cybercrime
14 – 15 October 2010	Buenos Aires, Argentina	National Conference on Cybercrime
5-6 April 2011	Colombo, Sri Lanka	Regional workshop on cooperation against cybercrime in South Asia
27-29 April 2011	Tonga, Pacific Islands	Pacific Islands – Workshop on cybercrime legislation
10-11 November 2011	Trier, Germany	LEAs/ISPs cooperation

[18] This topic will be taken up at the 2012 Octopus Conference (www.coe.int/octopus2012).

3.4 Result 4 - Financial investigations

Expected Result 4: Financial investigations: enhanced knowledge among high tech crime units and FIUs to follow money flows on the internet and stronger cooperation between financial intelligence and investigation units, high-tech crime units and the private sector

Under this component, the project:

- Initiated and supported the preparation of a typology research study on criminal money flows on the Internet
- Contributed to the preparation of the typology study
- Organised or contributed to eight specific activities.

These activities helped bring the anti-cybercrime and financial investigations/anti-money laundering worlds together. They helped create awareness of the need for financial investigations and the confiscation of crime proceeds also on the Internet, contributed to interagency and public/private cooperation in this respect and enhanced knowledge among relevant stakeholders. They furthermore helped mainstream the topic of financial investigations and criminal money flows on the Internet into additional technical cooperation projects and the work of MONEYVAL:

- The Octopus workshop on criminal money flows on the Internet (March 2009) prepared the ground for the design (in July/August 2009) of a typology exercise in cooperation with MONEYVAL and the MOLI-RU2 Project on money laundering in the Russian Federation. In September 2009, the MONEYVAL plenary decided to undertake this study. A project team was subsequently created that was led by the Russian Federation with contributions of MONEYVAL members, the Global Project on Cybercrime, MOLI-RU2 as well as the private sector
- The draft of the study was finalised by December 2011. The study was formally adopted by MONEYVAL in March 2012.[19] Among other things, this study is expected to feed into further work of MONEYVAL and the Financial Action Task Force
- The topic was put on the agenda of the joint MONEYVAL/Euro-Asia Group typology meeting in Moscow in October 2010 which thus helped create awareness also in Central Asia and China
- Financial investigation and criminal money flow components were built into the CyberCrime@IPA and CyberCrime@EAP joint projects; and in turn anti-money laundering projects, such as MOLI-Serbia, now also participate in activities related to cybercrime
- Public/private cooperation and information exchange was strengthened[20]
- The newly consolidated 40 Recommendations of the Financial Action Task Force recommend implementation of the Budapest Convention on Cybercrime.[21]

[19] http://www.coe.int/t/DGHL/cooperation/economiccrime/cybercrime/Documents/Reports-Presentations/MONEYVAL(2012)6_Reptyp_flows_en.pdf

[20] Visa Europe also became a project partner in the second half of 2011.

[21] http://www.fatf-gafi.org/dataoecd/49/29/49684543.pdf

Assessment:

- This result was fully achieved. It is an example of the approach pursued under the Global Project on Cybercrime since the launch of Phase 1 in September 2006: an Octopus conference identified the need for measures against criminal money on the Internet. The project engaged in a partnership with MONEYVAL and the MOLI-Russia Project on money laundering to undertake a typology study. At the same time, the findings were mainstreamed into new initiatives (such as the CyberCrime@IPA and CyberCrime@EAP projects)
- It helped that the adoption of the typology study by MONEYVAL coincided with the adoption of the revised FATF recommendations. It can be assumed that the process of financial investigations and interagency cooperation targeting crime proceeds on the Internet will be sustainable.

The following activities contributed to the achievement of this result:

10-11 March 2009	Strasbourg	Octopus Interface conference with a workshop on criminal money flows on the Internet
8-9 September 2009	Lyon, France	Meeting at Interpol on the underground economy
26 March 2010	Strasbourg	Meeting of the working group on criminal money flows (in cooperation with MONEYVAL and the MOLI-Russia project)
4-5 October 2010	Moscow, Russian Federation	Meeting of the working group on criminal money flows (in cooperation with MONEYVAL and the MOLI-Russia project)
25-27 October 2010	Kuala Lumpur, Malaysia	Regional seminar on money laundering, trafficking and cybercrime (organised by France)
2-4 November 2010	Moscow, Russian Federation	Meeting of the working group on criminal money flows (in cooperation with MONEYVAL and the MOLI-Russia project)
9-10 November 2010	Moscow, Russian Federation	Contribution to the MONEYVAL/Euro-Asia Group meeting on money laundering typologies
28-29 January 2011	Milano, Italy	OLAF Symposium 2011

3.5 Result 5 – Training

Expected Result 5: Judges and prosecutors: Training for judges and prosecutors in cybercrime and electronic evidence institutionalised

Under this component, the project:

- Adopted a judicial training concept and supported its implementation
- Supported 14 specific activities on judicial training and disseminated the concept in a range of other meetings.

Through these activities major progress was made towards institutionalising or mainstreaming judicial training, that is, towards making training for judges and prosecutors on cybercrime and electronic evidence components of the curricula of judicial training institutions:

- The need for sustainable and replicable judicial training was identified at the 2009 Octopus Conference.[22] In the months following that conference, a concept for the training of judges and prosecutors on cybercrime and electronic evidence was developed and finalised under the Project on Cybercrime in cooperation with the Lisbon Network of the CoE and a range of judicial training institutions and private sector representatives.[23] The concept was adopted in September 2009 and subsequently endorsed by the Consultative Council of European Judges, the Consultative Council of European Prosecutors as well as the European Commission for the Efficiency of Justice (CEPEJ)
- The concept was translated into eleven languages[24] to permit broad dissemination
- Following a workshop for ASEAN countries (Manila, January 2010) organised with the support of the project, the issue of judicial training was taken up by ASEAN TELSOM (Telecomm Senior Officials Meeting). Malaysia subsequently organised judicial training workshops in 2010 and 2011 with the support of the project
- Components on judicial training were included in the CyberCrime@IPA and CyberCrime@EAP projects through which implementation of the concept is further supported and under which training materials are being developed in countries of South-eastern and Eastern Europe. This experience will be of benefit also for other region
- The project supported law enforcement training and the 2Centre[25] initiative that was first presented at the 2009 Octopus Conference.

22 http://www.coe.int/t/dghl/cooperation/economiccrime/cybercrime/cy%20activity%20interface%202009/2079%20if09_SUMMARY1.pdf

23 http://www.coe.int/t/dghl/cooperation/economiccrime/cybercrime/Documents/Training/2079_train_concept_4_provisional_8oct09.pdf

24 Translations also with the support of the PROSECO, CyberCrime@IPA, CyberCrime@EAP and Cybercrime in Georgia projects.

25 http://www.2centre.eu/

Assessment:

- This result was fully achieved. The fact that judicial training components were included in the CyberCrime@IPA and CyberCrime@EAP project ensures impact that would not have been possible with the limited resources of the Global Project. As in the case of financial investigations the approach typical for this project was also pursued here: The need for judicial training was identified in an Octopus conference. The project engaged in a partnership with the then Lisbon Network. A concept was developed that was broadly disseminated around the world. It was also mainstreamed into additional technical cooperation projects
- Overall, it can be assumed that the process initiated by the project will be sustainable. However, in order to disseminate good practices and accelerate the process in different regions of the world, judicial training components should be incorporated into future projects on cybercrime.

The following activities contributed to the achievement of this result:

10-11 March 2009	Strasbourg	Octopus Interface Conference with workshop on training
20 March 2009	Lisbon, Portugal	Training workshop for judges and prosecutors
16-17 April 2009	Albania	Workshop for judges, prosecutors and law enforcement (PROSECO)
6 July 2009	Lisbon, Portugal	Working group meeting on institutionalising training on cybercrime for judges and prosecutors
3-4 September 2009	Strasbourg	Workshop on the judicial training concept
15-18 November 2009	Sharm el Sheikh, Egypt	The fourth annual IGF Meeting
6-10 December 2009	Cairo, Egypt	Training workshops for judges on cybercrime and child abuse and Round table discussion on a concept for the training of judges in cybercrime/electronic evidence, including online child abuse
26-28 January 2010	Manila, Philippines	ASEAN/APRIS workshop on cybercrime legislation and capacity building
23-24 February 2010	Islamabad, Pakistan	Cybercrime training for law enforcement and judges
23- 25 March 2010	Strasbourg	Octopus Interface Conference with specific workshop on judicial training
2 July 2010	Paris, France	Contribution to the training course for judges at the Ecole National de la Magistrature
25-29 October 2010	Kuala Lumpur, Malaysia	ASEAN Cybercrime Training Workshop for Judges and Prosecutors by the Judicial and Legal Training Institute (ILKAP)
1 July 2011	Paris, France	Judicial training course at the Ecole nationale de magistrature (ENM)
4 – 8 July 2011	Kuala Lumpur, Malaysia	Judicial training workshop

3.6 Result 6 - Data protection and privacy

Expected Result 6:
Data protection and privacy: Data protection and privacy regulations in connection with cybercrime investigations improved in line with Council of Europe and other relevant international standards

Under this component, the project carried out less activities than anticipated but focused its limited resources on an area that is of strategic interest from a data protection and cybercrime perspective, namely, (transborder) law enforcement access to data in the context of cloud computing.

The activities of the project contributed to and will have an impact on "security and privacy in the clouds":

- Through the project, the Council of Europe positioned itself in the international discussion on cloud computing. Participation in events of the OECD, the International Telecommunication Union, the European Dialogue on Internet Governance (EuroDIG) or the Cloud Security Alliance, and the organisation of workshops at Internet Governance Fora[26] and Octopus Conferences[27] contributed to this
- The work of the project, including the preparation of studies, informed the work of the Cybercrime Convention Committee (T-CY), which in November 2011 decided to establish an ad-hoc group to prepare solutions to the question of transborder access to data.[28]

The project contributed to preparing the ground for accession to Data Protection Convention 108[29] by non-member states of the Council of Europe:

- Access to this treaty was promoted in a range of project activities. By December 2011, a number of countries in Africa and Latin America signalled their interest in this respect
- In several countries, counterparts responsible for cybercrime legislation also took responsibility for data protection legislation
- Following the internal reorganisation of the Council of Europe Secretariat, cybercrime and data protection are dealt with within one Division. This reinforced the external message that security and privacy go hand in hand.

[26] http://www.protecciondedatos.org.mx/2009/11/igf-workshop-on-privacy-and-security-implications-of-cloud-computing-in-sharm-el-sheikh/

[27] http://www.coe.int/t/dghl/cooperation/economiccrime/cybercrime/cy-activity-Interface-2010/Presentations/default_en.asp

[28] http://www.coe.int/t/DGHL/cooperation/economiccrime/cybercrime/Documents/Reports-Presentations/2079_reps_IF10_yvespoullet1c.pdf

[29] Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data (ETS 108) http://conventions.coe.int/Treaty/Commun/QueVoulezVous.asp?NT=108&CM=8&DF=02/04/2012&CL=ENG
Protocol 181 covers supervisory authorities and transborder data flows
http://conventions.coe.int/Treaty/Commun/QueVoulezVous.asp?NT=181&CM=8&DF=02/04/2012&CL=ENG

Assessment:

- This objective has been achieved to some extent. Reasons include resource constraints but also the fact that the decision to pro-actively open Convention 108 to non-member States become only effective in the course of the project. Nevertheless, the ground has been prepared for engaging non-member states in data protection activities. The structure of the Council of Europe Secretariat, that now combines cybercrime and data protection within one division, should be conducive.

The following activities contributed to this result:

5-9 October 2009	Geneva, Switzerland	ITU Telecom World 2009 - Workshop on the cost of cybersecurity
14 October 2009	Paris, France	OECD: cloud computing workshop
15-18 November 2009	Sharm el Sheikh, Egypt	The fourth annual IGF Meeting
16-17 March 2010	Barcelona, Spain	SecureCloud 2010 – ENISA joint Conference on Cloud Computing
23-25 March 2010	Strasbourg	Octopus Interface conference
29-30 April 2010	Madrid, Spain	EuroDIG 2010

3.7 Result 7 – Children

Expected Result 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

Under this component, the project:

- organised or contributed to 14 activities
- offered platforms for experience exchange and cooperation among different stakeholders
- promoted implementation of the Budapest Convention in combination with the Convention on the Protection of Children against Sexual Exploitation and Sexual Abuse (Lanzarote Convention CETS 201).

The activities of the project not only enhanced knowledge of the Budapest and Lanzarote Conventions but facilitated practical cooperation and specific measures:

- The project facilitated cooperation with APEC, the European Commission, the OECD, ECPAT, InHope, UNICEF, eNASCO and a range of other organisations and the private sector
- The Council of Europe – through the Global Project – contributed to the OECD report on "The Protection of Children Online"[30]
- The project – in particular through workshops at Octopus Conferences – helped advance discussions on issues such as access blocking to child abuse materials or the obligations of service providers
- The project permitted sharing of information on new technical and other solutions to online child sexual abuse, such as PhotoDNA
- The project launched a comparative study on substantive criminal law provisions related to the sexual exploitation and abuse of children. The study will contribute to the protection of children against sexual exploitation by encouraging countries to become parties and support the implementation of the Convention on Cybercrime and the Convention on the Protection of Children against Sexual Exploitation and Sexual Abuse and it could be used to monitor the legislation on child protection against sexual exploitation including online all over the world as well as a database on legislative approaches of different countries. It will feed into the work of the Committee of the Parties to the Lanzarote Convention
- The project promoted the Lanzarote Convention in different regions of the world. It encouraged the use of this treaty as a guideline for comprehensive approaches to the protection of children. In the medium term, this is expected to lead to accession requests from non-CoE member states
- In 2011, the project cooperated with the Virtual Global Taskforce on combating online child sexual abuse.[31] In November 2011, the Interpol General Assembly adopted a "legislative engagement strategy".[32] The intention is to encourage countries to adopt legislation to protect children against online sexual abuse and to facilitate international law enforcement cooperation against such crimes. The Budapest and Lanzarote Conventions serve as benchmarks. Subsequently, during the Octopus Conference (21-23

[30] http://www.oecd-ilibrary.org/docserver/download/fulltext/5kgcjf71pl28.pdf?expires=1333526351&id=id&accname=guest&checksum=266E4A1C7ED04661B8495F496F409EA0

[31] http://www.virtualglobaltaskforce.com/

[32] http://www.virtualglobaltaskforce.com/2011/strengthening-laws-to-combat-online-child-sexual-exploitation/

November 2011), the VGT and the Council of Europe signed an agreement expressing their intention to cooperate with each other in the implementation of this strategy.

Assessment:

- This result was achieved to a large extent. The direct impact on the drafting of legislation based on the Lanzarote Convention may have been limited, but the Lanzarote and Budapest Conventions are now widely recognised as benchmarks that countries should meet. This will facilitate future legislative support and accession to the Lanzarote Convention. The project allowed the Council of Europe to gain valuable information on the state of legislation in different regions of the world. The experience of the project will feed into the activities of the Committee of the Parties of the Lanzarote Convention. The project exceeded expectations with regard to multi-stakeholder interaction and non-legal measures. Given resource constraints priority was given to promoting the Lanzarote Convention while the activities related to the Convention on Action against Trafficking in Human Beings (CETS 197) were not pursued.

The following activities contributed to the achievement of this result:

10-11 March 2009	Strasbourg	Octopus Interface Conference
15 April 2009	Singapore	Child protection online OECD – APEC symposium
5 May 2009	Brussels	Public Presentation on "Protecting children using the internet" organised by the European Economic and Social Committee (EESC)
30 June 2009	Berlin, Germany	International Conference "Protection of Girls and Boys against Sexual Violence in the New Media"
16 September 2009	Luxembourg	EC: Second meeting of Internet Focus Group "Fighting against online child abuse images"
15-18 November 2009	Sharm el Sheikh, Egypt	The fourth annual IGF Meeting
11-13 December 2009	Courmayeur Mont Blanc, Italy	International Conference on Protecting Children from Sexual Offenders in the Information Technology Era
Since December 2009	Strasbourg	Study on the criminalisation of child pornography and related measures
23-25 March 2010	Strasbourg	Octopus Interface conference
25-27 October 2010	Kuala Lumpur, Malaysia	Regional seminar on money laundering, trafficking and cybercrime (organised by France)
17-18 March 2011	Lisbon, Portugal	ERA-CSJ seminar on child pornography
11-15 April 2011	Vienna, Austria,	Twentieth session of the Commission on Crime Prevention and Criminal Justice
8- 9 September 2011	Lyon, France	Virtual Global Task Force, Board of Management meeting
21-23 November 2011	Strasbourg	Octopus Interface Conference

4 Achievement of objective

Project objective	To promote global implementation of the Convention on Cybercrime (CETS 185) and its Protocol on Xenophobia and Racism (CETS 189) and related international standards on data protection (CETS 108, CETS 181) and the online sexual abuse of children (CETS 201).

4.1 Contribution to the impact of the Budapest Convention

The 10th anniversary of the Budapest Convention on 23 November 2011 was used to take stock of the key achievements and impact of this treaty. While the approach of the Council of Europe includes several elements (standard setting, follow up through the Cybercrime Convention Committee and technical cooperation projects), and while it is primarily the Parties that need to ensure the functioning of the treaty, much of the impact of the Budapest Convention – in particular with respect to outreach beyond the Parties – was ensured through the Global Project on Cybercrime:

Budapest Convention: key achievements and impact	**Contribution by the Global Project on Cybercrime**
The Budapest Convention provided guidance to a process of legislative reform worldwide. Such reforms have been carried out or are underway in at least 120 states. The Budapest Convention has served as a guideline to most of these countries. The Convention thus facilitated a minimum of harmonization of legislation around the world.	The Global Project on Cybercrime (Phase 1 from September 2006 to February 2009 and Phase 2 from March 2009 to December 2011) was the primary tool to support countries worldwide either directly or in cooperation with Parties and other organisations in their reform efforts based on the Budapest Convention.
The treaty had a reach beyond Europe. 55 countries had ratified or signed it or been invited to accede, including 14 non-European countries. The Council of Europe engaged with at least another 55 countries in technical cooperation on the basis of the Budapest Convention.	Cooperation with most of these countries beyond Europe was carried out through the Global Project on Cybercrime.
The Convention served as a catalyst for technical cooperation. Not only the Council of Europe, but also major donors such as the European Union now recognize that measures against cybercrime contribute to the rule of law and help countries make use of the development opportunities of information and communication technologies.	The Global Project on Cybercrime was the basis for the launch of joint projects of the Council of Europe and the European Union (in Georgia, in Eastern European and in South-eastern Europe), for other EU supported projects (e.g. a twinning project in Turkey), for the proposal for a global capacity building effort discussed at the United Nations (UN Crime Congress and Crime Commissions) etc. It also contributed to the decision of the European Union to open up the Instrument for Stability to support measures on cybercrime and cybersecurity worldwide.
In countries that have implemented the Budapest Convention, an increase in criminal justice measures against cybercrime is noted.	This is mostly due to efforts undertaken by public authorities. However, in many countries the Global Project provided guidance and support.

Police-to-police and judicial cooperation increased considerably between many of the parties to the Budapest Convention. All parties now have functioning 24/7 points of contact in line with Article 35.	This is mostly due to efforts undertaken by public authorities. With respect to the 24/7 points of contact, it was primarily the technical cooperation projects (Global Project, CyberCrime@IPA and CyberCrime@EAP that ensured the creation of contact points by the remaining parties.
The Budapest Convention has been one of the Council of Europe's main contributions to multi-stakeholder cooperation for Internet governance. This has been most visible during the Internet Governance Fora since 2006, the European Dialogue on Internet Governance or the Octopus Conferences since 2004. Multi-stakeholder cooperation includes in particular public-private cooperation. The private sector has supported the implementation of the Budapest Convention.	The Global Project on Cybercrime ensured the Council of Europe's contribution to IGF, EuroDIG and other fora, and thus the Budapest Convention is now considered part of a multi-stakeholder approach to Internet governance. The Octopus Conferences have been part of and were funded under the Global Project on Cybercrime. Public/private cooperation was ensured by the Global Project while other bodies focused on inter-governmental cooperation. Practical results included the guidelines on law enforcement/service provider cooperation in the investigation of cybercrime of 2008 or the typology report on criminal money flows adopted by MONEYVAL.
Governments have a positive obligation to protect people through effective laws and law enforcement measures, for example, by implementing the Budapest Convention as noted by the European Court of Human Rights.[33] Article 15 helps strike a fair balance between the need for effective law enforcement and procedural safeguards.	Through the technical cooperation projects (Global Project and CyberCrime@IPA) work was undertaken to "operationalise" article 15 and to create links between cybercrime and data protection activities.[34] The projects helped explain that the Convention is about "protecting you and your rights".[35]

[33] See the case K.U. v. Finland
http://cmiskp.echr.coe.int/tkp197/view.asp?action=html&documentId=843777&portal=hbkm&source=externalbydocnumber&table=F69A27FD8FB86142BF01C1166DEA39864919
Regarding Article 15 see
http://www.coe.int/t/DGHL/cooperation/economiccrime/cybercrime/Documents/Reports-Presentations/2467_SafeguardsRep_v18_29mar12.pdf

[34] Data protection was also on the agenda of the Cybercrime Convention Committee in 2010 (www.coe.int/tcy).

[35] See Octopus conference 2011 – Outlook Panel 1
http://www.coe.int/t/DGHL/cooperation/economiccrime/cybercrime/cy_Octopus_Interface_2011/Presentations/default_en.asp

4.2 Contribution to impact of other instruments and multi-stakeholder cooperation

The Council of Europe is committed to a multi-stakeholder approach to Internet governance.[36]

In a multi-stakeholder model, the strength of an instrument such as the Budapest Convention depends on the links to other partners and to related instruments and tools. For that reason, the Global Project on Cybercrime promoted related instruments such as the Protocol on Xenophobia and Racism committed through computer systems (CETS 189), the Lanzarote Convention on the Protection of Children against Sexual Exploitation and Sexual Abuse (CETS 201) as well as the Data Protection Convention 108 and its Protocol (CETS 181).

Even though fewer resources were available for specific support to the implementation of these treaties, through the Global Project in many countries outside Europe public institutions were familiarised for the first time with the opportunities that these agreements offer.

For the same reason, the Council of Europe – through the Global Project on Cybercrime – cooperated with a with a wide range public and private sector and international organisation either in the co-organisation of activities or by mutual participation in activities. In addition to public authorities from different countries, these included among others:

- ACONITE Internet Solutions
- AFA Association of French Internet Service Providers
- African Network Information Centre
- Anti-Phishing Working Group (APWG)
- ASEAN
- Asia-Pacific Economic Cooperation (APEC)
- Associated Chambers of Commerce and Industry (ASSOCHAM), India
- Basel Institute on Governance
- BITEK International
- CERT LEXSI
- Cloud Security Alliance
- COMNET Foundation
- Centre de Recherche Informatique et Droit (CRID)
- CGI
- Cyberdelincuencia.org
- Cybercrime Research Institute
- CYBEX
- ECO Association of German Internet Industry
- Ecole national de magistrature (ENM), France
- E-Discovery Europe
- ECPAT
- Electronic Frontier Foundation
- eNASCO European NGO Alliance for Child
- Kaspersky Lab
- London Action Plan
- LTU Technologies
- Max-Planck Institute for Foreign and International Criminal Law, Freiburg
- McAfee
- Messaging Anti-abuse Working Group (MAAWG)
- Microsoft
- Missing Children Europe
- Money Express
- Morgan Lewis Law Firm
- NSPCC-National Society for the Prevention of Cruelty to Children
- OECD
- Organisation of American States (OAS)
- OSCE
- PAYPAL
- POLCYB Society for Policing in Cyberspace
- PriceWaterhouseCoopers
- Regional Cooperation Council for Southeast Europe
- RG Data
- RIPE NCC
- Secretariat of the Pacific Community (SPC)
- Signal Spam
- STD Andorra Telecom

[36] https://wcd.coe.int/ViewDoc.jsp?id=1835773 *"The development and implementation of Internet governance arrangements should ensure, in an open, transparent and accountable manner, the full participation of governments, the private sector, civil society, the technical community and users, taking into account their specific roles and responsibilities. The development of international Internet-related public policies and Internet governance arrangements should enable full and equal participation of all stakeholders from all countries"* (Declaration by the Committee of Ministers on Internet governance principles adopted by the Committee of Ministers on 21 September 2011).

Safety Online
- ERA – Academy of European Law
- ENISA
- Euroclear
- EuroISPA
- EUROJUST
- European Dialogue on Internet Governance
- European Union
- Europol
- Financial Action Task Force
- France Telecom
- FOCUD Network
- GOOGLE
- Group-IB Investigations and Forensics, Russia
- Group SANOFI AVENTIS
- ICMEC
- Information Security Forum
- InHope
- International Association of Prosecutors
- International Automobile Federation
- International Multi-lateral Partnership against Cyber Threats (IMPACT)
- International Telecommunication Union
- Internet Governance Forum (IGF)
- Interpol
- Jamil and Jamil, Pakistan
- JP Morgan Chase Bank
- Judicial and Legal Training Institute (ILKAP), Malaysia
- SUN Microsystems
- Symantec
- TAC Together against Cybercrime
- Team Cymru
- Trend Micro
- 2Centre
- UNICEF
- United Nations Commission for Crime Prevention and Criminal Justice
- United Nations Congress on Crime Prevention and Criminal Justice
- United Nations Economic Commission for Africa
- United Nations International Scientific and Professional Advisory Council of the UN Crime Prevention and criminal Justice Programme (ISPAC) and Courmayeur Foundation
- United Nations Office on Drugs and Crime
- University College Dublin
- Universities of Amsterdam, Buenos Aires, Chiba, California University of Pennsylvania, Cologne, Karlstad, Lausanne, Montpellier, Northumbria, Paris II, Oslo, Rio de Janeiro, Verona, Sorbonne, Strasbourg, Teesside, Troyes, Waseda, Zurich
- VIGILO Consult
- Virtual Global Taskforce
- Visa Europe
- WetStone Technologies
- Yahoo!
- ZIUZ Visual Intelligence

The annual Octopus conferences – organised under the Global Project on Cybercrime - proved to be platforms highly conducive to multi-stakeholder cooperation and allowed organisations and individuals to interface.

During Phase 2 of the project, close cooperation was developed with the European Commission and in particular with DG Home. This facilitated coordination of policies of the Council of Europe and the European Union and also resulted in additional capacity building projects on cybercrime.

Microsoft had been the primary private sector partner in Phase 1 (2006 – 2009) and remained the main industry partner also in Phase 2 of the project. A high-level Council of Europe visit to Redmond in February 2009 helped prepare the ground for support during Phase 2. This cooperation was based on a shared interest in enhancing the security of information and communication technologies, and the need for:

- clear legal frameworks in countries worldwide
- public/private cooperation (including between service providers and law enforcement as well as public/private information sharing)
- addressing challenges related to cloud computing and law enforcement access to data
- protecting children against online sexual exploitation and abuse.

Microsoft not only provided co-financing, but also contributed subject-matter expertise in a number of activities. Council of Europe/Microsoft cooperation thus remained a good example of public/private cooperation for others to follow. In the second half of 2011, Visa Europe also became a project partner.

4.3 Progress in terms of signature, ratification, accession of Budapest Convention

The level of signatures, ratifications and accessions to the Budapest Convention is not the only but an important indicator for the impact of the project.

Status of signatures and ratifications of the Convention on Cybercrime (December 2011)

Ratified (32):

- Albania
- Armenia
- Azerbaijan
- Bosnia and Herzegovina
- Bulgaria
- Croatia
- Cyprus
- Denmark
- Estonia
- Finland
- France
- Germany
- Hungary
- Iceland
- Italy
- Latvia
- Lithuania
- Moldova
- Montenegro
- Netherlands
- Norway
- Portugal
- Romania
- Serbia
- Slovakia
- Slovenia
- Spain
- Switzerland
- The „former Yugoslav Republic of Macedonia"
- Ukraine
- United Kingdom
- United States of America

Signed (15):

- Austria
- Belgium
- Canada
- Czech Rep
- Georgia
- Greece
- Ireland
- Japan
- Liechtenstein
- Luxembourg
- Malta
- Poland
- South Africa
- Sweden
- Turkey

Not signed (4 CoE member States):

- Andorra
- Monaco
- Russian Federation
- San Marino

Invited to accede (8):

- Argentina
- Australia
- Chile
- Costa Rica
- Dominican Republic
- Mexico
- Philippines
- Senegal

The project contributed to additional signatures (1), ratifications (9) and invitations to accede (4) to the Budapest Convention and its Protocol (1 signature and 9 ratifications during the project period):

- Azerbaijan, Germany, Moldova, Montenegro, Portugal, Serbia, Spain, Switzerland and the United Kingdom ratified the Budapest Convention
- Turkey signed the Budapest Convention
- Argentina, Australia, Chile and Senegal were invited to accede
- Germany, Finland, Montenegro, Netherlands, Portugal, Romania and Serbia ratified the Protocol on Xenophobia and Racism committed through Computer Systems

- Italy signed the Protocol.

While a number of other countries made progress in the adoption of legislation and their internal ratification or accession procedures which should permit them to become Parties, progress during the lifetime of Phase 2 of the project has not been satisfactory.

Reasons may include:

- Implementation of the Budapest Convention requires changes in domestic criminal law, including procedural law. This takes time and may be subject to political discussions, in particular with regard to law enforcement powers. It is essential for the effectiveness of the treaty that countries have the necessary legal framework in place before becoming Parties
- For some governments or parliaments, the issue of cybercrime appears not to be sufficiently high on the political agenda and awareness of the threats among decision-makers seems to be limited. The lack of political commitment to legislative and other measures against cybercrime is a concern echoed by criminal justice experts in many countries
- Some European Union member states have been waiting for the adoption of the EU Directive on Attacks against Information Systems so as to implement the Budapest Convention in conjunction with this Directive. Adoption is expected by mid-2012, and since it appears to be largely compatible with the Budapest Convention, it should not cause further delays
- Some governments and organisations have been favouring the development of a new, United Nations treaty on cybercrime. This may have discouraged some countries from seeking accession or completing ratification or accession.

Regarding the last point, while there is little dispute on the substance of the Budapest Convention, the main argument brought forward is that non-European countries – with few exceptions – did not participate in the drafting of the treaty. Although the preparation of a meaningful treaty is unlikely to materialise in the coming years, for some countries this problem is that serious that it prevails over the benefits of urgent international cooperation against cybercrime and the practical and legal value of the Budapest Convention. For others, this is not a major obstacle; they consider it in their national interest to cooperate against cybercrime and see that the Budapest Convention offers an existing and functioning framework to that effect. They also recognise that once they are parties they will participate in the operation of the treaty and, as members of the Cybercrime Convention Committee, will participate in its further development, for example, through protocols.

By December 2011, 55 States had either ratified, signed or been invited to accede to the Budapest Convention. It is expected that in the course of 2012 the number of Parties will increase and that additional states will be invited to accede. Once all of these 55 States are Parties, the level of international cooperation against cybercrime will increase considerably.

Member states of the Council of Europe need to set an example and ratify as a soon as possible. Policy dialogue with member States and countries already invited to accede to complete the ratification/accession process must be enhanced.

4.4 Budget, management and implementation

The project was implemented over a period of 34 months and was possible due to contributions from a range of public and private sector partners.

At the outset of the project, the budget of the project was projected at EURO 1.4 million. Actual funding and expenditure amounted to approximately Euro 1 million. More than 55% was covered from the budget of the Council of Europe, some 20% by voluntary contributions from Microsoft and the remaining 25% by contributions from the Governments of Estonia, Japan, Monaco and Romania as well as McAfee and Visa Europe.

Given the large number of activities carried out, the geographic and thematic scope, and the impact of the project on the one hand, and the rather limited resources on the other, Phase 2 of the Global Project on Cybercrime the project can be considered effective and that efficient use has been made of the funds entrusted by donors and the member states of the Council of Europe.

The processes initiated have a high probability of sustainability. This is particularly true for the global process of legislative reform, the results related to financial investigations and money laundering prevention, and judicial training. In all fields, follow up is to be ensured through additional technical cooperation projects.

The approach of identifying issues through Octopus conferences, then seeking partnerships and synergies with public or private sector organisations to address an issue, and finally provide support under the project to ensure the delivery of results has proven to work and has become characteristic for this project.

The strategy of the Council of Europe on cybercrime includes the setting of common standards (Budapest Convention and related instruments), follow up through the Cybercrime Convention Committee (T-CY) and support through technical cooperation projects such as the Global Project on Cybercrime.

The separation of the work of the T-CY and cooperation programmes into two different directorates within the Council of Europe Secretariat had been an impediment, in particular given that both sectors were underfunded.

The internal reorganisation along thematic areas as from October 2011 brought together the T-CY and cooperation programmes. In November 2011, the T-CY adopted a workplan which foresees, among other things, assessments of implementation by the Parties, work on an instrument on transborder access to data and other activities. The workplan furthermore foresees close interaction between the T-CY and cooperation programmes, in particular the Global Project on Cybercrime (Phase 3). This consolidated structure should help further increase the impact of the Budapest Convention.[37]

[37] http://www.coe.int/t/dqhl/standardsetting/t-cy/T-CY_2011_10E_PlenAbrMeetRep_V4%20_28Nov2011.pdf

5 Conclusion

5.1 Summary of findings

The aim of the project was to promote broad implementation of the Convention on Cybercrime (CETS 185) and its Protocol on Xenophobia and Racism committed through computer systems (CETS 189) as well as related international standards, that is, in particular the Lanzarote Convention on the Sexual Exploitation and Sexual Abuse of Children (CETS 201) and the Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data (CETS 108).

The project organised or supported some 130 activities to produce deliverables under each of the seven expected results:

1. Legislation and policies
2. International cooperation
3. Investigation through law enforcement/service provider cooperation
4. Financial investigations
5. Judicial training
6. Data protection and privacy
7. Protection of children against online sexual exploitation and abuse.

By December 2011, 55 countries – including 12 non-European countries – were either Parties, or had signed or been invited to accede to the Budapest Convention. Progress was made in this respect during Phase 2 and political support to this treaty has been growing steadily. The treaty is functioning and makes an impact not only in terms of global harmonisation of legislation, but also in terms of cooperation and criminal justice capacities. The Global Project on Cybercrime made a major contribution to this impact and thus achieved its objective.

However, the level of ratifications and accessions is not yet satisfactory. Member states of the Council of Europe, in particular, need to undertake urgent efforts to become Parties. Other countries need to decide whether or not it is in their interest to engage in effective international cooperation against cybercrime and to join this treaty.

Greater synergies between Cybercrime Convention Committee (T-CY) and technical cooperation projects should facilitate ratification and accession by new states and the level of implementation by the Parties to the Convention.

Activities were designed and implemented to trigger sustainable processes. Under the Global Project and other projects, tools were produced that will continue to support such processes, that help implement and supplement the Budapest Convention and that can feed into additional projects.

The experience of Phase 2 underlines the importance to conceive measures against cybercrime as measures to strengthen human rights and the rule of law ("protecting you and your rights"). This includes implementation of Article 15 (conditions and safeguards) of the Budapest Convention but also the protection of personal data.

The Governments of Estonia, Japan, Monaco and Romania as well as Microsoft, McAfee and Visa Europe were project partners that provided resources and contributed to the success of this project.

The above results were achieved during a period of 34 months with a budget of less than Euro 1 million. The project has been efficient and made effective use of the resources entrusted to it by project partners.

The experience of Phase 2 shows that the strength of a treaty such as the Budapest Convention depends on the strength of its links to other standards, tools, initiatives and stakeholders. The project involved in its activities public authorities of more than 100 countries and more than 90 private sector, academic and international organisations and initiatives. This is a reflection of the multi-stakeholder approach pursued by the project. The Octopus conferences provided a platform where many of these came together once a year.

The Global Project on Cybercrime facilitated the launching of several joint projects of the Council of Europe and the European Union on cybercrime covering Georgia, South-eastern Europe and Eastern Europe. In turn, these projects then helped enhanced the impact of the Global Project. This is an excellent example of synergies and efficient use of resources. This also reinforced cooperation between the Council of Europe and the European Union in cybercrime matters.

5.2 Capacity building against cybercrime: lessons learnt

Ten years of experience in the implementation of the Budapest Convention and six years of experience of technical cooperation under the Global Project on Cybercrime involving that many countries and stakeholders is a tremendous asset.

With regard to technical assistance for capacity building, lessons learnt for the future include:

- A major capacity building effort is still needed to help countries worldwide meet the challenge of cybercrime. The Octopus Conference of March 2010 and the subsequent United Nations Congress on Crime Prevention and Criminal Justice (Brazil, April 2010) reflect broad consensus on this. This consensus should facilitate cooperation between international organisations to provide best possible services to societies in all regions of the world.

- Cybercrime affects core interests and development opportunities of societies. Measures against cybercrime will enhance human rights and the rule of law as well as confidence and trust in information and communication technologies. Official development aid should increasingly be made available for technical assistance against cybercrime.

- A general prerequisite for technical assistance projects is the commitment of governments or counterparts to engage in a process of change. This also applies to projects on cybercrime. Accession to the Budapest Convention is an expression of commitment by a government to cooperate against cybercrime. Accession or an invitation to accede should be a crucial indicator for partners and donors when deciding whether to make scarce resources available for technical assistance against cybercrime.

- Therefore, while any country requesting assistance in the preparation of legislation should be supported, the Council of Europe, when providing assistance beyond legislation, should give priority to countries that are signatories or Parties or that have requested accession to the Budapest Convention.

- The Budapest Convention serves as a guideline and common normative benchmark around which technical assistance can be designed. A wide range of related standards[38] and tools should be made use of when supporting countries.

[38] In particular Data Protection Convention 108 and Lanzarote Convention 201.

- Fields of intervention may range from support to cybercrime policies and strategies, to legislation, reporting systems, specialised units, training, public private cooperation, international cooperation and specific measures to protect children, to confiscate crime proceeds and to prevent terrorist use of information and communication technologies.[39]

- Projects on cybercrime should be designed to protect human rights and the rule of law. The Budapest Convention can help ensure that human rights and rule of law conditions are met when taking measures against cybercrime.
- Multi-stakeholder approaches, including public/private cooperation, can be pursued when implementing projects without rendering them complex and unmanageable, as demonstrated during Phase 2 of the Global Project. Donors are not only donors but should be partners that can offer more than simply funding.

- The European Union gives strong political support to the Budapest Convention on Cybercrime. The experience of joint projects of the Council of Europe and the European Union against cybercrime within Europe[40] has been positive. This experience should now be replicated in joint projects at the global level.

The Global Project on Cybercrime will continue in 2012/13 with a Phase 3.[41] This phase will put a stronger focus on the documentation and sharing of good practices and on the assessment of cybercrime legislation worldwide. It will continue to assist countries in the implementation of the Budapest Convention and related standards and good practices.

The main difference to Phase 1 and 2, however, is that it will be closely linked to and support the Cybercrime Convention Committee (T-CY). The internal reorganisation of the Council of Europe Secretariat in October 2011 and the adoption of the T-CY workplan in November 2011 allow for greater synergies and pooling of resources. Phase 3 will again rely on extra-budgetary resources and support by public and private sector project partners.

Phase 3 will contribute to the implementation of the Internet Governance Strategy of the Council of Europe 2012-2015 with respect to cybercrime.[42]

The Global Project on Cybercrime (Phase 3) will continue to pursue a multi-stakeholder approach and make efficient use of resources to produce impact.

---

[39] See appendix for a list of fields of intervention.

[40] Project on Cybercrime in Georgia, CyberCrime@IPA and CyberCrime@EAP.

[41] http://www.coe.int/t/DGHL/cooperation/economiccrime/cybercrime/cy_project_Phase3_2571/2571_Phase3_summary_V6_Mar2012.pdf

[42] http://www.coe.int/t/DGHL/cooperation/economiccrime/cybercrime/Documents/Internet%20Governance%20Strategy/Internet%20Governance%20Strategy%202012%20-%202015.pdf

6 Appendix

Capacity building

for cybercrime prevention and criminal justice

- Suggestions[43] -

Rationale

Cybercrime violates the rights of millions of people, generates vast amount of illicit proceeds, causes major damage, undermines confidence and trust in information and communication technologies, puts critical information infrastructure at risk, and thus affects the security and other core interests of societies. The issue is therefore high on the agenda of the European Union, the Council of Europe and other organisations as well as of many governments and the private sector.

Societies need to cope with:

- offences against the confidentiality, integrity and availability of computer data and systems
- offences by means of computers, such as fraud, child pornography/child abuse, intellectual property rights violations
- electronic evidence stored on computers in relation to any crime

Cybercrime is fast evolving and transnational in nature, with offenders, ICT infrastructure and victims in multiple jurisdictions. Internal and external dimensions of security are thus connected.

Agreements, tools and good practices to meet the challenge of cybercrime are already available and can be applied by any country. These include in particular the Budapest Convention on Cybercrime (CETS 185), but also other instruments on cybercrime and related matters such as organised crime, the exploitation of children, the terrorist use of the internet, financial investigations, money laundering, the protection of personal data and others. Tools for law enforcement and judicial training, for public/private cooperation and for international cooperation have been developed.

A major capacity building effort to help countries worldwide make use of existing tools, instruments and good practices is the most effective way ahead.

A global approach is required to respond to needs in a pragmatic manner, follow up on expressed commitment by governments, react to incidents, generate or build on momentum in a given country or region, and exploit opportunities to engage in cooperation against cybercrime.

The Octopus conference 2010 and the United Nations Congress on Crime Prevention and Criminal Justice (Salvador, Brazil, April 2010) underlined broad international consensus on the need for technical assistance aimed at strengthening the capacities of States to counter cybercrime.

[43] Based on a presentation made by the Council of Europe at the EU Expert Workshop on cyber security and enhancing law enforcement in third countries: Options for EU External Action, Brussels, 9 December 2011.

Fields of intervention

Experience suggests that capacity building programmes for cybercrime prevention and criminal justice could address the following:

Cybercrime policies and strategies

- Comprehensive and coherent approaches to cybercrime
- Engagement by decision-makers
- Synergies and links with cybersecurity strategies
- Multi-stakeholder participation
- Contributions by donors and cooperation with partners
- Human rights and rule of law requirements
- Management of implementation, monitoring/assessment of results and impact

(See: Discussion paper on cybercrime strategies)

Legislation

- Substantive law measures to criminalise offences against and by means of computers
- Procedural law tools for efficient investigations and use of electronic evidence
- Safeguards and conditions for investigative powers (Article 15 Budapest Convention)
- Data protection regulations (in line with Data Protection Convention 108)
- Harmonisation with the Budapest Convention on Cybercrime

(See: www.coe.int/cybercrime)

Cybercrime reporting

- Reporting channels for individuals and for public and private sector organisations
- Triggering law enforcement investigations
- Intelligence for better understanding of scope, threats and trends
- Collation of data to detect patterns of organised criminality

Prevention

- Public awareness/education of users and society in general
- Technical, administrative, procedural measures to protect systems
- Specific measures for users, groups and sectors at risk

Specialised units

- Police-type cybercrime or high-tech crime units
- Prosecution-type cybercrime units
- Computer forensic capabilities
- Specialisation within judiciary
- Interagency cooperation

(See: CoE/EU/EUCTF (2011): Specialised cybercrime units – good practice study)

Law enforcement training

- Sustainable, standardised, replicable, scalable training
- Skills to investigate cybercrime, secure electronic evidence, carry out computer forensic analyses, assist other agencies and contribute to network security
- Skills/competencies required for respective functions and at appropriate level (from first responder to forensic investigators)
- Make use of materials and models already developed
- Law enforcement, academia, industry cooperation (www.2Centre.eu)

(See: CyberCrime@IPA (2011): Law enforcement training strategy)

Judicial training

- Initial and in-service training for judges and prosecutors by training institutions on cybercrime and electronic evidence
- Advanced training for a critical number of judges and prosecutors
- Specialisation and technical training of judges and prosecutors
- Enhanced knowledge through networking among judges and prosecutors

(See: Council of Europe/Project on Cybercrime (2009): Judicial training concept)

Public/private cooperation

- Cooperation in cybercrime reporting systems (spam, botnets, child abuse materials)
- Information and intelligence sharing (finance and other sectors)
- Law enforcement/service provider cooperation

(See: Council of Europe/Global Project on Cybercrime (2008): Guidelines for LEA/ISP cooperation)

International cooperation

- Chapter III of Budapest Convention on Cybercrime and accession to this treaty
- Police to police cooperation (direct cooperation, use of Interpol and other channels)
- Judicial cooperation
- 24/7 points of contact

(See: Council of Europe: Resources: international cooperation against cybercrime)

Specific field: Protection of children

- Prevention, protection, prosecution
- Conditions for effective enforcement
- Public private cooperation
- Legislative engagement based on Budapest Convention on Cybercrime and Lanzarote Convention on the Protection of Children against Sexual Exploitation and Sexual Abuse

(See: www.coe.int/children and EU Safer Internet Programme)

Specific field: Financial investigations and prevention of fraud and money laundering

- Crime reporting systems
- Prevention and public awareness
- Regulation, licensing, supervision
- Risk management and due diligence
- Harmonised legislation
- Specialised units and interagency cooperation
- Public-private cooperation and information exchange
- Training
- International cooperation
- Implementation of Budapest Convention in combination with FATF recommendations or CoE Convention on Laundering, Search, Seizure and Confiscation of the Proceeds from Crime and on the Financing of Terrorism (CETS 198)

(See: Typology Report on Criminal Money on the Internet)

Specific field: Prevention and control of terrorist use of ICT

- Legislation and institution building for the implementation of the Convention on the Prevention of Terrorism in combination with Budapest Convention and other tools
- Rule of law and human rights requirements (Council of Europe guidelines 2002)

(See: www.coe.int/terrorism)

Geographical scope

- Projects at country, regional or global levels
- Countries invited to accede or interested in Budapest Convention
- Legislation as starting point to engage in cooperation
- Cooperation with regional organisations (AU, ASEAN, APEC, ECOWAS, OAS, SPC and others)
- A flexible resource to respond to needs and opportunities in any country

Experience

- Council of Europe **Global Project on Cybercrime** (since 2006): Support to several hundred activities involving some 120 countries worldwide on harmonisation of legislation, law enforcement and judicial training, public-private cooperation and international cooperation. Annual Octopus conferences on cooperation against cybercrime. So far funded by Estonia, Japan, Monaco, Romania, Microsoft, McAfee and Visa Europe as well as the budget of the Council of Europe. Phase 3 to start in January 2012

- EU/CoE joint **Project on Cybercrime in Georgia** (2009/2010): Assisted Georgia in adoption of legislation on cybercrime and on the protection of personal data, design of a high-tech crime unit and of training programmes for judges and prosecutors, and in conclusion of a memorandum of understanding between law enforcement and service providers

- EU/CoE joint project on cooperation against cybercrime in EU pre-accession countries (2010 – 2013): "**CyberCrime@IPA**" covers eight countries and areas in South-eastern Europe. Launched in November 2010 it focuses on cybercrime policies and strategies, harmonisation of legislation, international cooperation, law enforcement training, financial investigations, law enforcement/service provider cooperation, assessment of progress made

- EU/CoE joint Eastern Partnership regional project (2011-2013): "**CyberCrime@EAP**" 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/service provider cooperation, financial investigations, international cooperation

(See: www.coe.int/cybercrime)

Contact

Council of Europe
Data Protection and Cybercrime Division
Directorate General of Human Rights and Rule of Law
Strasbourg, France
Email alexander.seger@coe.int

Version 30 March 2012

www.coe.int/cybercrime