Project on Cybercrime
www.coe.int/cybercrime

COUNCIL OF EUROPE CONSEIL DE L'EUROPE

Strasbourg, 22 July 2010
Provisional

Global Project on Cybercrime (Phase 2)

Progress report – Update

1 March 2009 – 30 June 2010

Prepared by the
Economic Crime Division
Directorate General of Human Rights and Legal Affairs

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

For further information please contact:

Economic Crime Division
Directorate General of Human Rights and Legal Affairs
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

Contents

Executive summary

This report provides a compendium of activities implemented under the Global Project on Cybercrime (Phase 2) between 1 March 2009 and 30 June 2010. It updates the progress report covering the period March to September 2009.

The project organised or contributed to more than 75 activities since it was launched in March 2009, ranging from legislative reviews, training workshops and two global Octopus conferences to contributions to events organised by others. As in the past, the project relied on cooperation with a multitude of other stakeholders, be it national authorities, international organisations as well as the private sector and non-governmental initiatives. The project – in particular the partnership with Microsoft – is itself a good example of public/private cooperation.

In addition to the initial voluntary contributions from Romania, Microsoft, McAfee and allocations from the Council of Europe budget, new contributions were received from Estonia, Monaco and Microsoft in the first half of 2010, which were crucial to continue the implementation of this project scheduled for 28 months (1 March 2009 – 30 June 2011). Nevertheless, the project remains underfunded and it is uncertain whether activities foreseen can indeed be completed to achieve the intended impact.

The aim of the project is to promote broad implementation of the Budapest Convention on Cybercrime (CETS 185) and its Protocol on Xenophobia and Racism (CETS 189) as well as related international standards on data protection and the online abuse of children. It builds on the achievements of phase 1 of the Project on Cybercrime which ended in February 2009[1].

Progress towards the project objective so far was satisfactory with Germany, Moldova and Serbia ratifying the Convention on Cybercrime in 2009 and Azerbaijan, Montenegro, Portugal and Spain in 2010, with Romania, Serbia, Montenegro and Portugal ratifying the Protocol on Xenophobia and Racism, with Chile having been invited to accede to the Convention on Cybercrime and Argentina and Australia also seeking accession. Legislative reforms continue in many countries, often with the support of the project. The judicial training concept developed during this period, the promotion of measures for the protection of children against sexual exploitation and abuse, the activities on international cooperation and law enforcement/service provider cooperation, and the initiation of activities related to criminal money flows on the internet as well as data protection are promising. As in phase 1, the project has been able to cooperate with a large number of public and private sector stakeholders which enhances markedly the impact of this project. The relationship between measures against cybercrime and the promotion of fundamental rights and the rule of law have been reinforced.

In the previous report, the fact that many member States of the Council of Europe had not ratified the Budapest Convention and five had not signed it was considered a major concern undermining the credibility of this important treaty in other regions of the world. One the one hand, this concern still holds (18 CoE member States including 10 EU countries are not yet parties; Andorra, Monaco, Russian Federation, San Marino and Turkey have not yet signed it). On the other hand, progress has been made compared to early 2009, and ratification and the adoption of relevant legislation are now high on the agenda of almost all European countries. For the European Union, implementation of the Budapest Convention is a clearly defined policy objective (see, for example, the Stockholm Programme). In many other

[1] Final Report available at www.coe.int/cybercrime

regions of the world, cybercrime legislation is being developed in line with the Budapest Convention and interest in acceding is clearly growing.

Beyond the impact in terms of signatures, ratifications and accessions as well as the quality of implementation, it should be underlined that the global Project on Cybercrime uses the Budapest Convention as a vector to promote human rights and the rule of law on the internet, supports the implementation of related European and international agreements (for example on data protection, the protection of children or the prevention of terrorism), creates additional tools for training, institution building and public/private cooperation, and provides a platform for multi-stakeholder cooperation.

Since the launching of Phase 1 in 2006, the project thus considerably enhanced the global value of the Budapest Convention.

Cross-cutting activities

The project consists of seven components reflected in seven "expected results". Between March 2009 and June 2010 a number of cross-cutting activities were carried out that contributed to several results and the project objective. These include in particular:

- the global Octopus Conferences on cooperation against cybercrime in Strasbourg in March 2009 and March 2010, each with some 300 participants which prepared the ground for project activities on training, international cooperation, criminal money flows on the internet and the online protection of children against sexual exploitation and abuse
- contributions to the meetings of the Cybercrime Convention Committee (T-CY) in March 2009 and June 2010
- contributions to shaping of global cybercrime policies (UN Crime Congress and UN Crime Commission)
- work on solutions to the challenges related to cloud computing
- strengthening of cooperation with the European Union and the OECD
- synergies between the present global Project on Cybercrime and the Project on Cybercrime in Georgia, the PROSECO joint project of the CoE and the European Commission on judicial networking in south-eastern Europe and the joint project on money laundering and the financing of terrorism in the Russian Federation
- participation in the meetings of the European Dialogue on Internet Governance (EuroDIG) and the Internet Governance Forum (IGF).

Progress made specifically towards the seven expected results can be summarised as follows:

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

- Azerbaijan, Germany, Moldova, Montenegro, Portugal, Serbia and Spain ratified the Convention on Cybercrime
- Chile was invited to accede to the Convention and Argentina and Australia are seeking accession
- Montenegro, Portugal, Romania and Serbia ratified the Protocol on Xenophobia and Racism committed through Computer Systems
- Reforms in Bosnia and Herzegovina and "the former Yugoslav Republic of Macedonia" have been initiated. Both are parties to the Convention on Cybercrime but legislation does yet not comply fully with the treaty

- Legislative advice was provided to countries of ASEAN, Latin America, North Africa and the Middle East countries through regional workshops
- Strong cooperation with the Organisation of American States (OAS)
- Intensive dialogue with Argentina on cybercrime legislation, policies and accession to the Budapest Convention
- Constructive cooperation with Indonesia continued and this country could seek accession to the Convention
- Cooperation with Morocco was taken up again and Morocco could seek accession to the Convention
- Legislative advice was provided to Senegal. Given the law on cybercrime adopted in 2008, Senegal could seek accession to the Convention on Cybercrime
- Legislative advice was also provided to Nigeria and Uganda. Unless support to reform efforts in Africa is intensified, Africa will become a major source of cybercrime given the expansion of fibre optic networks on this continent
- Legislative advice was also provided to Montenegro, Vietnam and Korea
- Cooperation with Pacific island states commenced and initial advice was provided
- In Turkey, progress was made concerning the possible signing of the Budapest Convention.

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

- The study on the functioning of 24/7 points of contact and the workshop held at the Octopus conference helped clarify the role and limitations of 24/7 points of contact and encouraged the more recently created contact points in Europe to become more active
- Measures to render contact points more effective were identified.

While cooperation between the G8 High-tech Crime Subgroup and the CoE will require further discussion by the Cybercrime Convention Committee, the Project on Cybercrime should focus not only on contact points but also on other channels of cooperation (such as Interpol) and on making mutual legal assistance more efficient.

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

- The LEA-ISP guidelines adopted at the Octopus conference in 2008 are yielding an impact in several countries and at the level of the European Union
- The guidelines are now available in many languages (English, French, Arabic, Georgian, Portuguese, Romanian, Russian, Spanish, Ukrainian)
- The Project on Cybercrime helped create a working group in Ukraine to improve LEA-ISP cooperation
- LEA-ISP cooperation was also promoted in India
- The Governmental Advisory Committee of ICANN endorsed law enforcement proposals to ensure due diligence and prevent criminal misuse of domains that have also been supported by the Project on Cybercrime.

In addition to activities carried out under the Global Project on Cybercrime the joint European Union/Council of Europe Project on Cybercrime in Georgia contributed to a memorandum of understanding between law enforcement and service providers in Georgia in May 2010 based on the principles of the guidelines.

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

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. The MONEYVAL plenary confirmed this study in September 2009. A project team led by the Russian Federation was established and by June 2010 agreement had been reached on the structure of the report, replies to a questionnaire had been received and tasks had been distributed. The study is thus well on track.

The study will help create bridges between anti-money laundering and anti-cybercrime worlds and may have important impact around the world.

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

- Between March and September 2009 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. This is a major achievement and may yield considerable impact
- Judges and prosecutors trained through workshops in Albania, Egypt, Germany, Pakistan, Portugal and Romania.

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

Specific activities under this component have been limited so far. However, data protection and privacy issues were raised on a number of occasions and the ground was prepared for future activities:

- The authorities of Morocco were encouraged in July 2009 to seek accession to the CoE's Convention on data protection (CETS 108) since new legislation is now in place in this country
- Following an exchange of letters, the Project on Cybercrime is now able to participate in the meetings of the OECD's Working Group on Information Security and Privacy
- A presentation was made on "privacy and security: what are the issues?" at the meeting of the European Dialogue on Internet Governance (EuroDIG) in Geneva on 14 September 2009
- The issue of data protection in connection with cloud computing was raised in multiple events, including the Octopus Conference in March 2010.

In terms of data protection policies the decision of the CoE's Committee on Data Protection (T-PD) to work towards a modernisation of the data protection convention CETS 108 and of the CoE to encourage non-member States of the CoE to accede to this treaty (and its Protocol CETS 181) are positive developments. Data protection legislation and systems in line with this treaty and accession to this treaty should be of interest to non-European countries as it would indicate that they meet European data protection standards which in turn facilitates off-shoring of services from Europe as well as law enforcement cooperation with Europe.

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

- Between March 2009 and June 2010, the Project on Cybercrime organised or contributed to eleven events through which implementation of Article 9 of the Convention on Cybercrime and of the Convention on the Sexual Exploitation of Children (CETS 201) was promoted. This treaty entered into force on 1 July 2010
- A comparative study on substantive criminal law provisions related to the sexual exploitation and abuse of children was launched
- Cooperation with APEC, ECPAT, UNICEF, the European Commission, the OECD and a range of other organisations and initiatives (e.g. eNASCO, the European Financial Coalition etc) as well as the private sector was sought to seek synergies and enhance the impact of the Project on Cybercrime in this respect.

The way ahead

The first sixteen months of implementation clearly demonstrated the growing impact of the Project on Cybercrime and the coming months will build on this. Project priorities in the period July to December 2010 include:

- Policy dialogue with CoE member States in view of signatures and ratification of the Convention on Cybercrime
- Legislation – Continued support to the strengthening of legislation and the process of ratification/accession to the Convention on Cybercrime in particular with regard to CoE member States and countries already invited to accede
- Judicial training – Support to the implementation of judicial training concept and the delivery of training seminars
- Criminal money – Completion of the typology exercise on criminal money flows on the internet
- Children – Completion of the analysis of substantive criminal law provisions on the protection of children from sexual exploitation and abuse, and activities to promote the Convention on the Sexual Exploitation and Sexual Abuse of Children (CETS 201)
- Cloud computing – continued research on solutions to transborder access, jurisdiction, data protection and procedural safeguards (including support to the work undertaken by the Cybercrime Convention Committee)
- Initiation of a concept paper on cybercrime strategies for discussion at the 2011 Octopus Interface conference.

Demands for assistance are increasing. However, the ability of the Council of Europe and this project to respond to such demands is limited by a lack of resources. The tight budgetary situation means that some activities had to be cancelled already and others are at risk.

As indicated above, the project was launched with initial contributions from Romania, Microsoft and McAfee as well as funding from the budget of the CoE (project DGHL/1429 on economic crime). In the first half of 2010, additional contributions were received from Estonia, Monaco and Microsoft. Nevertheless, by June 2010 less than 50% of the estimated budget of Euro 1.4 million had been received and most of this already spent. The remaining balance is very limited and it is rather unpredictable which of the activities planned are actually feasible in terms of funding.

In short, the conditions for further global impact of this project are there: clear standards of reference to work towards, subject matter expertise, momentum created in and requests for assistance from many countries, a vast network of contacts and expertise, support by the private sector and credibility among stakeholders across sectors and regions.

The Convention on Cybercrime has received strong support by the European Union[2], Interpol, the Asia-Pacific Economic Cooperation, the Organisation of American States[3] and other organisations[4] and initiatives as well as the private sector. Many model laws, guidelines or handbooks are based on this treaty.

Donors and organisations may want to take advantage of the opportunities that the project provides and become active partners in this global effort against cybercrime.

Furthermore, and as follow up to discussions at the Octopus Interface conference in March 2010 and the meeting of the Cybercrime Convention Committee in June 2010, the possibility of setting up an agreement on action against cybercrime to assess needs, facilitate technical assistance and global capacity building, as well as to assess progress made by countries against cybercrime will need to be further explored. Such an agreement could help create a more sustainable basis and add an element of monitoring and accountability to global efforts against cybercrime.

---

[2] In the Stockholm Programme for the period 2010-2014 (adopted in December 2009), the European Union states, for example, that "this Convention should become the legal framework of reference for fighting cyber-crime at global level" (section 4.4.4).
http://www.se2009.eu/polopoly_fs/1.26419!menu/standard/file/Klar_Stockholmsprogram.pdf

[3] See for example the recent Recommendations of Sixth Meeting of the Working Group on Cybercrime, Washington DC, 21-22 January 2010. http://www.oas.org/juridico/english/cyb_VIrec_en.pdf

[4] For example, several detailed workshops on cybercrime legislation on the basis of the Budapest Convention have been held with ASEAN member states, the most recent one in Manila, Philippines, on 26-28 January 2010 as a joint activity of the ASEAN Secretariat, the European Union and the Council of Europe.

1 Background

Cybercrime poses new challenges to criminal justice and international cooperation. In order to counter cybercrime and protect computer systems, Governments must provide for:

- effective criminalisation of cyber-offences. The legislation of different countries should be as harmonized as possible to facilitate cooperation
- investigative and prosecutorial procedures and institutional capacities, which allow criminal justice agencies to cope with high-tech crime
- conditions facilitating direct cooperation between State institutions, as well as between State institutions and the private sector
- efficient mutual legal assistance regimes, allowing for direct cooperation among multiple countries.

The "Budapest" Convention on Cybercrime (CETS 185) of the Council of Europe helps countries respond to these needs. It was opened for signature in November 2001 and by June 2010 had been ratified by 30 and signed by another 16 countries. These include non-European countries such as Canada (signed), Japan (signed), South Africa (signed) and the USA (signed and ratified). Chile, Costa Rica, the Dominican Republic, Mexico and the Philippines have been invited to accede. The Additional Protocol on the Criminalisation of Acts of a Racist and Xenophobic Nature Committed through Computer Systems (CETS 189) of January 2003 has been ratified by 17 and signed by another 17 States. Equally important is that a large number of countries worldwide are using the convention as a guideline or "model law" for the strengthening of their cybercrime legislation.

From September 2006 to February 2009, the CoE implemented the first phase of the Project on Cybercrime. That phase of the project was possible due to generous funding and support provided by Microsoft and the Government of Estonia that complemented CoE funding.

The aim of the project was to promote broad implementation of the Convention on Cybercrime (CETS 185) and its Protocol on Xenophobia and Racism (CETS 189), and to deliver specific results in terms of legislation, criminal justice capacities and international cooperation.

More than 110 activities were carried out during that period ranging from legislative reviews, training workshops and global conferences to contributions to events organised by others. The project relied on cooperation with a multitude of other stakeholders, be it national authorities, international organisations as well as the private sector and non-governmental initiatives.

The project helped create and sustain a global momentum towards stronger legislation. As a result, more than 100 countries around the world either have cybercrime laws in place or are in the process of preparing legislation using the Convention on Cybercrime as a guideline or "model law". The project thus helped establish the Convention as the primary standard of reference globally.

Results also included:

- the preparation of guidelines for law enforcement – Internet service provider cooperation which were adopted by the global conference in Strasbourg in April 2008 and which have since been made use of by the European Union and different countries
- the promotion of the training of judges and prosecutors

- the establishment of 24/7 points of contact in countries that are parties to the Convention
- the strengthening of multi-stakeholder cooperation, among other things through the global Octopus conferences.

Based on the experience and the additional needs identified during Phase 1, a follow up Phase 2 was launched in March 2009 at the global Octopus Conference with the following objectives 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)
Output 1	Legislation and policies: Cybercrime policies and legislation strengthened in accordance with the Convention on Cybercrime and its Protocol
Output 2	International cooperation: Capacities of 24/7 points of contact, high-tech crime units and of authorities for mutual legal assistance strengthened
Output 3	Investigation: Law enforcement – service provider cooperation in the investigation of cybercrime improved on the basis of the guidelines adopted in April 2008
Output 4	Financial investigations: enhanced knowledge among high tech crime units and FIUs to follow money flows on the internet and stronger cooperation between financial intelligence and investigation units, high-tech crime units and the private sector
Output 5	Judges and prosecutors: Training for judges and prosecutors in cybercrime and electronic evidence institutionalised
Output 6	Data protection and privacy: Data protection and privacy regulations in connection with cybercrime investigations improved in line with CoE and other relevant international standards
Output 7	Exploitation of children and trafficking in human beings: Enhanced knowledge of standards against the sexual exploitation and abuse of children and trafficking in human beings on the internet

Contributions from the Government of Romania, Microsoft and McAfee in addition to CoE funding allowed Phase to commence. In early 2010, Estonia (which had been co-funding Phase 1) and Monaco also became partners in Phase 2 of the project.

The present report summarises activities implemented under the Global Project on Cybercrime (Phase 2) between 1 March 2009 and 30 June 2010.[5]

[5] This thus includes information already contained in the first progress report of September 2009 and adds activities carried out since then.

2 Activities and results

2.1 List of completed activities

Date	Place	Description
March 2009	Strasbourg	Finalisation of the study on 24/7 points of contact
9 March 2009	Strasbourg	Indonesia – Legislative review workshop
9 March 2009	Strasbourg	Project planning meeting
10-11 March 2009	Strasbourg	Octopus Interface conference
20 March 2009	Portugal	Training workshop for judges and prosecutors
26 March 2009	New Delhi, India	Workshop on international cooperation and law enforcement – ISP cooperation
7 April 2009	Bosnia and Herzegovina	Legislative review workshop (PROSECO)
15 April 2009	Singapore	Child protection online OECD – APEC symposium
16-17 April 2009	Albania	Workshop for judges, prosecutors and law enforcement (PROSECO)
27-28 April 2009	Tallinn, Estonia	Presentation at EU Ministerial Conference on Critical Information Infrastructure Protection
29 April 2009	Ukraine	Workshop on law enforcement – ISP cooperation
April	Strasbourg	Provide legislative advise on the new amendments to the Criminal Code and updated the country profile in Macedonia
5 May 2009	Brussels	Public Presentation on "Protecting children using the internet" organised by the European Economic and Social Committee (EESC)
7 May 2009	Brussels (via teleconference)	2CENTRE Cybercrime Centres of Excellence Network WG Open Meeting
14-15 May 2009	Trier, Germany	Contribution to workshop on effective responses to cybercrime (Academy of European Law)
15 May 2009	Strasbourg	Provide legislative advise 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 in Uganda
19 May 2009	Strasbourg	Analysis of the legislation on cybercrime in Senegal
2 June 2009	Strasbourg	Providing update comments on the amendments on cybercrime legislation in "the former Yugoslav Republic of Macedonia"
8-10 June 2009	Amsterdam	MAAWG conference
30 June 2009	Berlin	International Conference "Protection of Girls and Boys against Sexual Violence in the New Media"
6 July 2009	Lisbon	Meeting on institutionalizing training on cybercrime for judges and prosecutors
7 – 27 July 2009	Strasbourg	Drafting the concept paper on the training of judges
14 -15 July 2009	Morocco	Workshop on cybercrime legislation
20-27 July 2009	Strasbourg	In cooperation with MONEYVAL a proposal for the preparation of a "typology project" was drafted on "Criminal money flows on the internet"
29-30 July 2009	Nigeria	Workshop on the Cybercrime Convention
July 2009	Strasbourg	Internet Governance Forum and EuroDIG preparations
July 2009	Strasbourg	CoE submission to the Inquiry into Cyber Crime conducted by the Australian Standing Committee on Communications
Aug 2009	Strasbourg	Update of the country profile for Vietnam
3-4 September 2009	Strasbourg	Workshop on cybercrime training for judges and prosecutors
8-9 September 2009	Lyon	Meetings at Interpol
14 September 2009	Geneva	Contribution to the EuroDIG

16 September 2009	Luxemburg	EC: Second meeting of Internet Focus Group "Fighting against online child abuse images"
21 September 2009	Strasbourg	Project Planning Group meeting (via conference call)
5-9 October 2009	Geneva	ITU Telecom World 2009. Contribution to a workshop on the cost of cybersecurity
6-7 October 2009	Vienna	UNODC: Expert Group Meeting on Cybercrime
8-9 October 2009	Bucharest	ERA- TAIEX seminar on Fight against cybercrime
12-14 October 2009	Paris	OECD Working Party on Information Security and Privacy (WPISP)
14 October 2009	Paris	OECD: cloud computing workshop
13-15 October 2009	Asunción, Paraguay	Contribution to US DOJ workshop on cybercrime legislation for countries of Latin America
16 October 2009	Buenos Aires, Argentina	Bilateral meetings to promote accession by Argentina to the Convention on Cybercrime
1-3 November 2009	Vancouver	Information Security Forum 20th Anniversary Annual World Congress
5-6 November 2009	Brussels	EC: Annual cybercrime conference: EU-US cooperation
15-18 November 2009	Sharm el Sheikh, Egypt	The fourth annual IGF Meeting
18-19 November 2009	Hanoi	Séminaire francophone Droit des technologies de l'Information
27 November 2009	Brussels	EC: Conference on Public-Private Sector dialogue on tackling online illegal activities
7-8 December 2009	Egypt	Training workshop 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
11-13 December 2009	Courmayeur Mont Blanc, Italy	International Conference on Protecting Children from Sexual Offenders in the Information Technology Era
September/ December 2009	Strasbourg	Study on the criminalisation of child pornography and related measures
12 January 2010	Ankara, Turkey	Ankara Bar Association International Law Congress 2010 – Cyber Crimes 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 (preparatory meeting)
10 February 2010	Buenos Aires, Argentina	Meeting on the Budapest Convention on Cybercrime
16-18 February 2010	Malta	MENA Cybercrime Legislation Workshop
17-18 February 2010	Brussels	EastWest Institute - the 7th Worldwide Security Conference
23-24 February 2010	Islamabad, Pakistan	Cybercrime training for law enforcement and judges
16-17 March 2010	Barcelona, Spain	SecureCloud 2010 - ENISA joint Conference on Cloud Computing
23-25 March 2010	Strasbourg	Global Octopus Interface conference on cooperation against cybercrime

26 March 2010	Strasbourg	Working meeting on the typology study on criminal money on the Internet
31 March – 1 April 2010	Lille	French National Gendarmerie: International Forum on Cybercrime
12-19 April 2010	Salvador, Brazil	The 12th United Nations Congress on Crime Prevention and Criminal Justice
29-30 April 2010	Madrid	EuroDIG 2010
6 May 10	Brussels	Brainstorming session on the EU Internal Security Strategy
17–21 May 2010	Vienna, Austria	Nineteenth session of United Nations Commission on Crime Prevention and Criminal Justice
18 May 10	Como, Italy	Contribution to meeting of the International Automobile Federation (FIA): Legal and Consumer Commission's workshop held on 18 May 2010 in Como
9-11 June 10	Izmir, Turkey	Contribution to International Informatics Law Assembly
7- 12 June 10	Malta	Contribution to Commonwealth workshop on "Legal Frameworks for ICTs"
16-18 June 10	Strasbourg	Advisory paper for meeting of ICT ministers from Pacific Islands in Tonga (written submission)
22 June 10	Rome, Italy	Contribution to UNICRI Symposium on the state of Online Trust in Europe
23 June 10	Geneva	Contribution to the Cyber Security Course: Meeting the Cybersecurity Challenge (Geneva Security Forum)
24-25 June 2010	Paris, France	Contribution to the meeting of the Cybercrime Convention Committee (T-CY)

2.2 Cross-cutting activities

2.2.1 Setting up the project team (March – July 2009)

In addition to the head of the Economic Crime and Information Society Department who continues to follow the projects on cybercrime, the team responsible for the project consists of:

- A programme manager for cybercrime (an expert seconded by the Ministry of Justice of Romania from 15 March 2009)
- An assistant project officer (from 1 July 2009 until 1 June 2010)
- An administrative assistant (from 1 March, working part time on these projects).

The global Project on Cybercrime was managed jointly with the Project on Cybercrime in Georgia which started on 1 June 2009 and ended on 31 May 2010. This allowed for synergies and reinforced the project team with benefits for both projects.

In CoE activities cybercrime is increasingly a cross-cutting issue reflected in different projects. For example:

- Several activities were organised in cooperation with the PROSECO project (networking among prosecutors against organised crime and corruption in South-eastern Europe): while the PROSECO project provided funding and logistics and ensured interaction with counterparts from prosecution services and ministries of justice, the Project on Cybercrime took responsibility for the substance and the selection of speakers
- Through the MOLI projects against money laundering and terrorist financing in the Russian Federation and in Ukraine, the participation of representatives of these two countries in the Octopus Conference (Strasbourg, March 2009), in particular the workshop on criminal money on the internet, was ensured
- The cybercrime project team also interacts closely with activities of the CoE related to the information society, the protection of children, money laundering (MONEYVAL), the Internet Governance Forum or the European Dialogue on Internet Governance.

This horizontal interaction creates synergies and broadens the impact of the Project on Cybercrime.

2.2.2 Project planning meetings, activity and progress reports

On 9 March 2009, a project planning meeting was held at the CoE with the participation of representatives of confirmed donors (Romania, Microsoft and McAfee), a prospective donor (Germany), the chairperson of the Cybercrime Convention Committee as observer and the CoE. A second meeting of the planning group was held on 21 September in the form of a telephone conference and a third one in conjunction with the Octopus Conference in March 2010.

Regular activity reports were sent to donors and published on the project website.

A first progress report covering the period 1 March to 15 September 2009 had been prepared in September 2010. The present progress report was finalised in July 2010 to update the previous report covering in a cumulative manner the period 1 March to 30 June 2009. The next update of report will be due in January 2011.

2.2.3 Octopus Interface conference (Strasbourg, 10-11 March 2009)

Some 300 cybercrime experts from more than 70 countries, international organisations and the private sector met at the Council of Europe in Strasbourg from 10 to 11 March 2009. The extensive materials and presentations made available are evidence of the high quality and variety of the discussions.

- The conference provided an update on:
  - The implementation of the Convention on Cybercrime. More than 100 countries worldwide use the Convention as a guideline for their legislation. Progress has been made in terms of ratifications and accessions but countries are encouraged to accelerate the ratification/accession process. Ratification of the Convention by Germany on the day before the Conference was very much appreciated as encouragement to others
  - The guidelines on law enforcement – ISP cooperation in the investigation of cybercrime adopted at the last conference have been taken up by the European Union, France and other countries

- Phase 2 of the global Project on Cybercrime was launched. The themes covered by the conference reflected the components to be covered by this project. The conference thus provided guidance to the project

- Access to training resources: The conference showed what training on cybercrime is on offer for law enforcement, prosecutors and judges. The conference in particular saw the launch of the "2CENTRE", a joint action of law enforcement and industry for cybercrime training. With regard to prosecutors and judges proposals have been discussed to further improve training materials and institutionalise judicial training. The Lisbon Network of the Council of Europe and the Global E-Crime Prosecutors Network (GPEN) offer opportunities in this respect. CYBEX has developed a model training course for judges. Common issues are the question of certification of training and trainees, the different levels of knowledge required by different people and the sustainability and replicability of training

- Criminalising child pornography and sexual exploitation and abuse of children on the Internet: Article 9 of the Convention on Cybercrime and the Convention on the Sexual Exploitation and Sexual Abuse of Children (CETS 201) provide a comprehensive normative framework in this respect. However, only a few countries have so far fully implemented Article 9. Many other countries should therefore review and improve their current provisions in line with this Article. Countries should update their country profiles to facilitate such reviews. Consideration should also be given to the implementation of the new offences introduced by Convention 201. With regard to the obligations or liability of ISPs for child abuse materials there are differences regarding access, hosting and content providers. A number of issues require further debate: Should these obligations be governed by contract, self-regulation or formal legislation? To what extent do ISPs have the obligation to prevent crime or only to support investigations? What are the consequences of a failure to comply? It may be useful to further study good practices regarding different approaches and their implications

- Following criminal money on the Internet: The conference helped share experience, good practices and opportunities for cooperation in terms of (a) typologies of proceeds generating crime, money flows and money laundering, (b) strategies,

techniques and tools to search, follow, seize and confiscate such proceeds, and (c) opportunities for multi-stakeholder action to follow criminal money and prevent cyber-fraud and cyber-laundering. The conference pointed at the need to establish trust between different public and private sector stakeholders involved in anti-cybercrime and anti-money laundering and terrorist financing measures, and to build bridges between the anti-cybercrime and anti-money laundering communities, between law enforcement, internet industry, financial services and others. Examples discussed included the Financial Action Task Force, Moneyval, the Anti-Phishing Working Group, the London Action Plan, the Advance Fee Fraud coalition or the Hi-tech Crime Forum in Ireland. Countries should also make sure that different types of cybercrime are predicate offences for money laundering. Countries should also be aware of the risks of networks such as VoIP that may need further regulations

- Effectiveness of international cooperation: the conference discussed proposals to make international cooperation against cybercrime more effective. For example, contact points need to become more proactive and make themselves known, and help facilitate mutual legal assistance. The Council of Europe and the G8 High-tech Crime Subgroup should organise their management of the 24/7 network of contact points. Solutions need to be found to expedite mutual legal assistance (article 31 of the Convention). As a minimum, countries should make use of possibilities for direct cooperation between authorities that are provided for in a number of European instruments. The network of 24/7 points of contact is primarily for urgent measures. For other, less urgent cases, other channels are used, in particular Interpol. The strengthening of law enforcement – ISP cooperation remains a concern in many countries. The Project on Cybercrime could study good practices and further possibilities regarding a contact list for law enforcement and Internet Service Providers to facilitate cooperation not only at the national but also international level

- The future of cybercrime – challenges and solutions: The conference stimulated the debate on "jurisdiction, national borders and law enforcement in the times of cloud computing". Computer data and services will increasingly move from specific, identifiable computers in a specific location to the "clouds", that is, they are hosted in data centres in unspecified locations. And different technologies will become increasingly interconnected. This has implications for security and law enforcement and creates legal uncertainties and inconsistencies. These and other questions raise a number of challenges related to data protection and identity management. The Council of Europe should further study the implications of "cloud computing" on jurisdiction, law enforcement and national borders. It may also be necessary to review in this light the adequacy of data protection instruments that have been in place for more than 25 years.

Follow up:

- The issues raised at the conference are followed up to under the different components by the Project on Cybercrime and within the limits of the resources available.

2.2.4 Cybercrime Convention Committee, T-CY (Strasbourg, 12-13 March 2009)

The Project on Cybercrime participated in the meeting of the T-CY, and presented among other things, studies it had been tasked to be prepared in the 2008 meeting, that is:

- A study on the functioning of 24/7 points of contact
- A study on Internet jurisdiction

The need for the Project on Cybercrime to work globally in a pragmatic manner was underlined as stated in the meeting report:

> The Project on Cybercrime emphasised the fact that the implementation of the Convention must be supported worldwide. Therefore, a pro-active involvement of the Parties is necessary to:
> - achieve political, moral and practical support for the accession process from Parties and experts;
> - obtain funding, as resources are limited;
> - be able to respond to any need, also from non-member states. A pragmatic approach of flexibility to co-operate with non-member states is necessary.
>
> The Project on Cybercrime also underlined that it is in the interest of the Parties to the Convention on Cybercrime that co-operation in the framework of technical assistance projects is extended to interested states or territories worldwide with a view to strengthening national legislation and international co-operation (including the 24/7 contact points) in the fight against cybercrime, even if these states and/or territories may not necessarily accede to the Convention.

2.2.5 EU Ministerial Conference on CIIP (Tallinn, Estonia, 27-28 April 2009)

The CoE participated at EU Ministerial Conference on Critical Information Infrastructure Protection (27-28 April 2009, Tallinn, Estonia). The aim was to present the Convention on Cybercrime as a key element of strategies to protect critical information infrastructure.

The event was organised by the Estonian Ministry of Economic Affairs and Communications under the auspices of the Czech Presidency and in cooperation with the European Commission which had a few weeks earlier issued its Communication on Critical Information Infrastructure Protection (COM(2009)149). The meeting underlined the importance that Estonia attributes to CIIP and cybercrime. It consisted of a ministerial segment on 27 April and workshops and plenary discussions on 28 April.

While the meeting focused on CIIP, the discussion paper made available by the Estonian organisers underlined that "*the social and economic dimensions of the process of enhancing network and information security in Europe must be synergetic with the needs and strategies of law enforcement and of the fight against cyber-crime and cyber-terrorism*".

The CoE was invited to speak in the workshop on international cooperation and legal instruments. The CoE speaker underlined that

- instruments against cybercrime (in particular the Convention on Cybercrime) should be made use of in relation to CIIP as it may be more appropriate, in most cases, to deal with attacks against public infrastructure as a crime issue than as a question of defence/national security
- given the transnational nature of attacks, the focus on tools and instruments at the level of the European Union (as presented by most speakers during the conference) may be too limited. A more open approach would be appropriate. The Convention on Cybercrime and the Convention for the Prevention of Terrorism of the Council of Europe provide solutions, at least for cybercrime and terrorist use of information and communication technologies. In particular the Convention on Cybercrime is

already applied globally. The European Commission and the EU Council have repeatedly called on EU m/s not only to ratify the Convention on Cybercrime but also to promote its implementation worldwide.

In his key note address, H.E. Toomas Hendrik Ilves, President of the Republic of Estonia underlined that countries should make use of the Convention on Cybercrime.

Follow up:

- The links between CIIP and cybercrime and between solutions to these threats should be analysed in greater detail. The Octopus conference in March 2010, among other things, discussed the role of CERTS/CSIRTS[6] with respect to cybercrime.

2.2.6 Cooperation with the OECD (Strasbourg, May 2009 – June 2010)

Further to the Ministerial Conference on the Future of the Internet Economy of the Organisation for Economic Cooperation and Development (OECD) in Seoul on 16-17 June 2008, the Deputy Secretaries General of both organizations agreed to intensify cooperation in cybercrime matters.

This was followed up by an exchange of letters between the two Deputy Secretaries General in May/June 2009. Both organisations agreed that cooperation could be strengthened in the following areas:

- Malware: the OECD, in cooperation with the Asia-Pacific Economic Cooperation (APEC), in 2008 prepared a malware study which calls for the launching of a global "Anti-Malware Partnership". The CoE is supporting the strengthening of legislation, law enforcement and international cooperation against malware and other types of cybercrime. The CoE could share its experience with the OECD, and the OECD in turn could help promote the Convention on Cybercrime and other standards in non-European countries, including the APEC region. The CoE could also consider participating in the "Anti-Malware Partnership", in particular with regard to legal frameworks and law enforcement
- Protecting children online: the OECD is developing policies and raising awareness in this field. The CoE is promoting criminal law measures to protect children from sexual exploitation and abuse online, as well as the safer use of the internet by children. Both organizations could share each other's experience and promote each other's standards and practices. The OECD and the CoE are already coordinating the preparation of their respective studies on the online protection of children (OECD) and substantive law approaches to the sexual exploitation of children on the internet (CoE)
- Cloud computing and other challenges: both organizations could cooperate to explore solutions to arising challenges such as the question of jurisdiction and cross-border law enforcement in the times of cloud computing
- Data protection and privacy: both organizations already cooperate and participate in each other's activities in this field. The CoE intends to further promote data protection and privacy standards through technical cooperation activities against cybercrime. The CoE could share its experience in this respect with the OECD, and the OECD could take CoE standards into account when cooperation also with non-member States of the CoE.

[6] Computer Emergency Response Teams/Computer Security Incidents Response Teams. For a list of CERTS/CSIRTS see http://www.cert.org/csirts/national/contact.html.

Follow up given:

- Malware/botnets: the OECD Working Party on Information Security and Privacy (WPISP) meet in Paris on 12-13 October 2009, among other things, to discuss the Anti-Malware Partnership. The Council of Europe was invited to participate. Follow up activities were planned on that occasion
- Protecting children online: The Council of Europe participated in an APEC/OECD workshop on the exploitation of children in Singapore on 15 April 2009. Follow up was discussed at the OECD WPISP meeting in Paris on 13 October 2009. The OECD has since then launched a study on enabling children for safe Internet use. With the CoE working on a study on criminal law measures to protect children, the OECD and the CoE closely consult with each other to ensure complementarity.
- The CoE and the OECD promoted each other work at the Internet Governance Forum in Egypt (November 2009)
- Cloud computing and other challenges:
  - The OECD organised on 14 October 2009 (in Paris) a foresight forum on cloud computing. The CoE was invited to participate. The CoE presentation underlined that full implementation of the Convention on Cybercrime will help meet some of the challenges related to privacy and security in the cloud but that also trusted privacy standards need to be implemented globally and that specific guidance may be necessary with regard to access to data stored on servers in other countries.
  - The CoE and the OECD participated in IGF workshop number 257 on "The Privacy & Security Implications of Cloud Computing" that was organised jointly by the CoE, Electronic Privacy Information Center (EPIC), the US Federal Trade Commission and the French Ministry of Foreign and European Affairs (Egypt, November 2009)
  - The OECD participated as observer in the meeting of the T-CY in June 2010.

2.2.7 EuroDIG and IGF preparations (Strasbourg, July/August 2009)

The Project on Cybercrime contributed to the preparations for the European Dialogue on Internet Governance (Geneva, 14-15 September 2009) and Internet Governance Forum (Sharm El-Sheikh, Egypt, 15-18 November 2009).,

The EuroDIG included a workshop on cybercrime and cybersecurity.

With regard to the IGF at the Open Consultations held at the United Nations in Geneva on 13 May 2009, the CoE organised an information session for IGF stakeholders on the Convention on Cybercrime and the latest developments regarding the Project on Cybercrime.

Regarding cybercrime-related IGF events in Egypt (November 2009), the CoE contributed to the preparation of or is scheduled to speak in a series of workshops and fora:

- 160. Securing Cyberspace: Strategy for the Future
- 232. Four sisters – Information security, data protection, privacy and electronic governance – another year and new developments
- 93. The Global Path for ensuring Online Child Protection and Safety: Effective Strategies and Specific Actions
- 68. Best practice forum: Developing comprehensive cybercrime legislation completed
- 288. Child Online Safety Indicators: Measuring the Un-measurable?

- 257. The Privacy & Security Implications of Cloud Computing
- 179. Cybercrime training for judiciary and law enforcement as a tool for internet governance.

2.2.8 EuroDIG (Geneva, 14-15 September 2009)

For a summary of the Project's contribution to EuroDIG see section 2.8.1.

2.2.9 ITU Telecom World 2009 (Geneva, 5-9 Oct 2009)

During the ITU Telecom World 2009, the CoE contributed to a workshop on the cost of cybersecurity. The main argument put forward by the CoE was that the "cost of cybersecurity" was not just a question of economics or technology but should also be evaluated in terms of human rights, democracy and the rule of law. Global rules are required and the Convention on Cybercrime, guidelines for public-private cooperation and other tools promoted by the Project on Cybercrime are instrumental in this respect. However, specific solutions would still need to be defined to address challenges related to cloud computing (privacy, transborder access to data etc).

2.2.10 UNODC Expert Group Meeting on Cybercrime (Vienna, 6-7 October 2009)

The CoE through the Project on Cybercrime, contributed to this Expert Group Meeting of the United Nations Office on Drugs and Crime (UNODC).

Participants: UNODC, Council of Europe, European Commission, Interpol, Europol, OSCE, OSCE-ATU, 2CENTRE, Microsoft, IMPACT, GPEN (UK), EBay, CYBEX (Spain), Technology Risk Limited (UK), Garda Computer Crimes Investigation Unit (Ireland), University College of Dublin, experts from Argentina, Brazil, China, Japan, Kenya, Korea, Qatar, Philippines, Pakistan, Russia, and US, Permanent Missions of Argentina, Russia and Tunisia.

The purpose of the meeting was to discuss what role UNODC could play in the fight against cybercrime, how it could cooperate with existing initiatives and how it could promote a more coordinated and sustainable approach to combat cybercrime in developing countries. Thus, an overview of the current initiatives and actors in the field addressing the threats of cybercrime was provided with a focus on the programmes and activities carried out in different regions and their impact, interaction and gaps. Although the report lacks important initiatives and developments at the global level, there is no doubt that UNODC could play a strong role in promoting the broad implementation of the Convention and providing technical assistance on cybercrime to various countries.

In the meeting, the active role of the CoE both in fighting cybercrime by promoting global standards and providing technical assistance also to many developing countries was underlined. While some interventions argued for a new United Nations treaty on cybercrime, most others were supportive of the idea of focusing on capacity building to ensure the implementation of existing tools and instruments.

2.2.11 Launching the CoE Newsletter (Strasbourg, October 2009)

The purpose of the newsletter is to send periodically an update on the activities carried out under the Project on cybercrime.

2.2.12 20th World Congress of the ISF (Vancouver, 31 October – 3 November 2009)

Some 400 information security professionals from major corporations, primarily from Europe and northern America (e.g. ABN AMRO, Air France, Barclay's Bank, Boeing, BBC, British Airways, Credit Suisse, EADS, Fujitsu, Goldman Sachs, Hewlett Packard, IBM, Michelin, Microsoft, Orange, PricewaterhouseCoopers, Samlink, Société Générale, Volvo etc.) participated in the 20th Annual World Congress of the Information Security Forum.

The CoE participated in a cyber-response panel with the CEO of the IFS and former White House Cybersecurity Adviser) and the Assistant Director of Interpol as well as in a "guru panel" together with BT, Oracle and the former Assistant Secretary of Homeland Security underlining the links between security, data protection and fundamental rights.

The meeting showed that:

- cloud computing is very high on the agenda of all stakeholders and is indeed an issue that the Council of Europe through the Project on Cybercrime, T-CY and T-PD should be dealing with from a cybersecurity and data protection/privacy perspective;
- data protection/privacy is very much of concern to US and European companies. Harmonisation of regulations within Europe is a particular concern of European companies
- in Europe a more cooperative approach is pursued between industry and law enforcement with respect to information security than in the USA
- the "end-to-end-trust" approach proposed by Scott Charney could be indeed a means to enhance security through authentication while ensuring privacy.

A number of representatives confirmed their interest in contributing to the work of the CoE with regard to security and privacy. The Information Security Forum could be used as a means to reach out to hundreds of major corporations. The meeting was furthermore useful in terms of reinforcing contacts with the FBI and Interpol.

2.2.13 EU-US expert meeting on cross-border cooperation (Brussels, 5-6 November 2009)

Some 35 representatives of EU member States, the US Department of Justice, Secret Service and the FBI, Europol as well as INHOPE, the European Financial Coalition and the Council of Europe. The CoE made a presentation on the policy context of cybercrime and moderated the session on jurisdiction.

The meeting:

- expressed its support to the Budapest Convention on Cybercrime. This is reflected in the draft Stockholm Programme and the US Cyber Policy Review
- agreed that a public-private contact list should be established to facilitate cooperation among law enforcement, ISPs and hotlines
- agreed that the question of the role of law enforcement in internet governance should be strengthened. Key issues to be addressed in this context are due diligence and accountability of registrars, and the privatisation of WHOIS (which would make law enforcement much more difficult). Interlocutors for discussions are ICANN (Governmental Advisory Committee) and regional registrars (e.g. RIPE for

Europe, Middle East and Russia). A position could be developed for the ICANN meeting in June 2010 in Amsterdam
- concluded that a regular dialogue between the US and the EU should be held.

2.2.14 Fourth Meeting of the IGF (Sharm El Sheikh, Egypt, 15-18 November 2009)

The fourth meeting of the Internet Governance Forum focused on the overall theme of 'Internet Governance – Creating Opportunities for All'.

With more than 1800 participants from 112 countries (96 governments were represented) the meeting had the biggest attendance.

Parallel to the main sessions, more than 100 workshops, best practice forums, dynamic coalition meetings and open forums were scheduled around the broad themes of the main sessions and the overall mandate of the IGF.

The meeting discussed new issues related to the continued growth of social networks, and the ensuing governance issues that are emerging, in particular the need for new approaches regarding privacy and data protection, rules applicable to user-generated content and copyrighted material, and issues of freedom of expression and illegal content.

To objective of CoE participation was to promote its instruments and tools on internet governance, including:

- Convention on the Protection of Individuals with regard to the Automatic Processing of Personal Data (CETS 108)
- Convention on Cybercrime (CETS 185)
- Convention on the Protection of Children against Sexual Exploitation and Sexual Abuse (CETS 201)
- Concept for cybercrime training of judges and prosecutors.

Overall the IGF meeting confirmed that the CoE is perceived as a valuable partner in internet governance with whom other stakeholders wish to cooperate.

Discussions examined:

- ways to improve Internet access by all and promote local content and cultural diversity;
- ensure the safety of the Internet and fight cybercrime;
- manage key Internet resources such as the root server system, technical standards, interconnection and telecommunications, the domain name system and Internet protocol addresses.

Events and results related to cybercrime included:

2.2.14.1 Briefing by European NGO Alliance on Child Safety Online - eNASCO (Saturday, 14 Nov 09)

The briefing – addressed also by EU Commissioner Viviane Reding – included in particular the presentation of "A Digital Manifesto – an agenda for change".

Added value of CoE participation:

- eNASCO pledged to reflect CoE instruments (in particular Convention on the Protection of Children against Sexual Exploitation and Sexual Abuse (CETS 201)

and Convention on Cybercrime (CETS 185) in a revised complete version of the "Manifesto".

2.2.14.2 Workshop 93: The Global Path for Ensuring Online Child Protection and Safety: effective strategies and specific actions (Sunday, 15 Nov 09)

The CoE co-organised this workshop together with ECPAT and ATT and provided one speaker. The workshop focused on effective strategies and specific actions in developing and promoting a safe and productive experience for children and youth online and protecting children and youth from exploitation and abuse. It was aimed at promoting multi-stakeholder cooperation by identifying common elements (strategies/specific actions/good practices), contributions by and synergies between different stakeholders, and mechanisms for interaction and cooperation.

Added value of CoE participation:

- Speakers and participants underlined the need for a clear legal basis to investigate crimes related to the sexual exploitation of children and to hold offenders accountable
- Approaches need to make sure that fundamental rights are protected (including privacy, the freedom of expression, self-determination) and the security of children is ensured at the same time
- The workshop concluded that in order to put a comprehensive legislative framework in place that is internationally harmonized and permits efficient international cooperation, countries should make use of the Convention on the Protection of Children against Sexual Exploitation and Sexual Abuse (CETS 201) and the Convention on Cybercrime (CETS 185).

2.2.14.3 Best Practice Forum 87: 2CENTRE, the Cybercrime Centres of Excellence for Training, Research & Education (Monday, 16 Nov 09)

2CENTRE is a European project which aims at uniting law enforcement, industry and academic expertise to provide an internationally coordinated cybercrime investigation training program for law enforcement agencies and the industry in the European Union and beyond. The CoE participated with one speaker.

Among the four memoranda of understanding signed on 18 November by the Egyptian Government in a special session in the presence of the First Lady of Egypt, Mrs. Mubarak, was also a MoU with Microsoft aiming to establish a 2CENTRE of excellence for training and supporting innovation in internet safety for the youth online.

Added value of CoE participation:

- Speakers and participants provided excellent feedback on the role of the CoE in measures against cybercrime and helped strengthen ties with the Ministry of Communication and Information Technology of Egypt, University College Dublin, Microsoft and others.

2.2.14.4 Main session workshop on Security, Openness and Privacy (Monday, 16 Nov 09)

- Main session workshops are high-profile events that are translated into the official languages of the UN, transcribed and broadcasted through webcast. The CoE participated with one panellist, who focused on security and fundamental rights:

how to ensure security while maintaining due process, freedom of expression and privacy in a global environment?

Added value of CoE participation:

- Nomination for participation in the panel of the main session is a reflection of the recognition of the work of the CoE.
- Following the workshop a short meeting with the Minister of Communication and Information Technologies of Egypt was held. The Minister pledged to initiate work on cybercrime and data protection legislation and to consult with the CoE in these matters.

2.2.14.5 Workshop 179: Cybercrime training for judges and law enforcement (Tuesday, 17 November 09)

The CoE was a co-sponsor of this event, funded the participation of India (main organizer of the workshop) and provided two speakers.

Added value of CoE participation:

- The event allowed the CoE to present the "concept on cybercrime training for judges and prosecutors", which had recently been developed by the Project on Cybercrime and the Lisbon Network, and the workshop and round table that will be organized in Egypt in December with the support of the Project on Cybercrime.
- It was agreed that the training concept should also be promoted in India through a workshop in 2010.
- During the workshop as well as in a subsequent discussion with UNODC it was agreed that the CoE and UNODC should cooperate in cybercrime training. With regard to the forthcoming UN Crime Congress in Brazil, the UNODC representative pledged to have the CoE participate in an ancillary meeting on cybercrime and possibly also in a plenary session (UNICRI also was interested to have the CoE intervene in a workshop on cybercrime and organized crime).

2.2.14.6 Best Practice Forum 68: Developing cybercrime legislation (Tuesday, 17 November 09)

The event underlined that comprehensive and consistent legislation is essential to help societies meet the challenge of cybercrime and thus to enhance the security of and confidence in information and communication technologies. Legal frameworks should take into account the rights of users and the role of the private sector on the one hand, and security concerns on the other. The Convention on Cybercrime of the Council of Europe provides a global guideline in this respect. The CoE was the main organizer of this forum, funded three experts from Germany, India and Sri Lanka and provided one speaker.

Added value of CoE participation:

- Promoted globally harmonised legislation based on international standards, in particular the Council of Europe Convention on Cybercrime.
- The workshop also highlighted the substantial assistance provided by the Council of Europe within the Project on cybercrime to different countries to harmonise their criminal law provisions on cybercrime with those of other countries in order to facilitate international cooperation.
- The participants' questions underlined the complexity of the legislation on cybercrime and the need for assistance and international joint efforts.

2.2.14.7 Workshop 257: The security and privacy implications of cloud computing (Tuesday, 17 November 09)

The CoE was a co-organiser of this workshop together with EPIC and the French Ministry of Foreign Affairs, and participated with two speakers.

The Coe intervention focused on how to ensure security and privacy in the clouds:

- Existing instruments make sense, and thus full implementation of the Budapest Convention on Cybercrime will help address some of the challenges ("Exploiting existing opportunities by all")
- Enhance the efficiency of application of international cooperation provisions of the Convention on Cybercrime and others
- Develop additional international standards on law enforcement access to data stored abroad / in the clouds
- Insist on procedural safeguards/due process / clear procedures for cooperation between cloud providers and law enforcement -> provide guidance to service/cloud providers
- Establish globally trusted privacy / data protection standards and systems
- Cloud provider that cannot guarantee data protection/privacy standards and procedural safeguards will have a competitive disadvantage.

2.2.14.8 Workshop 288: Child Online Safety Indicators: Measuring the Un-measurable? (Wednesday, 18 November 09)

This event was organised by the Cyber Peace Initiative of Egypt and the ITU. The CoE provided one speaker.

Added value of CoE participation:

- The workshop showed how the Convention on the Protection of Children against Sexual Exploitation and Sexual Abuse (CETS 201) provides benchmarks to measure progress made in the implementation of actions to protect children
- CoE participation confirmed close cooperation with the authorities of Egypt
- It furthermore indicated that the CoE is prepared in principle to cooperate with the ITU.

2.2.14.9 Follow up

- The Council of Europe – through the Project on Cybercrime – to continue supporting widely the strengthening of comprehensive legislation on cybercrime, data protection and protection of children against sexual exploitation and sexual abuse and to promote relevant instruments globally
- Cloud computing: the CoE – through the Project on Cybercrime – organised a discussion on the security and privacy issues at stake for discussion at the Octopus conference (March 2010)
- The IGF prepared the ground for closer cooperation between Egypt and the CoE. In December 2009, the Project on Cybercrime organised training sessions for judges in Cairo. Further support should focus on the preparation of legislation on cybercrime, data protection and child exploitation in view possible future accession to Conventions 108, 185 and 201
- The question of the role of ICANN and registries to ensure due diligence and prevent the criminal abuse of domains was be discussed at the Octopus conference in March 2010, and the CoE supported the respective recommendations also at the ICANN meeting in Brussels in June 2010

- In order to ensure stronger involvement in Internet governance, the CoE became an observer in the Government Advisor Committee (GAC) of ICANN in June 2010.

2.2.15 Preparation of the 1st West African Internet Fraud Summit (Abuja, Nigeria, 2-3 Feb 2010)

The meeting discussed the organisation of the 1st West African Cybercrime Summit, which will take place in autumn 2010 in Abuja, Nigeria. The event is hosted by EFCC in partnership with UNODC and the private sector.

The participants (Council of Europe, ECOWAS, EFCC, European Union Delegation Nigeria, Europol, French Gendarmerie, Google, INTERPOL, Microsoft, UK SOCA, UNODC, US Department of Justice) agreed:

- The 1st West African Cybercrime Summit will focus on: raising political awareness and commitment to combat cybercrime, legislative framework, training, capacity building/sustainability and international cooperation
- The event will bring together an international group of political leaders and decisions makers, criminal justice authorities, industry representatives and other relevant stakeholders
- Summit Planning Committee: EFCC (West African LE), Microsoft (Industry), UNODC (Intl Development), ECOWAS (Region), IMMWG (US/UK LE).

On this occasion the song "Maga No Need Pay" was launched in Nigeria within an awareness campaign supported by EFCC, Microsoft and UNODC.

Follow up:

- CoE, as a member of the planning committee, to participate in the organization of the Summit
- Organise the workshop on legislation, which will propose concrete activities to allow West Africa to develop its capacity
- Contribute to the plenary sessions, which have the objective to demonstrate to political leaders that developing capacity against cybercrime and online fraud will have a positive impact on the economic development of the regions
- Invite the EFCC and Microsoft to present the song at the opening session of the Council of Europe global Octopus Conference on cooperation against cybercrime, which will showcase the song as a global best practice for education and awareness against cybercrime.

2.2.16 EWI 7th Worldwide Security Conference (Brussels, 17-18 February 2010)

This conference covered a wide range of security issues, including a special consultation on "international pathways to cybersecurity". In this context, the CoE through the Project on Cybercrime, participated in a workshop on legal cooperation.

Follow up:

- The EastWest Institute intends to focus stronger on the question of cybersecurity through its "Worldwide Cybersecurity Initiative". However, it would be useful that this initiative be more closely linked to existing mechanisms and initiatives underway, build on progress made already, and put a stronger focus on criminal justice issues.

2.2.17 SecureCloud 2010 (Barcelona, Spain, 16-17 Mar 10)

The CoE, through the Project on Cybercrime, contributed to this joint conference of ENISA and the Cloud Security Alliance on cloud computing which involved several hundred participants. The CoE presentation focused on law enforcement and data protection issues.

The meeting helped prepare for the Octopus conference and secured the participation of ENISA and the Cloud Security Alliance in Octopus.

2.2.18 Octopus Interface conference (Strasbourg, 23-25 March 2010)[7]

More than 300 cybercrime experts representing countries from all continents, international organisations and the private sector met at the Council of Europe in Strasbourg from 23 to 25 March 2010 to enhance their cooperation against cybercrime. At the close of the conference participants adopted key messages aimed a guiding further action.

Participants share a common interest in pursuing the most effective approaches against the growing threat of cybercrime that societies worldwide are faced with.

Effective approaches against cybercrime comprise a wide range of innovative initiatives and actions that need to be pursued in a dynamic and pragmatic manner by public and private sector stakeholders.

At the same time, measures against cybercrime are a shared responsibility and should be based on a set of common principles to allow for clear guidance to governments and organisations, to facilitate partnerships and to ensure the political commitment to cooperate.

In this connection, participants in the conference underline that:

- For security and the protection of rights to reinforce each other, measures against cybercrime must follow principles of human rights and the rule of law.
- Security and the protection of rights is the responsibility of both public authorities and private sector organisations.
- Broadest possible implementation of existing tools and instruments will have the most effective impact on cybercrime in the most efficient manner.

Following detailed discussions, participants recommend:

- Making decision makers aware of the risks of cybercrime and encouraging them to exercise their responsibility. Indicators of political commitment include steps towards the adoption of legislation and institution building, effective international cooperation and allocation of the necessary resources
- Implementation of the Budapest Convention on Cybercrime worldwide to sustain legislative reforms already underway in a large number of countries. Countries should consider becoming parties to make use of the international cooperation provisions of this treaty. Consensus on this treaty as a common framework of reference helps mobilise resources and create partnerships among public and private sector organisations. In this connection, the ratification of the Budapest Convention by Azerbaijan, Montenegro and Portugal prior and during the conference, and the expression of interest to accede by Argentina and other countries serve as examples to other countries

[7] See Appendix for key messages and workshop summaries of the conference.

- Establishing the Budapest Convention as the global standard goes hand in hand with strengthening the Cybercrime Convention Committee (T-CY) as a forum for information-sharing network, policy-making and standard-setting. It is encouraged to address issues not (exhaustively) regulated by the provisions of the Cybercrime Convention such as electronic evidence, jurisdiction and liability of ISP's
- Coherent and systematic training of law enforcement, prosecutors and judges based on good practices, concepts and materials already available
- The establishment and strengthening of high-tech crime and cybercrime units, and incidents response and reporting teams and systems
- The development of cooperation procedures between law enforcement agencies, CERTs/CSIRTs as well as internet service providers and the IT industry
- Due diligence measures by ICANN, registrars and registries and accurate WHOIS information. Endorsement of the "Law Enforcement Recommended Amendments to ICANN's Registrar Accreditation Agreement (RAA) and Due Diligence Recommendations" in line with data protection standards. ICANN is encouraged to implement these recommendations without delay
- The many networks and initiatives against cybercrime that exist already create a dynamic and innovative environment involving a wide range of actors. Stronger networking among networks is encouraged to allow for synergies and reduce duplication. The mapping of networks exercise initiated by the Council of Europe should be continued
- A contact list for enhanced cooperation between industry and law enforcement should be established. A proposal for a secure portal for interested parties is in preparation
- Initiatives aimed at preventing, protecting and prosecuting the sexual exploitation and abuse of children are most valuable but require stronger support and consistency. The "Lanzarote" Convention of the Council of Europe (CETS 201) offers guidance in this respect and provides benchmarks to determine progress
- Making use of the guidelines for law enforcement – ISP cooperation adopted at the Octopus Conference in 2008
- Completion and broad dissemination of the results by the Council of Europe of the typology study on criminal money flows on the Internet that is currently underway.
- In order to meet the law enforcement and privacy challenges related to cloud computing existing instruments on international cooperation – such as the Data Protection Convention (CETS 108) and the Budapest Convention – need to be applied more widely and efficiently. Additional international standards on law enforcement access to data stored in the "clouds" may need to be considered. Globally trusted privacy and data protection standards and policies addressing those issues need to be put in place and the Council of Europe is encouraged to continue addressing these issues in its standard-setting activities as well as by the Global Project on Cybercrime.

Public authorities, international organisations, civil society (including non-governmental organisations) and the private sector should apply existing tools and instruments without delay and cooperate with each other to identify additional measures and responses to emerging threats and challenges.

In order to add impetus and resources to efforts against cybercrime and allow societies worldwide to make best possible use of tools, instruments, good practices and initiatives already available, a global Action Plan aimed at obtaining a clear picture of criminal justice capacities and pressing needs, mobilising resources and providing support, and assessing progress made should be launched, preferably by the United Nations and the Council of

Europe in partnership with the European Union, Parties to the Budapest Convention, and other interested parties.

The results of the Octopus conference should be submitted to the United Nations Crime Congress in Salvador, Brazil (12-19 April 2010) for consideration.

2.2.19 Project on Cybercrime – Partners' meeting (Strasbourg, 25 March 2010)

Following the Octopus Conference a meeting for actual and prospective project donors and partners was held on 25 March 2010 with the participation of representatives from public (Croatia, Estonia, France, Mexico, Monaco and Romania) and private sectors (CERT-Lexsi, Kaspersky Labs, Microsoft, Orange Labs, MAAWG, PayPal, SAP, Team Cymru, and Visa Europe).

Participants discussed progress made and further plans under the Global Project on Cybercrime as well as reasons for becoming a partner, including:

1. Partners share common objectives, that is, enhancing security and trust in information technologies on the basis of human rights and rule of law standards
2. Partners participate in a cost-effective way in a global capacity building effort and thus respond to needs expressed by countries worldwide
3. The project strengthens the eco-system, that is, the regulatory and institutional framework for information technologies
4. Partners engage in public-private cooperation
5. Partners inform each other and receive up to date information on developments worldwide
6. Participation in this project entails reputational benefits and visibility
7. The project produces results.

The example of Microsoft – a partner since 2006 – illustrates the value of public-private cooperation against cybercrime. In addition to voluntary contributions:

- Expertise from Microsoft is feeding into project activities
- Council of Europe expertise feeding into activities organised by Microsoft
- The Council of Europe and Microsoft carry out joint activities
- Microsoft is sharing information on relevant developments in different regions of the world
- Microsoft facilitating contacts and providing logistical support.

Follow up:

- The interest expressed by participants needs to be translated into specific cooperation agreements.

2.2.20 International Forum on Cybercrime (Lille, 31 March – 1 April 2010)[8]

This event organised for the 4th time by the Gendarmerie of France provided a platform for many hundred participants from different countries but primarily from France to exchange ideas. It took place shortly after the Octopus conference and allowed to follow upon some of the key messages, as reflected in the presentation of the Minister of Interior of France.

[8] http://www.fic2010.fr/fr/php/accueil.php4

The CoE, through the Project on Cybercrime presented the results of the Octopus conference and the need for a global capacity building effort based on existing instruments in the plenary session on "La mobilisation européenne et internationale pour la lutte contre la cybercriminalité" and in a workshop organised by the OSCE on "Une approche globale de la cyber-sécurité".

2.2.21 12th United Nations Crime Congress (Salvador, Brazil, 12-19 April 2010)

The United Nations Congress on Crime Prevention and Criminal Justice held intensive discussions on cybercrime in Committee II (agenda item 8. recent developments in the use of science and technology by offenders and by competent authorities in fighting crime, including the case of cybercrime) and in the negotiation of the political "Salvador Declaration".

In Committee II some speakers argued for the preparation of a new treaty on the grounds that this would enhance ownership also of developing countries, while others underlined the need for operational action on the basis of existing instruments and in particular the Budapest Convention on Cybercrime. There was, however, general agreement on the need for technical assistance to build criminal justice capacities to cope with cybercrime. Specific reference was made by some speakers to the outcome of the Octopus conference. The discussions in Committee II are reflected in the draft report A/CONF.213/L.4/Add.1. This document, in Paragraph 17, proposes the preparation of an Action Plan for capacity building.

The compromise reached regarding cybercrime in the political Salvador Declaration is reflected in paragraphs 41 and 42:

> *41. We recommend that the United Nations Office on Drugs and Crime, upon request, provide, in cooperation with Member States, relevant international organizations and the private sector, technical assistance and training to States to improve national legislation and build the capacity of national authorities, in order to deal with cybercrime, including the prevention, detection, investigation and prosecution of such crime in all its forms, and to enhance the security of computer networks.*
>
> *42. We invite the Commission on Crime Prevention and Criminal Justice to consider convening an open-ended intergovernmental expert group to conduct a comprehensive study of the problem of cybercrime and responses to it by Member States, the international community and the private sector, including the exchange of information on national legislation, best practices, technical assistance and international cooperation, with a view to examining options to strengthen existing and to propose new national and international legal or other responses to cybercrime.*

In short: broad agreement on technical assistance and capacity building as well as public-private cooperation, but no agreement on the preparation of a new treaty.

The Council of Europe had closely consulted with Parties to the Budapest Convention and other partners prior to the Congress. Octopus Conference (23-25 March 2010), and the Secretariat of the Council of Europe (submission of the Secretary General to the UN Crime Congress, statement of the Director General at the Congress) had argued that a global capacity building effort based on existing instruments was the most effective way ahead. The UN Crime Congress confirmed this as the most feasible option.

2.2.22 United Nations Crime Commission, Nineteenth session (Vienna, 17-21 May 2010)

The UN Commission on Crime Prevention and Criminal Justice held intensive informal consultations on the outcome of the Salvador Crime Congress and as to which of the recommendations to take on.

With regard to cybercrime, discussions focused on the establishment of an intergovernmental expert group. In this respect, as part of umbrella Resolution IV regarding follow up to Salvador, the wording of Article 42 of the Salvador Declaration was accepted, but it was added that this expert group be convened "prior to the twentieth session of the Commission" (that is, before May 2011):

> *Draft resolution IV*
> *Twelfth United Nations Congress on Crime Prevention and Criminal Justice*
>
> *The General Assembly,*
> *……*
> *9. Requests the Commission on Crime Prevention and Criminal Justice to establish, in line with paragraph 42 of the Salvador Declaration, an open-ended intergovernmental expert group, to be convened prior to the twentieth session of the Commission, to conduct a comprehensive study of the problem of cybercrime and responses to it by member States, the international community and the private sector, including the exchange of information on national legislation, best practices, technical assistance and international cooperation, with a view to examining options to strengthen existing and to propose new national and international legal or other responses to cybercrime;*

An earlier draft of this resolution reflected Article 41 of the Salvador Declaration on technical assistance/capacity building ("We recommend that the United Nations Office on Drugs and Crime, upon request, provide, in cooperation with Member States, relevant international organizations and the private sector, technical assistance and training to States …"). However, in the course of the consultations at the UN Crime Commission, this provision was deleted. According to some delegations there was reluctance to broaden the mandate of UNODC given the scarcity of resources that it has at its disposal. On the other hand, there is a reference to technical assistance related to cybercrime in connection with the UN Convention on Transnational Organised Crime which could provide an entry point.

Follow up:

- The Council of Europe and other interested organizations and parties other public and private sector stakeholders would need to undertake increased efforts to respond to requests for assistance
- The question of a mechanism to assess needs, mobilize assistance and assess progress made needs to be further explored
- The CoE to participate in the intergovernmental expert group as an observer.

2.2.23 EuroDIG (Madrid, 29-30 April 2010)

This workshop on "Cross-border cybercrime jurisdiction under cloud computing" allowed to continue the discussion of the Octopus conference and to identify the questions that need to be addressed with regard to cross-border law enforcement access to data on cloud servers, the role of Internet service providers and the question of data protection. It re-affirmed the need for international guidance through best practice guidelines, or a soft-law instrument (recommendation) or a binding hard-law instrument (for example a protocol to the Budapest Convention on Cybercrime). The need for globally trusted data protection systems (based for example on the data protection convention 108 of the Council of Europe) was underlined once again.

EuroDIG recommended:

- Full implementation of existing tools and instruments against cybercrime, in particular of the Budapest Convention, and for the protection of personal data, using Convention 108 as the starting point will help address a number of the challenges related to cloud computing
- The Council of Europe in cooperation with the European Union and other international organisations to establish a multi-stakeholder working group composed of experts of the private sector, civil society, academics and government representatives to provide guidance on issues raised by cloud-computing, covering cybercrime aspects as well as data protection, jurisdiction and conflict of law aspects
- The Council of Europe to draft specific policies and guidance for LEA to carry out trans-border criminal investigations
- The Secretary General of the Internet Governance Forum to consider the issue of cybercrime jurisdiction in the agenda of the upcoming IGF meeting in Vilnius (Lithuania).

2.2.24 Symposium on the state of online trust in Europe (June 21-22, 2010, Rome, Italy)

The event was organised by UNICRI with the support of VeriSign and it was intended as a 'pilot' to examine the feasibility of hosting further events of the same format (throughout Europe, Asia and Africa) to share experiences among various sectors (e.g. financial, e-commerce, governmental and law enforcement).

50 participants, mostly experts or representatives of different organizations and initiatives, participated in the meeting. The Council of Europe presented the work carried out under the global Project on Cybercrime, which includes cooperation with various stakeholders and private sector, calling for building upon the work that has been already done in the past years.

Follow up:

- Explore the possibility of cooperation with VeriSign, which expressed its interest to work with the Council of Europe.
- Invite VeriSign to contribute to the event to be held in August in Mexico.

2.2.25 Meeting the Cybersecurity Challenge (23 June 2010, Geneva)

The Council of Europe was invited to speak at the "Cyber Security Course: Meeting the Cybersecurity Challenge" at the Geneva Centre for Security Policy (GCSP) to address the participants of cybersecurity course held on 23-24 June 2010.

The Geneva Centre for Security Policy (GCSP) is an international training centre for security policy with 40 member states that offers courses for civil servants, diplomats and military officers from all over the world.

The course had the following objectives:

- To deepen course participants' understanding of cyber threats and vulnerabilities, including the potential effects on critical infrastructures
- To gauge the national security threat posed by cyber insecurity and cyber attacks

- To give participants an overview of measures taken at the national and international level to protect information and communication technologies.

The discussions look into these issues mostly from the angle of protecting the computer systems.

In the panel on "Legal challenges to cyber security" the Council of Europe representative stressed on the need to work not only on the measures to protect computer systems from such attacks but also to enforce criminal law measures that would enable the authorities to prosecute the perpetrators.
The Council of Europe's approach with regard to technical cooperation to countries worldwide, achievements and lesson learnt during the past years work on cybercrime have been presented.

Follow up:

- Consider the possibility of involving the Geneva Centre for Security Policy in the research of the Project and invite the (GCSP) to the Octopus Conference in 2011.

2.2.26 Meeting of the Cybercrime Convention Meeting, T-CY (Paris, 24-25 June 2010)[9]

The Project on Cybercrime participated in the meeting of the T-CY and contributed in particular to discussions on:

- the question of a possible partial agreement on action against cybercrime to allow for enhanced activities of the T-CY but also to assess needs, facilitate technical assistance and assess progress made against cybercrime worldwide
- transborder access to data, which is particularly relevant in the context of cloud computing. The T-CY decided to undertake a study to identify possible solutions to this challenge.

[9] For meeting documents see: http://www.coe.int/t/dghl/standardsetting/t-cy/Meetings_2010_en.asp

2.3 Activities related to 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

Indicators:

- Legislation analysed of at least 30 countries
- At least 10 legal opinions provided and at least 15 draft laws available
- Country profiles available for at least 75 countries
- Workshops and conferences on cybercrime legislation organised covering up to 100 countries

Summary of progress towards the expected result:

- Germany, Moldova, Serbia in 2009, and Azerbaijan, Montenegro, Portugal and Spain in 2010 ratified the Convention on Cybercrime
- Chile was invited to accede to the Convention
- Romania, Serbia, Montenegro and Portugal ratified the Protocol on Xenophobia and Racism committed through Computer Systems
- Reforms in Bosnia and Herzegovina and "the former Yugoslav Republic of Macedonia" have been initiated. Both are parties to the Convention on Cybercrime but legislation does yet not comply fully with the Convention
- Constructive cooperation with Indonesia continued and this country could seek accession to the Convention
- Cooperation with Morocco was taken up again and Morocco could seek accession to the Convention
- Argentina and Australia are seeking accession to the Budapest Convention and soon will be formally invited
- Legislative advice was provided to Senegal. Given the Law on Cybercrime of 2008, Senegal could seek accession to the Convention
- Legislative advice was provided to Nigeria, Senegal and Uganda. Unless support to reform efforts in Africa is intensified, Africa will become a major source of cybercrime given the expansion of fibre optic networks on this continent
- Legislative advice was also provided to Montenegro, Vietnam and Korea
- An advisory paper on cybercrime legislation was prepared for Pacific Island States
- Legislative advice was provided to ASEAN countries, Latin America, North Africa and the Middle East countries through regional workshops.

Progress has thus been satisfactory but obviously the path towards legislative reforms remains difficult. The fact that 18 CoE member States have not yet ratified the Convention and five member States (Andorra, Monaco, Russian Federation, San Marino and Turkey) have not yet signed it weakens the credibility of this important treaty in other regions of the world.

The following activities contributed to the progress made:

2.3.1 Indonesia – Legislative review workshop (9 March 2009, Strasbourg)

On 9 March 2009, ten representatives of the Indonesian Ministry of Communication and Information Technology and the Indonesian National Police visited Strasbourg in order to review further draft laws to strengthen Indonesian legislation in line with the Convention on Cybercrime. The delegation also participated in the Octopus Conference on 10-11 March.

In March 2008, the Indonesian Parliament had adopted the Act on Information and Electronic Transactions taking into account proposals made by CoE experts. In November 2008, at a joint ASEAN/EU/Council of Europe workshop in Kuala Lumpur further needs for reform were identified.

The Indonesian Ministry of Communication and Information Technology subsequently prepared a draft "Cybercrime Law" and a draft "Law on the Ratification of the Convention on Cybercrime". The review of these drafts in Strasbourg on 9 March 2009 suggests that with some improvements they would close existing gaps in particular with respect to procedural law.

The workshop concluded that given the important legislation already adopted in 2008 and the current amendments underway, Indonesia could already now seek accession to the Convention on Cybercrime.

2.3.2 Bosnia and Herzegovina – Legislative review workshop (7 April 2009)

On 7 April 2009, a workshop on cybercrime legislation was held in Sarajevo. It was organised under the PROSECO Project in cooperation with the Global Project on Cybercrime.

Although Bosnia and Herzegovina is a Party to the Convention on Cybercrime the current legislation does not meet the requirements of this treaty. The objective of the event was therefore to identify provisions that need further reform in order to ensure full compliance with the Convention. More than 20 representatives from the State level (Ministry of Security, State Prosecutor' Office of Bosnia and Herzegovina), Ministries of Justice and Ministries of Interior from the Federation of Bosnia and Herzegovina and the Republika Srpska participated in the meeting.

The two entities, the Federation of Bosnia and Herzegovina (FBiH) and the Republika Srpska (RS), and Brčko District (BD) have each their separate criminal codes and criminal procedure codes. In some fields legislation is enacted at the State level (e.g. international cooperation, organised crime, terrorism etc.) although some provisions at the state, entity and district level are overlapping. There are thus also State level criminal and criminal procedure codes.

Initially, in 2003, similar provisions on criminal law had been adopted under the criminal codes and criminal procedural codes for FBiH, RS and BD. However, after six years the provisions on cybercrime legislation appear to be diverging.

Existing provisions on substantive law cover only partially the offences required by the Convention. Moreover, they require improvements with regard to the consistency of terms used, coherence and, finally, the level to which they comply with the standards of the Convention.

With regard to procedural law measures required many gaps have been identified. With the exception of search and seizure and interception most of the procedural measures and powers provided for by the Convention seem not to be implemented, although the Convention was already ratified in 2006.

The area of international cooperation also raises questions. The different responsibilities and competent institutions, and the legislation enacted at state, entity and district levels, create difficulties in the cooperation with other countries. Bosnia and Herzegovina may thus only to a limited extent be able to fulfil the obligations on international cooperation that the country assumed when ratifying the Convention.

During the workshop participants agreed on the following recommendations:

- to establish a Working Group within the State-level Ministry of Justice of Bosnia and Herzegovina with representatives of the competent authorities from the Federation of Bosnia and Herzegovina, the Republika Srpska and Brčko District with the task of implementing the requirements of the Convention on Cybercrime by developing a draft law containing the same provisions at the entities and district level
- considering the different provisions on cybercrime adopted at the entities and district level in Bosnia and Herzegovina to discuss the possibility of implementing the Convention on Cybercrime at the State level - within the existing competence of the state - in the ongoing negotiation of the TEAM-WG (Working group for monitoring and assessing criminal legislation)
- to supplement the Criminal Procedure Code at the State level with the provisions of Chapter III of the Convention on Cybercrime in order to ensure the legal framework for Bosnia and Herzegovina to cooperate internationally against cybercrime.

In order to facilitate the discussion after the meeting the Council of Europe submitted a report providing arguments for a regulation at the state level of cybercrime (transnational dimension of cybercrime) and background information for each article of the substantive criminal law and procedural law section of the Convention on Cybercrime. Furthermore, the translation of the Convention on Cybercrime was reviewed.

2.3.3 "The Former Yugoslav Republic of Macedonia" – Legislative advice (Strasbourg, March 2009)

At a request, comments on amendments to the Criminal Code of "the former Yugoslav Republic of Macedonia" were provided and the country profile was updated.

The analysis focused on Articles 1 to 9 of the Convention on Cybercrime and the conclusions underlined that generally the amendments target the main gaps of the substantive law required by the Convention (e.g. Article 1 – definitions (partially) and Articles 4-5). Moreover, they also include some provisions of the Additional Protocol on Xenophobia and Racism and of the Convention on the Protection of Children against Sexual Exploitation and Sexual Abuse (2007). Further consideration should be given to the provisions not yet fully implemented (e.g. Article 1 - the definitions on "service provider" and "traffic data"; Article 6 and Articles 7-8).

With regard to Article 9 and the definitions of "child pornography" and "minor" the amendments are in line with the standards of the Convention with the exception of the acts provided for under Article 9 c.

2.3.4 Montenegro – Legislative advice (Strasbourg, 15 May 2009)

At the request of the Ministry of Justice, the CoE – under the Project on Cybercrime – provided comments on some articles of the Criminal Code (Article 142 CC - definitions and Chapter 28: Articles 349 - 355) concerning their compliance with the requirements of the Convention on Cybercrime.

The comments reflected that the existing provisions of the Criminal Code cover to some extent the requirements of the Convention, in particular Article 1 – definitions (partially), Article 2 – illegal access, Article 3 – illegal interception (partially) and Article 4 – data interference. However, some gaps have been identified in the way of implementing some of the offences required by the Convention while other offences are not provided at all (e.g. Article 6 – Misuse of devices and Article 7 – Computer-related forgery).

The general assessment of the cybercrime provisions suggested that there was a need for further reform of the existing legislation on cybercrime of Montenegro in order to fully comply with the Convention.

In March 2010 Montenegro deposited the instrument of ratification at the Council of Europe.

2.3.5 Uganda – Legislative advice on the Computer Misuse Bill 2008 (Strasbourg, 19 May 2009)

On 19 May 2009, the CoE through the Project on Cybercrime provided general comments on the provisions of Computer Misuse Bill 2008 in the view of implementing the Convention on Cybercrime.

The Bill represents a step forward for Ugandan authorities to criminalise cybercrime including the admissibility of electronic evidence in legal proceedings. However, some important amendments would be required in order to harmonise the law with the content of the Cybercrime Convention. In the field of substantial criminal law most of the offences are only partially covered (e.g. illegal access, illegal interception, data interference, system interference, misuse of devices and computer-related fraud) and some important constituent elements are missing when establishing these offences, or the provisions combine different offences; there is an inconsistency in the use of terms and a number of overlapping provisions.

With regard to criminal procedural law the Bill provides only for search and seizure. It seems that more provisions are in preparation that would cover procedural law measures (i.e. real time collection of data, interception of content data, preservation order) and thus close the main gaps identified in the Bill.

2.3.6 Senegal – Analysis of the legislation on cybercrime (Strasbourg, 19 May 2009)

At the request of the authorities of Senegal, a review of Law 2008-11 on cybercrime of 25 January 2008 was provided by the Project on Cybercrime. The review suggests that this law brings the legislation of Senegal close to the Convention on Cybercrime. Minor amendments would help further improve the law. A number of issues raised may be covered through other laws, in particular with regard to international cooperation.

Given the legislation in place – and although further improvements may be helpful – Senegal could seek accession to the Convention on Cybercrime.

2.3.7 Morocco – Workshop and discussions on cybercrime legislation (Rabat, 14 – 15 July 2009)

The Council of Europe through the Project on Cybercrime participated in a workshop on cybercrime at the Institut d'etudes judiciares (Rabat, 14 July 2009). The purpose was to

assist Morocco in the strengthening of cybercrime legislation and in the possible accession to the Convention on Cybercrime.

Following the "statut avancé" of association that Morocco was granted by the European Union in October 2008, and the subsequent letter of the Deputy Secretary General of the CoE to the Ambassador of Morocco in Brussels there is a strong interest of Morocco to adopt European standards, including CoE instruments. Adherence to CoE conventions is a specific item in the document on the "Statut Avancé".

Discussions with Moroccan counterparts suggest that the Convention on Cybercrime and conventions on children are high on the list of treaties to be implemented. The Ministry of Justice has been tasked to study these treaties, and interest in accession to the Convention on Cybercrime has been expressed by all interlocutors.

Regarding cybercrime legislation most of the substantive law provisions are available already with the exception of Article 3 (illegal interception). A new Penal Code has been prepared and comments have been received from different ministries. It is to be submitted to the Parliament in October 2009 but amendments could still be incorporated.

In terms of procedural law the need for further reforms was pointed out. The Criminal Procedure Code as amended in 2003 is not considered sufficient although provisions are applied by analogy in cases related to cybercrime and electronic evidence. A new CPC is in preparation but the draft is not yet public.

Regarding data protection, a law on the protection of personal data was recently adopted and only the supervisory authority remains to be established. According to Moroccan authorities this law meets the requirements of the EU data protection directive. It was therefore suggested that Morocco consider accession to the Council of Europe Data Protection Convention (CETS 108) as this may then facilitate also cooperation with European law enforcement authorities.

2.3.8 Nigeria – Workshop on the Cybercrime Convention (Abuja, 29-30 July 2009)

On 29–30 July 2009, a Council of Europe mission visited Abuja (Nigeria) within the framework of the Project on Cybercrime. The visit involved a meeting on 29 July held at the Federal Ministry of Justice with representatives of different institutions, and a workshop (with some 200 participants) on the Convention on Cybercrime organised by the Ministry of Justice in cooperation with the law firm Technology Advisers on 30 July.[10]

The major legislative gaps identified:

- Offences against the confidentiality, integrity and availability of computer data and systems are currently not criminalised in Nigeria
- General legal provisions against forgery and fraud exist (intellectual property right of violations, or child pornography) but they are insufficient to cover all situations where they are committed through computer systems
- Electronic evidence is not admissible in court (e.g. under Article 419 of the Penal Code, fraud can be prosecuted based on banking records and criminal money flows, but not on the basis of evidence found on computer systems)
- Law enforcement authorities do not have the power to order the preservation of data, to search and seize computer systems or to order the production of electronic

[10] The visit was facilitated by Mr. Basil Udotai, Technology Advisers, Abuja.

evidence. Traditional criminal law provisions are of limited use, as data is not a "thing"/tangible object and as in any case electronic evidence is not admissible in criminal proceedings

- Nigeria is unable to cooperate internationally as cybercrime is not an offence in Nigeria and in the absence of procedural powers for law enforcement to execute a foreign request.

This situation should be of concern for Nigerian society but also for the international community given the transnational outreach of Nigerian criminal groups (as reflected in the "419" fraud schemes).

In 2004, a working group led by the Directorate of Cybersecurity of the Office of the National Security Adviser had prepared the "Computer Security and Critical Information Infrastructure Bill 2005" in order to close the above gaps. The Council of Europe, through the Project on Cybercrime, had analysed the 2005 Bill and in January 2008 provided detailed comments. The conclusion was that while the Bill reflected almost all provisions of the Convention, some improvements (often only minor corrections) would be necessary. While the 2005 Bill was read in the Senate, the time was not sufficient to complete the process before the end of the legislative period.

In 2008, the House of Representatives prepared a new version of the Bill entitled the "Cyber Security and Information Protection Agency Bill 2008". Articles 1 to 6 (related to the establishment of an agency) are new, while the remaining articles seem to be similar to those of the 2005 Bill. The comments provided by the Council of Europe in January 2008 have not been taken into account. However, discussions in Abuja on 29-30 July 2009 clearly showed that the comments proposed by the Council of Europe in the analysis of January 2008 remain valid as articles 7 to 38 of the 2008 Bill more or less correspond to articles 2 to 34 of the 2005 Bill.

Following two readings of the 2008 Bill, the House of Representatives held a Public Hearing on the Bill on 8 July 2009. A working group was tasked to consolidate the views expressed into a new version of the Bill.

Discussions in bilateral meetings and the workshop suggest the following:

- In the absence of cybercrime legislation and of the possibility to use electronic evidence, in legal terms Nigerian society is currently unprotected against offences committed against or through computer systems. This situation also creates risks to other countries and should thus be very much of concern to the international community. The authorities of Nigeria should therefore take urgent action and adopt legislation as quickly as possible
- The adoption of legislation will need to be followed by capacity building measures, including the training of law enforcement, prosecutors and judges, and measures to strengthen public-private cooperation, in particular between law enforcement and service providers
- The "2008 Bill" foresees in Article 31 that computer evidence be deemed primary evidence. This will have major positive implications, unless if it is limited to evidence gathered by the Cyber Security and Information Protection Agency that is to be established under the Bill. It may be more appropriate to modify the Evidence Act in order to broaden the scope
- While a central body responsible for coordinating policies and measures on cybercrime and cybersecurity, or for providing technical support to other law enforcement bodies in the investigation or prosecution of cybercrime or for taking on the investigation of particularly complex cases may have benefits, the creation

of an agency with the sole responsibility for the "investigation of all cyber crimes" and the enforcement of the bill (including all investigative powers) was questioned. An increasing number of offences involve electronic evidence and therefore it would not be practical if only one agency in Nigeria would have the authority to examine and collect such evidence. Thus many law enforcement bodies in Nigeria that are investigating offences involving electronic evidence (e.g. Copyright Commission) need to have the necessary powers. It should be noted that the 2005 Bill, in its Article 1, conferred the enforcement of the provisions of the Bill "to any law enforcement agency in Nigeria to the extent of the agency's statutory powers in relation to similar offences committed with or without the use of a computer"

- Full implementation of the provisions of the Convention on Cybercrime into national law is required before accession to this treaty by a country is possible. The adoption of an improved version of the current Bill would allow Nigeria to move towards accession. It should be in the interest of Nigeria and of the international community to have Nigeria as a party to the Convention on Cybercrime.

However, it seems that by June 2010, matters had not progressed and Nigeria de facto is still without cybercrime legislation. The forthcoming 1st West African Cybercrime Summit, which will take place in autumn 2010 in Abuja, Nigeria hosted by EFCC in partnership with UNODC and the private sector, could be a good opportunity to accelerate the process.

2.3.9 Australia – CoE submission to Parliamentary inquiry (Strasbourg, July 2009)

The Council of Europe was invited to make a submission to the Inquiry into Cyber Crime conducted by the Standing Committee on Communications of the House of Representatives/Parliament of Australia.

In the submission, the CoE provided comments on:

- the nature and prevalence of e-security, underlining the trends and the challenges for criminal justice
- legislative and regulatory initiatives, stressing the importance of the Convention on Cybercrime in helping countries to address these challenges
- international cooperation; Australia has established a 24/7 point of contact and participates in the network of the G8
- future initiatives to mitigate e-security risks to Australia, showing that full implementation of and accession to the Convention on Cybercrime in the near future would bring a number of benefits to Australia and help further mitigate e-security risks.

The report resulting from this inquiry ("Hackers, Fraudsters and Botnets: Tackling the Problem of Cyber Crime"[11] – June 2010) includes Recommendation 9 that Australia "move expeditiously to accede to the Council of Europe Convention on Cybercrime". Australia indeed expressed its intention to accede, and by June 2010, the invitation to Australia to accede was being processed. It is expected that by the end of September Australia will be formally invited.

[11] http://www.aph.gov.au/house/committee/coms/cybercrime/report.htm

2.3.10 Vietnam – Legislative support (July/August 2009)

Following the ASEAN workshop supported by the Project on Cybercrime (Phase 1) in November 2008 and participation of representatives of Vietnam in the Octopus Conference in March 2009, the authorities of Vietnam, the US Department of Justice and the CoE had planned a joined event in Vietnam in August 2009. Although this event had to be postponed for technical reasons, the Project on Cybercrime assisted in the translation of the Convention on Cybercrime into Vietnamese and carried out an initial analysis of Vietnamese legislation against the provisions of the Convention on Cybercrime.

The strengthening of Vietnamese cybercrime legislation would facilitate international cooperation between Vietnam and other countries, including European countries. Reportedly, financial institutions in some European countries suffer from phishing attacks launched from Vietnam.

Follow up was given in November 2009 (colloquium in Hanoi) and January 2010 (ASEAN workshop on cybercrime legislation in Manila, Philippines).

2.3.11 Belarus dialogue (Strasbourg, July 2009)

In 2008, the CoE contributed to a workshop organised by the OSCE on cybercrime legislation in Belarus. In July 2009, the authorities of Belarus confirmed their interest in cooperating with the CoE in the strengthening of legislation in view of future accession to the Convention on Cybercrime.

However, by June 2010 the Project on Cybercrime had not yet received relevant laws for analysis.

2.3.12 OAS/US DOJ regional workshop on cybercrime (Asunción, Paraguay, 13-15 October 2009)

The CoE contributed to this workshop organised by the United States Department of Justice, the Government of Paraguay and the OAS General Secretariat as follow up to the regional workshop organised in 2008 in Bogota, Colombia by the OAS and the CoE.

Representatives from executive, legislative and judicial institutions from Costa Rica, Ecuador, Guatemala, Mexico, Paraguay, Peru, and Uruguay met to analyze the progress made and the steps that should be taken with respect to legislation to prevent, investigate and sanction cyber-crime.

The goal was to provide assistance to a few promising countries which may be faced with specific drafting problems and the discussions focused on country reports, identifying common issues, updating country profiles and presenting recommendations.

Participating countries were invited to present and discuss with the facilitators from the U.S. Department of Justice, the General Secretariat of the OAS and the Council of Europe the progress made as well as difficulties encountered in adopting legislation on cybercrime in compliance with the standards of the Convention on Cybercrime[12].

The participants examined, exchanged information, and provided reciprocal assistance in improving the substantive and procedural aspects of domestic cybercrime legislation, as well

[12] In the preparation of the event some participating countries had submitted their reports assessing the national legislation and difficulties encountered in implementing the Budapest Convention

as international cooperation, taking into account what is provided in this regard in the Council of Europe Convention on Cybercrime.

Some concerns raised by countries referred to:

- Costa Rica:
  - existing legislation partially implements the Convention but amendments are considered to fully implement the Convention requirements, especially with regards to substantive law provisions.
- Ecuador:
  - there is no criminal law reform strategy
  - cybercrime is not a priority; need to include cybercrime legislation on the internal agenda
  - high tech crime police unit is not established
  - criminal provisions ensure protection for individuals but not for the state.
- Guatemala:
  - two draft laws on cybercrime that should be unified;
  - some provisions are not covered (e.g. distributing child pornography)
  - need to inform the Parliament about the Convention on Cybercrime in order to adopt legislation in compliance with implement its standards.
- Mexico:
  - legislation covers partially the provisions of the Convention
  - the challenge in implementing the Convention is that some of the offences provided by the Convention should be regulated at the federal level while others at the local level (31 Entidadas with 31 criminal codes)
- Paraguay:
  - draft law in Parliament with the purpose to fill the gaps and implement the Convention
  - interest also for training on cybercrime, in particular the CoE concept on cybercrime training for judges and prosecutors.
- Peru:
  - ongoing draft law aiming to separate the acts into different offences considering that under the existing legislation all the acts are regulated in two articles
  - interest to implement the CoE Convention
  - speed up the process in the Parliament.
- Uruguay:
  - no legislation on cybercrime in place
  - representatives (cybercrime police unit) declared that the process will be initiated and based on the discussions in the workshop a report will be presented to the relevant authorities.

As follow up, a workshop focusing on those countries that are fairly advanced in their legislative process and that are considering accession to the Budapest Convention is scheduled for August 2010 in Mexico.

2.3.13 Visit to Argentina on accession to the Budapest Convention (Buenos Aires, 16 Oct 2009)

On 16 October 2009, a Council of Europe mission visited Buenos Aires (Argentina) within the framework of the Project on Cybercrime. The visit involved meetings with the Secretary of State (Ministry of Justice, Security and Human Rights), Undersecretary of Technologias de Gestion (Cabinet of Ministers), Undersecretary Criminal Police (Ministry of Justice, Security and Human Rights) other representatives from Ministry of Justice, Security and Human

Rights including the Senior Adviser of the Undersecretary of Criminal Policy, Focal Point on cybercrime and a Round Table discussion organised by Microsoft with key people involved in the process of assessing the compliance of the Argentinean legislation with the Convention on Cybercrime (judges, CERT, lawyers, private sector).

The discussions were fruitful and the governmental officials expressed a clear interest in becoming a Party to the Convention and the need for additional cooperation with Argentina (e.g. training for judges and prosecutors).

It was underlined that:

- the legislative reforms undertaken in Argentina brought the legislation in line with the Convention on Cybercrime, in particular the amendments to the Criminal Code adopted in 2008
- the reform on procedural law continues
- the Council of Europe has already made use of the expertise provided by experts from Argentina
- Argentina could play a strong role in international efforts against cybercrime in Latin America and beyond
- Argentina could consider seeking accession to the Convention on Cybercrime
- By becoming Party to the Convention, Argentina would be a member of the Cybercrime Convention Committee (T-CY) and participate in the preparation of additional protocols and other developments related to this treaty

Follow-up:

- Argentina expressed strong interest in acceding to the Budapest Convention and by June 2010 the invitation to accede was being processed. It is expected that by the end of September Argentina will be formally invited.
- The authorities of Argentina also continued their work on supplementing the substantive law amendments adopted in 2008 with amendments to criminal procedure law.

2.3.14 Ankara Bar Association International Law Congress 2010 - Cyber Crimes Convention Workshop (Ankara, 12 Jan 2010)

The workshop was intended as follow-up of the Conference in Abant, 23/24 October 2009. About 40 participants (judges, prosecution officers, representatives of the ICT-board, government representatives) participating in the meeting with the aim to explore the possibility of signing and ratifying the Cybercrime Convention (Turkey is among the 5 CoE Member States that have not yet signed the Convention) and willing to take legislative and other actions, including launching initiatives in the private sector, as well as training for the judiciary. Statistics in 2009 showed that Turkey holds the third position on the list of countries from where malware is launched, after Serbia and Brazil.

It seems that the Turkish Criminal Law covers the substantive criminal law provisions of the Cybercrime Convention only partly (some of the provisions of paragraphs 242 ff contain minor and more serious deviations with the text of the Convention) and Turkish procedural and international criminal law are not in line with the Cybercrime Convention.

CoE presentation highlighted that there is a growth of internet users – also in Turkey – which will inevitably cause a strong growth of the number of victims and perpetrators of cybercrime. The international nature of cybercrime requires international solutions and

international co-operation. CoE could offer guidance and assistance for Turkey when implementing the Cybercrime Convention and its Protocol.

Microsoft made a presentation on internet security, the role of industry in its co-operation with governments and the 2Center Project.

Discussions suggested that cybercrime was not a priority in Turkey, that there was a lack of expertise for cybercrime investigations and that there was a limited understanding concerning the Budapest Convention on Cybercrime.

A follow-up meeting was organised by the ICT-association on 9-11 June 2010 in Izmir. The Council of Europe was requested to contribute with regard to the legislative process in preparation of implementation of the Cybercrime Convention.

2.3.15 Regional colloquium on legal challenges of ICT (Hanoi, Vietnam, 18-19 November 2009)

The regional colloquium on « es enjeux juridiques du développement des technologies de l'information et de la communication : état des lieux et perspective » was organised by the Maison du Droit Vietnamo-Francaise in Hanoi, 18-19 November 2009. In addition bilateral meetings with the Ministry of Justice were held. The objective of the participation in the meeting was to promote the Convention on Cybercrime and on the Protection of Personal data in Vietnam.

The colloquium comprised some 80 participants primarily from Vietnam (Ministries of Justice, Public Security and others, lawyers, researchers, private sector) as well as five representatives from Vietnam, four from Laos and one from Thailand.

Speakers on data protection included the Vice-President of the Commission Nationale de l'Informatique et des Libertés, CNIL and FUNDP Namur and speakers on cybercrime included the Director of the Department of Criminal and Administrative Law, Ministry of Justice, CoE, Microsoft Vietnam and the Assistant Inspector General of the Ministry of Science and Technology responsible for IPR.

Bilateral discussions and meetings were held with the Director of the Department of Criminal and Administrative Law, Ministry of Justice and other representatives from Ministry of Justice.

Discussion suggested:

- Vietnam, Laos and Cambodia had participated in a joint ASEAN-EU-Council of Europe workshop on cybercrime legislation in Kuala Lumpur in November 2008 as well as in the Octopus Conference of the Council of Europe in Strasbourg in March 2009. A country-specific workshop – planned for August 2009 as a joint event of the Ministry of Justice of Vietnam, US Department of Justice and the Council of Europe – had to be cancelled. However, the CoE provided a translation of the Convention on Cybercrime into Vietnamese language and in September 2009 an analysis of criminal legislation against the Convention on Cybercrime. The regional colloquium offered an opportunity for follow up
- In June 2009, amendments to the Criminal Code were adopted by the Parliament of Vietnam, which entered into force in January 2010: articles 224 and 225 were changed and 226 (a) and (b) added. These now help cover – at least partially –

article 2 (illegal access), 4 (data interference), 5 (system interference) and 8 needs for improvement

- In the course of 2010 the Criminal Procedure Code of Vietnam will be reformed for submission to Parliament in 2011. The procedural law provisions of the Convention on Cybercrime will be taken into account in this context. With this and further improvements of substantive law Vietnam may be in conformity with the Convention by 2011
- Participants emphasized the need to train judges and prosecutors. The training concept developed by the CoE will also be useful for Vietnam
- Furthermore, participants – in particular officials from the Ministry of Public Security pointed at problems related to international cooperation. Vietnam is currently considering the ratification of UNTOC. The value of acceding to the Convention on Cybercrime was underlined
- Interest was also expressed by representatives from Cambodia with regard to CoE assistance in the strengthening of legislation. In Cambodia as well as in Laos there is currently no legislation dealing with cybercrime. Thailand on the other hand adopted a fairly comprehensive law on cyber-related crimes in 2007
- The workshop confirmed that Vietnam is undertaking thorough reforms to establish a legal framework for cybercrime and other legislation related to ICT
- The visit was thus a cost-effective opportunity to continue the dialogue with Vietnam, to assess the current state of legislative reforms and to demonstrate the availability of the CoE to provide further assistance in view of ensuring the improvement of cybercrime legislation. With regard to data protection, the meeting primarily raised awareness to put legislation and other measures in place. A firm commitment to engage in such work was not expressed.

2.3.16 "Building Cyber security and Cyber confidence" (Ifraine, Morocco, 21-22 January 2010)

The regional Conference "Building Cyber security and Cyber confidence: Strategies, Awareness and Capacity Building was organised by the Ministry of Industry, Trade and New Technologies and Al Akhawayn University with some 150 participants, primarily from Morocco but also from Tunisia, Egypt and Malaysia as well as a number of European experts.

The Council of Europe (Project on Cybercrime) presented the conditions for criminal justice action against cybercrime in the plenary session on cyber threats:

- Legislation
- Training and specialisation
- Public-private cooperation
- International cooperation
- Safeguards.

The subsequent workshop on legal and policy capacity building clearly showed that most of the tools needed are already available (e.g. Budapest Convention, LEA-ISP guidelines, 2CENTRE concept, judicial training concepts but that a global capacity building effort was required to support countries in Africa and the near and middle east in their implementation.

2.3.17 Sixth Meeting of the REMJA Working Group (Washington D.C, 21-22 January 2010)

Representatives of national authorities and experts in the fight against cybercrime from the Member States of the OAS met at the Organisation's Headquarters, in Washington D.C. with

the objective of evaluating progress achieved and defining cooperative actions to prevent, investigate and punish crimes committed through information systems or against them.

As a result of the previous recommendations of the REMJA Working Group on Cyber-Crime in recent years, twelve regional training workshops have been held in Latin America for the development of legislation and other tools for the investigation and prosecution of these crimes; an Internet Portal has been created, which includes a component for the exchange of information between national authorities; and cooperation has been strengthened with other international organisations with activities in this area, such as the Council of Europe.

The meeting was opened by the Secretary General of the OAS, José Miguel Insulza. In his introductory remarks he referred to the challenges raised by cybercrime, the importance of cooperation between public and private sector and the new threats (e.g. child pornography, identity theft, malicious codes etc) that have to be faced by citizens. He highlighted the need for countries to bring their legislation in line with the Budapest Convention in order to enhance cooperation among states, and recognised the effort made recently by Colombia, which adopted new legislation on cybercrime. Mr. Insulza welcomed the workshops organised by the Council of Europe in the region to provide technical assistance for OAS member States.

The OAS Secretariat presented the legislative database available on the OAS website containing information on the status of implementation of the Budapest Convention by Member States.

An update on the progress made with regard to legislation and accession to the Convention was provided by each delegation. Most of the countries declared that efforts are being made to bring their national legislation in line with the Convention on Cybercrime and accession is considered:

- Argentina adopted legislation on cybercrime and organised a meeting on 10 February 2010 to discuss possible accession to the Convention (see 2.3.20) further to the CoE visit in November 2009 and the letter sent by the CoE to Argentina's authorities to consider accession
- Colombia due to the legislative progress made could now seek accession
- Chile presented the new developments stating that the legislation covers the basic standards of the Budapest Convention and accession is considered to this valuable instrument, which will provide more sophisticated tools do deal with cybercrime
- Canada deposited the Convention in the Parliament and two bills were introduced (C46 and C47) to implement the treaty. Due to the election the bills will have to be reintroduced when the Parliament resumes
- Mexico, Panama, Peru, Paraguay, Nicaragua, Ecuador, Guyana, Uruguay also presented their progress on the matter, including on bringing their legislation in line with the Convention.

The meeting adopted a set of recommendations. According to Recommendation 11 "*Recognize the consideration that certain OAS Member states have given to applying the principles of the Council of Europe's Convention on Cybercrime, acceding thereto, and adopting the legal and other measures required for its implementation, and recommend to those states that have not yet done so, to give due consideration thereto, bearing in mind the recommendations adopted by this Working Group and by the REMJAs at previous meetings. Similarly, to this end, that technical cooperation activities be continued under the auspices of the OAS General Secretariat and the Council of Europe".*

These recommendations were considered and confirmed by the Meeting of Ministers of Justice, other Ministers and Attorneys General of the Americas (REMJA), which took place on 24-26 February 2010 in Brasilia, Brazil.

2.3.18 ASEAN workshop on cybercrime legislation (Manila, Philippines, 26-28 Jan 2010)

Some 50 cybercrime and information security experts from eight ASEAN member states: Philippines, Cambodia, Indonesia, Laos, Malaysia, Singapore, Thailand and Vietnam participated in the event.

The purpose of the events was to:

- promote the adoption of the draft cybercrime law and the completion of the accession process by the Philippines to the Convention on Cybercrime (meetings with senior officials)
- strengthen cybercrime legislation in ASEAN countries (workshop for ASEAN member states in cooperation with the ASEAN Secretariat, the Philippines Commission for Information and Communication Technology and the EU-ASEAN Programme for Regional Integration).

Status of legislation/accession in participating countries:

- Cambodia: There is no relevant legislation in force, but an E-commerce act is in preparation and most provisions of the Budapest Convention have been copied into this act. The creation of a working group or commission is under consideration which would review this and other draft laws in detail. The CoE should assist this working group. The CoE should also analyse the updated country profile prepared by Cambodia during the workshop. A seminar on cybercrime was scheduled to take place in Cambodia in July 2010 with CoE support
- Indonesia: Further to legislative changes adopted in 2008 and a workshop in Strasbourg in March 2009, the Cybercrime Bill is now in the Parliament and in the priority list for 2010. With this bill, Indonesia covers almost all provisions of the Budapest Convention. The workshop recommended that Indonesia should already now seek accession to the Convention. The CoE should provide further support to the Parliament to help improve the draft law
- Laos: Similar to Cambodia, Laos is preparing an E-commerce act in which provisions of the Convention could be incorporated (approach followed by Vietnam; the present draft does not do so). It was recommended that a workshop on cybercrime should be held in Laos if possible in 2010 with the support of the CoE
- Malaysia: Following the READI/APRIS workshop in Kuala Lumpur in November 2008, a thorough review of information security legislation was undertaken by the authorities and completed in August 2009. The review contains recommendations to close legislative gaps to comply with the Budapest Convention (including specific provisions on child pornography) as well as to accede to the treaty. An updated country profile was prepared during the workshop. Given the legislation and the institutional capacities to ensure information security in place, the workshop recommended that Malaysia should already now seek accession to the Convention
- Philippines: The Philippines was invited to accede to the Budapest Convention in 2008 provided that relevant legislation has been adopted at the time of accession. The Council of Europe has been supporting legislative efforts since 2007. In the week prior to the workshop (mid-January 2010), the House of Representative adopted the cybercrime bill in its third and final reading. The Senate had the bill on its schedule for the week of 25 January 2010, but did not deal with the matter due

to political controversies unrelated to this bill. With general elections in early May, the Senate was not able to adopt the bill on time. It will thus need to be resubmitted in both, the House and the Senate again in summer 2010. In any case, the Philippines authorities are confident that the bill will be adopted in the course of 2010, and this will then be followed by accession to the Budapest Convention

- Singapore: The legislation and practice in place on the one hand suggest that they permit criminal law measures against cybercrime. On the other hand there are very few investigations and convictions. The workshop recommended that Singapore review its legislation in view of gaps identified during the workshop
- Thailand: The Cybercrime Act adopted in 2007 brought Thai legislation largely in line with the Convention. Some of the concerns identified seemed to be due to the English translation. The workshop recommended that Thailand seek accession to the Convention
- Vietnam: In July 2009, Vietnam adopted changes to the Criminal Code which added some provisions on cybercrime. However, a considerable number of measures will need to be added in the course of the reform of the criminal and criminal procedure codes in 2010/2011. In addition to the criminal law, two decrees (no 90 on Spam and 097 on service providers and illegal use of internet services) and the electronic transaction law of 2007 are relevant.

Overall, good progress was made since November 2008. Substantive law is well covered (although apart from the Philippines countries rely on general pornography provisions rather than specific articles for children), while procedural laws are less complete (most countries rely on data retention); specific elements on search and seizure are missing, including limitations, safeguards and conditions). A more detailed discussion would be necessary to review the functioning of provisions in practice.

In addition to the Philippines, Indonesia, Malaysia and Thailand could be invited to accede, while in parallel further support should be provided to improve legislation.

With regard to law enforcement/Internet service provider cooperation all countries pledged to initiate work on the matter based on the CoE guidelines adopted in 2008. Indonesia will establish a working group, while Malaysia will hold meetings to streamline cooperation which is already well functioning.

With regard to the training of judges and prosecutors, none of the countries – with the exception of Cambodia – foresee specific initial training for judges but provide for in-service training. It would seem that Malaysia is the only country with a specific centre for continued training for judges and prosecutors. The workshop recommended that the Malaysian centre could become a pilot centre along the lines suggested by the CoE training concept (the CoE was asked to present the concept to this centre). Countries were also interested in the 2CENTRE initiative for law enforcement training and it was recommended that at least one such centre should be established in the ASEAN region. On the suggestion of the Philippines, the workshop recommended that the issue of training (1. For judges and prosecutors using the CoE concept, 2. For law enforcement using the 2CENTRE approach and 3. On international cooperation for Prosecutors General Offices and Ministries of Justice on the basis the Budapest Convention) be taken up at a formal level by ASEAN. After the closure of the workshop, a "concept" was prepared for submission to the ASEAN TELSOM/TELMIN joint group in Brunei in February 2010 and subsequent consideration by TELSOM Ministers. Ministerial support is considered necessary to ensure implementation.

With respect to all matters, the eight ASEAN countries participating in this event are prepared to extend their cooperation with the CoE in cybercrime matters. Funds should be mobilised to follow up, possibly in cooperation with the European Union.

An ASEAN-wide judicial training workshop is scheduled to be held in Malaysia in October 2010.

2.3.19 First AfriNIC - Government Working Group and LEA Meeting (Mauritius, 25–26 Jan 2010)

The first AfriNIC - Government Working Group (AfGWG) and Law Enforcement Meeting of the African Network Information Center (AfriNIC) and Regional Internet Registry (RIR) for Africa was held in Ebene, Mauritius on 25–26 January 2010. The objectives of the meeting were to provide for the participants the opportunity to learn about the current challenges of Internet-related crimes, the steps being taken by law enforcement agencies to face such challenges and exchange ideas about the creation of an Internet Law Enforcement Working Group to promote security by facilitating global cooperation and coordination.

Representatives of Mauritius public institutions (e.g. Attorney General, Police Department, CERT), Department of Justice of the US, ARIN, RIPE NCC, CoE and some African countries (Benin, Kenya, Nigeria, Seychelles and Malawi), mainly from public institutions (law enforcement agencies) and regulators participated in the event.

The CoE speaker presented the Budapest Convention as an opportunity for countries of Africa and presented the guidelines for the cooperation between law enforcement and internet service providers against cybercrime.

The establishment of Law Enforcement Agencies and Regional Internet Registries joint working groups was discussed as a solution to enhance law enforcement capabilities and control the criminal misuse of IP addresses and domains.

The meeting confirmed once more the interest of African countries to take measures against cybercrime and the need for capacity building.

2.3.20 Meeting on Convention on Cybercrime (Buenos Aires, Argentina, 10 February 2010)

Further to the previous CoE visit in Buenos Aires in November 2009, the relevant authorities organised a meeting with the key stakeholders involved in the process of assessing the compliance of the cybercrime legislation of Argentina with the Convention on Cybercrime. Representatives of national authorities (e.g. Ministry of Justice, Security and Human Rights, Public Ministry, Ministry of Foreign Affairs) experts in the fight against cybercrime, judges, prosecutors, European Union Delegation and other stakeholders participated in the event.

Three experts on substantive law, procedural law and international cooperation on cybercrime presented the report analysing to what extent the domestic legislation of Argentina covers the provisions of the Convention. The presentations concluded that:

- substantive law part is mainly covered by the new legislation adopted and making use of some reservations allowed by the treaty Argentina will fully comply with the requirements of the Convention
- existent procedural law provisions should be amended

- international cooperation provisions under Convention would also require the implementation of the procedural law measures both at the national and international level
- although more legislative and institutional measures are required to better deal with cybercrime and fully comply with the Convention there is no impediment to request accession and in parallel to continue the legislative reform.

Following a presentation by the CoE representative, most of the speakers expressed a clear interest in becoming Party to the Convention and cooperating with the Council of Europe.

Argentina subsequently participated in the Octopus conference (March 2010) with a strong delegation and formally stated its interest in becoming a party to the Budapest Convention.

2.3.21 MENA Cybercrime Legislation Workshop (Malta, 16-18 Feb 2010)

The regional workshop for North Africa and the Middle East was organized by the US Department of Justice with the participation of the Council of Europe. The purpose of the meeting was to raise awareness on the importance of the cybercrime legislation and prepare legislative profiles using the text of the Cybercrime Convention as a basis and guidance.

Law enforcement representatives, prosecutors, judges and representatives responsible for national criminal policy participated in the event.

During the meeting the delegations updated their legislative profiles and make recommendations. With regard to specific countries:

- Tunisia: recognizes ICT and ICT-related as a strategic topic. Already a number of laws on the subject have been enacted, from e-commerce to IT-security. Since 1999 a Cybercrime Law is in force. At the national level training for LEA has been undertaken, forensic labs have been established. Tunisia assisted South-Africa in a project on IT-security. The delegation will apply the Cybercrime Convention as a test medium for its domestic law. Most of it - substantive criminal law - has already been implemented. In the field of Criminal Procedural Law there seem to be no problems. MLA requires attention and possibly amending of present law. Tunisia is working with the European Union on certain projects
- Egypt: there are laws in force concerning ICT, like e-signature, intellectual property, consumer protection, etc. Those laws may contain criminal law provisions, but there may be a review those provisions and put them together, in order to enhance consistency, relate them to criminal sanctions and in order to make them object of investigation under the powers of the Criminal Procedural Code. The Cybercrime Convention (article 22) offers inspiration for establishment of extraterritorial jurisdiction. Egypt avails over a MLA-agreement with US, Italy and France that encompasses the MLA-regulation of the Cybercrime Convention. Egypt does not have a 24/7 contact point, which is considered necessary after the exchange of views at the meeting. It was stressed that it takes a long time before letters rogatory are executed by the US. A recent amendment law might remove a number of impediments in internal US procedures
- Morocco will support the Cybercrime Convention which they consider to be a very useful instrument. Internally they will recommend reviewing domestic law. In a number of areas there is law, but it can and should be improved. Morocco might seek accession to the Convention. Domestic law will be reviewed on the basis of the Cybercrime Convention but also in view of other Arab legislation. Quite a number of ICT-related laws have been implemented in the Morocco Code. The last

is the Data Protection Act of 2009. The Cybercrime Law is mainly copied from the French Code Penal. From the discussions it became apparent that domestic law contains some minor gaps that will be reported to the responsible authorities. Morocco further invests in other means to fight cybercrime including keeping statistics and judicial training. Morocco as well as Tunisia maintain a comprehensive approach concerning e-activities

- Jordan has no specific Cybercrime Law in place. A specific article in its Code of 1960 today expands the scope of traditional crimes to cases where the crime is committed by electronic means. Internally, a draft Project on Cybercrime has been launched, but it not public. Criminal Procedural Law is very wide-ranging and may include most provisions of the Cybercrime Convention. An analysis will be undertaken if amendments are desirable
- Lebanon is interested in ICT-related legislation. Unfortunately, the civil war and the impossibility to form powerful and active governments caused postponement and serious delay, but there is political willingness to retake legislative action. The banking sector is important in Lebanon which is a strong impetus for the legislator to provide for adequate legal protection for these institutions as well as its customers. Lebanon copied many elements of its e-laws from other countries. A squad of specialized police officers regularly succeeds in solving cybercrime cases. Lebanon considers itself as a reliable Party in international co-operation and has entered into a number of multilateral and bilateral co-operation agreements
- Malta adopted a Computer Misuse Act drafted along the lines of the U.K. Computer Misuse Act. An amendment Bill is pending in order to bring Malta's law in accordance with the Cybercrime Convention, enabling Malta to ratify it. There is a small team of 5 police officers that deals with cyber crime cases. Malta expects to receive more MLA-requests in the future, since it promotes itself as a financial hub and place of settlement for (on-line) casinos. Malta is a member of the G8 24/7 network. Malta's Parliament is at present discussing an Amendment Bill that would allow Malta to ratify the Convention. Ratification therefore can be expected within a few months.

The CoE representative highlighted the urgency of adopting cybercrime legislation, arguments for Arab countries to join the Budapest Convention on Cybercrime and also the need for financial support for developing countries in order to be able to deal with cybercrime.

The meeting was highly appreciated and served as a platform for exchange of experiences and views between participants and increased the interest in the Cybercrime Convention and relating Council of Europe work.

2.3.22 Pacific Island Countries (advisory paper, June 2010)

In view of the Pacific Regional Information and Communication Technology Officials meeting (Nuku'alofa, Tonga, 16-17 June 2010) and particular in view of agenda item 3 on ICT policy, legislation and regulatory frameworks, the Project on Cybercrime prepared an advisory paper containing suggestions for the strengthening of cybercrime legislation in the Pacific region.[13] This followed earlier contacts and cooperation with representatives of the Secretariat of the Pacific Community (SPC).

The key suggestion of the paper is to carry out a detailed analysis of legislation in force or planned using the Budapest Convention as a benchmark and taking into account the experience of other countries. A regional workshop on cybercrime legislation with experts

[13] Available at http://www.spc.int/edd/en/meeting-agenda

from Pacific countries responsible for legislation may help identify strengths and weaknesses and result in proposals for specific solutions.

At the meeting, ICT Ministers adopted recommendations, through which, among other things, they:

> (iii) Direct their Officials to work with SPC, the Council of Europe, ITU and development partners on developing appropriate policy, legislative and regulatory frameworks and strategies to combat cyber crime and promote Internet safety and security, including child online protection.

2.3.23 International Informatics Law Assembly (Izmir, Turkey, 9-11 June 2010)

This biennial meeting was organised by the Turkish Informatics Association and supported by a large group of companies, amongst them Microsoft. It was a follow-up to the workshop organised by the Ankara Bar Association International Law Congress in Ankara on 12 January 2010.

The discussions focused on credit card fraud, financial fraud and the existing legal framework in Turkey. The representative of the Council of Europe contributed to the panel on the fight against cybercrime. A number of interventions were related to the Budapest Convention on Cybercrime as a solution, and the need for Turkey to become a party.

During and after the event the Turkish authorities announced the intention of Turkey to sign the Budapest Convention on Cybercrime within a few weeks.

2.3.24 Commonwealth workshop "Legal Frameworks for ICTs" (9 June 2010, Malta)

The Council of Europe through the Project contributed to this event organised by the Comnet Foundation for ICT Development and sponsored by the Commonwealth Fund for Technical Cooperation, Commonwealth Secretariat, UK and the Ministry of Foreign Affairs of Malta.

A total of 15 delegates from Commonwealth Countries located in the Caribbean, Africa and Asia attended the event. More than 300 cybercrime experts representing countries from all continents, international organisations and the private sector attended the conference to enhance their cooperation against cybercrime.

The discussions covered an introduction to the topics and case studies, internet governance and electronic communications regulations, cyber crime and intellectual property, data protection and information law, e-government and e-commerce's.

The Council of Europe contributed to the cybercrime and intellectual property session covering the following points:

- What is cybercrime: definition of cybercrime with a discussion on offences against the confidentiality, integrity and availability of computer data and systems; computer related offences; content related offences; and offences related to intellectual property rights and similar rights
- How does it affect us: examples how we are all now affected by cybercrime; cyber terrorism; homicide; fraud; money laundering; blackmail and sex tourism etc
- The solution: the Budapest Convention
- The aims of the Budapest Convention: the need to internationally harmonise domestic criminal laws and cooperate in the fight against cyber crime

- Other activities of the Council of Europe (e.g. annual Octopus Conference and some results in 2010; Global Project on Cybercrime and how the Council of Europe can assist)
- Need for training for law enforcement, prosecutors and judges
- Five reasons to become a partner.

Child protection and cyber crime have been identified as key prioritises for the Commonwealth. The Council of Europe's resource base and expertise would be highly valued in building up policy and legislative capacity in commonwealth countries, especially regarding the incorporation of the principles of the Budapest Convention into their laws.

Follow up:

- Further dialogue with a number of delegates from: Brunei Darussalam, Samoa, Sri Lanka, Tanzania, Trinidad and Tobago, Sri Lanka, Tanzania interested in working with the Council of Europe especially regarding how to incorporate the principles of the Cybercrime Convention into their laws
- Consider joining the Steering Committee of the Commonwealth Internet Governance Forum (CIGF)
- Possible dialog with the Malta Communications Authority (MCA), which is interested in the Council of Europe work on cloud computing.

2.4 Activities related to 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

Indicators:

- Directory of contact points updated on a regular basis in cooperation with the G8 High-tech Crime Subgroup
- Increase in the number of urgent requests sent and received by contact points
- Advice provided to 24/7 points of contact and high-tech crime units
- Cooperation manual on mutual legal assistance in cybercrime matters available

Summary of progress towards the expected result:

- The study and workshop helped clarify the role and limitations of 24/7 points of contact and encouraged the more recently created contact points in Europe to become more active
- Measures to render contact points more effective were identified.

While cooperation between the G8 High-tech Crime Subgroup and the CoE will require further discussion by the Cybercrime Convention Committee, the Project on Cybercrime should focus not only on contact points but also on other channels of cooperation (in particular Interpol) and on making mutual legal assistance more efficient.

The following activities contributed to the progress made:

2.4.1 Global – Study and Octopus workshop on 24/7 points of contact (Strasbourg, March 2009)

A study on the functioning of 24/7 points of contact that had been in preparation since September 2008 was finalised in March 2009 and discussed at the Octopus Interface conference on 11 March 2009 and at the Cybercrime Convention Committee on 12/13 March 2009. It was published at www.coe.int/cybercrime in August 2009 together with other resources regarding international cooperation against cybercrime.

The study was based on information received primarily from contact points established in countries that are parties to the Convention on Cybercrime and that have established contact points in line with article 35 of the Convention, that is, European contact points and the USA.

The overall conclusion is that in countries with active contact points the network is considered effective as a channel for particularly urgent requests for expedited preservation (articles 29 and 30 of the Convention). While in some countries the network is used frequently, a number of contact points have been rather inactive and some have yet to send or receive a request.

As the network is to be used for urgent cases only, for the vast majority of requests that are considered less urgent other channels are used. These include Interpol and the system of National Central Reference Points for e-crime that facilitates cooperation between more than 120 national cybercrime units.

The study and workshop discussions showed that the involvement of contact points in mutual legal assistance requests is limited, and they are reluctant to assume responsibility for expediting mutual legal assistance foreseen under article 31 of the Convention on Cybercrime (MLA regarding accessing of stored computer data).

Conclusions include that for the network to become more effective:

- contact points need to become more pro-active and in particular make themselves known
- contact points may need to take on more responsibility to facilitate MLA
- national regulations to facilitate preservations measures need to be put in place
- more countries to become party to the Convention on Cybercrime.

2.4.2 Global – Meeting with Interpol (Lyon, 9 September 2009)

The CoE and Interpol have been cooperating with each other for several years, and Interpol has been promoting the Convention on Cybercrime on many occasions. Given the fact that Interpol's system of National Central Reference Points for e-crime is capable of facilitating the application of international cooperation provisions of the Convention on Cybercrime, the CoE through the Project on Cybercrime and Interpol should enhance their interaction.

2.5 Activities related to 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

Indicators:

- Cooperation agreements concluded between law enforcement and ISPs in at least 5 countries in line with the guidelines developed during the first phase
- At least 10 events organised to promote LEA-ISP cooperation
- Further proposals for public-private cooperation developed

Summary of progress towards this expected result:

- The LEA-ISP guidelines adopted at the Octopus conference in 2008 are yielding an impact in several countries and at the level of the European Union
- The guidelines are now available in many languages (English, French, Arabic, Georgian, Portuguese, Romanian, Russian, Spanish, Ukrainian)
- The Project on Cybercrime helped create a working group in Ukraine to improve LEA-ISP cooperation
- LEA-ISP cooperation was also promoted in India
- The Governmental Advisory Committee of ICANN endorsed law enforcement proposals to ensure due diligence and prevent criminal misuse of domains that have also been supported by the Project on Cybercrime.

In addition to activities carried out under the Global Project on Cybercrime the joint European Union/Council of Europe Project on Cybercrime in Georgia contributed to a memorandum of understanding between law enforcement and service providers in Georgia in May 2010, which is based on the principles of the guidelines.

The following activities contributed to the progress made:

2.5.1 Global – Update on LEA-ISP cooperation at Octopus conference (March 2009)

The Octopus conference included a session on 10 March 2009 with an update regarding the guidelines on cooperation between law enforcement – internet service providers in the investigation of cybercrime that had been adopted at the previous Octopus conference in April 2008.

Presentations showed that practical use had been made of the guidelines by public authorities and/or ISPs in several countries (such as France and Romania) and that they helped launch the discussion on such cooperation in others. They were also used by the European Commission and are reflected in a resolution of the European Union's Justice and Home Affairs Council in November 2008 which recommended that the European Commission work on the basis of the guidelines adopted by the Council of Europe conference and took note of eight specific recommendations.

2.5.2 India – Workshop on international and LEA – ISP cooperation (New Delhi, 26 March 2009)

On 5 February 2009, the President of India signed the amendments to the Information Technology Act that had been adopted by the Parliament in December 2008 (ITA-A 2008). As a result Indian legislation is now largely in line with the Convention on Cybercrime.

The amendments reflect most of the comments made by the CoE in 2007 and the adoption had been accelerated by the Mumbai attacks in November 2008 which had relied heavily on information technologies (VoIP).

On 26 March 2009, a joint conference of the Council of Europe and the Indian Central Bureau of Investigations (CBI) on International Cooperation against Cybercrime was organised in New Delhi. The aim was to promote law enforcement – service provider cooperation as well as accession by India to the Convention on Cybercrime

Over 160 senior police officers from all over India, representatives of the private sector (IT industry) and high official of India Government participated in the event. Interpol was represented by a speaker. The meeting was opened by K.M. Chandrasekha, Cabinet Secretary of the Prime Minister of India, and closed by Jainder Singh, Secretary of the Ministry for Information and Communication Technology. Both underlined that India should consider accession to the Convention on Cybercrime in order to facilitate efficient international cooperation.

The conference emphasised the need for public-private cooperation, in particular law enforcement – service provider cooperation. The guidelines of the CoE Project on Cybercrime were considered useful since the adoption of the ITA-A 2008 will be followed by the preparation of secondary implementing regulations which raises concerns by the private sector.

A senior representative of the largest telecom provider in India, AIRTEL, showed how this provider had already implemented most of the CoE guidelines.

Several speakers underlined the need for data protection and privacy regulations. The ITA-A 2008 contains references to privacy which may provide an opening to the development of a more comprehensive approach to data protection in the future.

The event was of high visibility and well covered by the media.

2.5.3 Ukraine – Workshop on law enforcement – ISP cooperation (Kyiv, Ukraine, 29 April 2009)

On 29 April 2009, a workshop was organised in Kyiv to strengthen cooperation between law enforcement agencies and Internet service providers in the investigation of cybercrime in Ukraine. The guidelines on LEA-ISP cooperation of the CoE were translated into Ukrainian and Russian for this purpose.

Ukraine had ratified the Convention on Cybercrime in 2006, but so far has not fully implemented the procedural law provisions. Under the current Criminal Procedure Code law enforcement and ISPs are faced with a dilemma: according to Article 66, ISPs would have to provide any information requested by law enforcement but only once a formal investigation is opened. A judge will only approve the opening of an investigation if sufficient evidence is provided by law enforcement. Thus, law enforcement tends to request information from ISPs

without legally valid grounds, which means that ISPs risk to violate privacy laws or to have their servers confiscated as an urgent measure to preserve evidence.

The new draft Criminal Procedure Code would change the overall system although this draft does yet not contain cybercrime-specific provisions. The CoE is now supporting the finalisation and adoption of the CPC by the Government and Parliament of Ukraine. An analysis of the draft CPC was initiated by the CoE in August 2009.

Nevertheless, there is room to improve already now cooperation on the basis of the LEA-ISP guidelines adopted in Strasbourg in April 2009.

Discussions during the workshop resulted in the agreement to establish a working group by the Ukrainian Internet Association with the participation of the Ministry of Interior (State Service on Combating Economic Crime) and the State Security Service.

The working group held first meeting in July 2009 where it identified its objectives as follows:

- to develop efficient tools for strengthening of cooperation between law enforcement agencies and communication market actors in fighting against cybercrime
- to elaborate an approach for implementation of the 'guidelines for law enforcement - service provider cooperation in the investigation of cybercrime'
- to develop proposals for improvement of the cybercrime legal framework in Ukraine.

It was agreed that child pornography, terrorism and national/racial intolerance (extremism) are the priority targets to be fought.

The Action plan of the WG for the period of July - September 2009 includes:

- to elaborate methods for informing different target groups about jeopardy caused by cybercrime taking into account that viruses and botnets are the most dangerous elements
- to elaborate and sign a memo on cooperation against cybercrime
- to provide WG member with documents on interaction between providers and clients (agreement/Internet operation manual)
- to provide WG members with an updated version of the draft law no 1340
- to elaborate a memorandum on informing of law enforcement bodies about cybercrime cases by Internet providers.

A further point discussed during the April workshop was the establishment of a 24/7 point of contact in line with Article 35 of the Convention on Cybercrime.

2.5.4 Global – MAAWG conference (Amsterdam, Netherlands, 8-10 June 2009)

The Messaging Anti-Abuse Working Group (MAAWG) is a global organisation focusing on preserving electronic messaging from online exploits and abuse with the goal of enhancing user trust and confidence, while ensuring the deliverability of legitimate messages. Its members cover a broad base of Internet Service Providers (ISPs) and network operators representing almost one billion mailboxes, key technology providers and senders. MAAWG works to address messaging abuse by focusing on technology, industry collaboration and public policy initiatives.

At the MAAWG conference (8-10 June 2009, Amsterdam) the CoE was invited to participate in the workshop on 'Cross-Border Enforcement (Public Policy Committee) - Establishing foundations for effective cross-border enforcement mechanisms' in order to present its work regarding the harmonisation of legislation, including procedural rules and establishing a framework for cooperation between law enforcement and industry.

An ISPs meeting was also held within the conference launching the proposal for a 'social network' between ISPs and LEA open initially for MAAAGW members in order to share information on fighting cybercrime of which content will be discussed later on. The network should facilitate the initial contact with ISPs and prioritise the requests that are urgent by establishing contact points among ISP and LEA.

Undoubtedly, there is a need to strengthen the cooperation between LEA-ISP and establish the way to link up with each other in a pragmatic manner (through a contact list or similar). The advantage of involving MAAWG in such initiative would be its broad membership.

2.5.5 Public-private sector dialogue on tackling online illegal activities (Brussels, 27 Nov 2009)

The Conference was organised by the European Commission with the aim of setting up an informal platform for dialogue where different issues and topics related to the fight against online illegal activities could be discussed among private and public stakeholders as well as NGO-operated complaint hotlines.

The creation of such platform for dialogue builds upon the Council Conclusions of 27 November 2008 on a concerted work strategy and practical measures against cyber-crime, which invites Member States and the Commission, in particular, to draft, in consultation with private operators, a European agreement model for co-operation between law enforcement agencies and private operators.

Participants: Representatives of the private sector, including European associations of telecom operators, internet service providers and mobile phones operators – ETNO, EuroISPA, GSMA - as well as companies such as Microsoft and e-Bay, NGOs coordinating the action of complaint hotlines in Europe – INHOPE and INACH, national authorities from France, Germany, Ireland, Portugal, Romania, Spain, Sweden, The Netherlands, United Kingdom, EU Counter Terrorism Coordinator, EU Council Secretariat, Council of Europe, Europol and Interpol and Commission.

The EU Counter Terrorism Coordinator stressed the importance of online criminal activities as a growing problem and gave an overview of what had been done so far to prevent criminal activities online, especially in the field of counter-terrorism, including the amendment of the Framework Decision on combating terrorism as well as to the project Check the Web. He advocated the need to take tough action on the web to prevent illegal activities and differentiated between negative actions, including notice and take down, de-registration and filtering, and positive actions, in particular the empowerment of the users and the promotion of media literacy.

A number of examples of effective self-regulation on the Internet based on public-private partnerships were presented (the Netherlands project "Exploring the Islamist Extremist Web of Europe", INHOPE, Interpol, INACH) as well as examples of standard business conditions concerning illicit content, and of non-legislative measures to tackle terrorist related content. The law enforcement – ISP cooperation guidelines developed by the Council of Europe were also mentioned.

There was general agreement that the public-private dialogue on tackling illegal activities on the Internet needs to be continued.

2.5.6 Octopus workshop on mapping networks and initiatives (Strasbourg, 24 March 2010)

The Octopus workshop on networks and initiatives discussed on how public-private cooperation could be further strengthened and recommended a contact list for industry and law enforcement. Further to an agreement between US Department of Justice and European Commission, the European Commission is proposing a secure portal to interested parties.

2.5.7 Octopus workshop on law enforcement responsibilities (Strasbourg, 23 March 2010)

Participants identified the following challenges:

- Regulators, law enforcement agencies (LEAs) and Computer Emergency Response Teams (CERTs)/Computer Security Incident Response Teams (CSIRTs) play an important part in preventing and dealing with cyber security incidents and cyber crime. Lack or insufficient cooperation between any of these elements risks inappropriate policy responses, and prevents the control and investigation of cyber-incidents.
- Internet resources, such as domain names are managed/coordinated respectively by the Internet Corporation for Assigned Names and Numbers (ICANN) and Regional Internet Registries (RIRs) and their registrars (e.g. Internet Service Providers). To obtain these resources, a registrant has to provide certain personal information to the WHOIS database. According to a recent report for ICANN, less than half of records were fully accurate (only 23% when using strict definition of accuracy).[14] Inaccuracies are also found in WHOIS of RIRs. This is of deep concern to LEAs, as it hampers their efforts to track those who use CIRs for criminal activities. Current inaccuracies are to a large extent the result of insufficient control and vetting procedures and due diligence. The arrival of IPv6 is likely to aggravate further this situation, as large amounts of IP addresses will be distributed under the current registration procedures.

Good practices and opportunities include:

- Cyber crime units (central/regional) develop public-private cooperation and international cooperation, create instruments and procedures for investigations, and develop reporting systems.
- Public/private reporting systems crosscheck alerts at international level (European alert platform).
- LEAs and CERTs/CSIRTs and regulators play an active role in awareness raising about cyber security/crime, reporting possibilities and assistance to victims.
- Informal/trusted cooperation between LEAs and CERTs/CSIRTs.
- Contact point networks facilitate cooperation.
- The interest expressed by civil authorities to establish stronger cooperation with law enforcement, in particular with regard to training is a very positive development.
- LE concerns raised in dedicated working groups in ICANN (Government Advisory Council) and RIRs.

[14] 'Draft Report for the Study of the Accuracy of WHOIS Registrant Contact Information', Developed by NORC at the University of Chicago for ICANN 17 January 2010, p 2.

- Draft "Law Enforcement Recommended Amendments to ICANN's Registrar Accreditation Agreement (RAA) and Due Diligence Recommendations" are available and had been proposed to the Internet Corporation of Assigned Names and Numbers (ICANN) at the ICANN Seoul Meeting in October, 2009. The principle aim of these proposals is to promote a safe and secure Internet minimizing criminal activity on the Internet and preventing domain name abuse by:
  - Enacting enhanced due diligence procedures for ICANN's accreditation of Registrars and Registries, and Registrar's processing domain name registrations;
  - Accurate WHOIS information and availability for Law Enforcement;
  - Transparency and accountability concerning registrars, registries, domain name resellers and third party beneficiaries.

In terms of follow up the following was recommended:

- Establish cybercrime units, CERTs/CSIRTs and cyber incidents/crime reporting systems. Develop cooperation procedures among the stakeholders and the private sector (ISPs).
- Pending the full implementation of IPv6, preventive measures could already be implemented.
- Stronger due diligence policies and measures by ICANN, registrars and registries and accurate WHOIS information with applicable data protection safeguards is recommended and the "Law Enforcement Recommended Amendments to ICANN's Registrar Accreditation Agreement (RAA) and Due Diligence Recommendations" should be endorsed. ICANN is encouraged to implement these recommendations without delay.

The Governmental Advisory Committee (GAC) of the Internet Corporation for Assigned Names and Numbers (ICANN) met in Brussels, during June 19 - 23, 2010, and with regard to the "Law enforcement Due Diligence Recommendations" stated the following in its Communiqué dated 23 June 2010:

> "Absolute majority of countries made the following statement:
>
> The GAC encourages the Board, the RAA Working Group and registrars to work with law enforcement agencies to address their concerns and implement necessary changes without delay.
>
> Following from the GAC's Nairobi Communiqué, the GAC requests an update of progress on consideration of these proposals, including the Board's consideration of the due diligence recommendations.
>
> Based on the deliberations in Brussels and the previous meetings, the GAC endorses the proposals from law enforcement agencies to address criminal misuse of the DNS, noting that implementation of these proposals must respect applicable law and respect all requirements concerning the processing of personal data, such as privacy, accuracy and relevance.
>
> Some countries felt that the further efforts need to be deployed to clarify these proposals."

2.6 Activities related to 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

Indicators:

- Typology study on money flows and financial investigations adopted and disseminated among MONEYVAL, FATF and Euro-Asia Group members
- Up to 2 international workshops carried out
- Recommendations on financial investigations on the internet available
- Recommendations available on multi-stakeholder action against criminal money on the internet

Summary of progress towards this expected result:

- 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. The MONEYVAL plenary confirmed this study in September 2009. A project team led by the Russian Federation was established and by June 2010 agreement had been reached on the structure of the report, replies to a questionnaire had been received and tasks had been distributed. The study is thus well on track.

  The study will help create bridges between anti-money laundering and anti-cybercrime worlds and may have important impact around the world.

The following activities contributed to progress made:

2.6.1 Global – Workshop on criminal money on the internet at Octopus conference (March 2009)

The Octopus conference included a specific workshop on criminal money flows on the internet. The workshop helped share experience, good practices and opportunities for cooperation in terms of (a) typologies of proceeds generating crime, money flows and money laundering, (b) strategies, techniques and tools to search, follow, seize and confiscate such proceeds, and (c) opportunities for multi-stakeholder action to follow criminal money and prevent cyber-fraud and cyber-laundering. The conference pointed at the need to establish trust between different public and private sector stakeholders involved in anti-cybercrime and anti-money laundering and terrorist financing measures, and to build bridges between the anti-cybercrime and anti-money laundering communities, between law enforcement, internet industry, financial services and others. Examples discussed included the Financial Action Task Force, MONEYVAL[15], the Anti-Phishing Working Group, the London Action Plan, the Advance Fee Fraud coalition or the Hi-tech Crime Forum in Ireland. Countries should also make sure that different types of cybercrime are predicate offences for money laundering.

[15] MONEYVAL is the Council of Europe's anti-money laundering monitoring body. It is an "FATF-style Regional Body" and covers the 27 European countries that are not members of the Financial Action Task Force. The FATF and MONEYVAL closely cooperate with each other.

The Octopus Conference recommended that in order to ensure broadest possible impact and cooperation between anti-money laundering and anti-cybercrime mechanisms, the mapping of criminal money flows foreseen under the Project on Cybercrime should be carried out in the form of a typology exercise in cooperation with MONEYVAL.

2.6.2 Global – Initiation a typology study on "criminal money flows" (Strasbourg, Sep 2009)

In cooperation with MONEYVAL a proposal for the preparation of a "typology project" was drafted on "Criminal money flows on the internet: methods, trends and multi-stakeholder counteraction" in August 2009, and subsequently adopted by the MONEYVAL plenary on 24 September 2009.

The objective of the typology project will be to examine methods, trends and typologies and to develop indicators to identify criminal money flows and money laundering on the internet, and recommendations for multi-stakeholder action aimed at preventive measures, the seizure and confiscation of criminal money and the investigation of money laundering and terrorist financing on the internet.

The study is to be prepared in view of the typology meeting of MONEYVAL and the EURO-ASIA Group in October 2010 in which the Financial Action Task Force will also participate. This will then ensure global dissemination of the study.

The final version of the study could then be adopted by MONEYVAL in December 2010.

2.6.3 Working meeting on the typology study on money flows (Strasbourg, 26 Mar 2010)

The first meeting of the project team was held in March 2010 where agreement was reached on the structure of the study. Tasks were subsequently assigned to different members of the team.

The next meeting is scheduled to be held in October 2010 in Moscow.

2.7 Activities related to Result 5 (training)

Expected Result 5: Judges and prosecutors: Training for judges and prosecutors in cybercrime and electronic evidence institutionalised Indicators: ▪ Training concept for judges and prosecutors adopted and widely disseminated ▪ Model training manual and workshop for judges and prosecutors available and tested in up to seven training events. ▪ Up to 150 judges and prosecutors trained ▪ Training manual disseminated

Summary of progress towards this expected result:

- Between March and September 2009 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. This is a major achievement and may yield considerable impact
- Judges and prosecutors trained through workshops in Albania, Egypt, Germany, Pakistan, Portugal and Romania.[16]

The following activities supported by the Project on Cybercrime contributed to this expected result:

2.7.1 Global – Octopus workshop on training (Strasbourg, 10-11 March 2009)

The conference showed what training on cybercrime is on offer for law enforcement, prosecutors and judges. The conference in particular saw the launch of the "2centre", a joint action of law enforcement and industry for cybercrime training. With regard to prosecutors and judges proposals have been discussed to further improve training materials and institutionalise judicial training. The Lisbon Network of the Council of Europe and the Global E-Crime Prosecutors Network (GPEN) offer opportunities in this respect. CYBEX has developed a model training course for judges. Common issues are the question of certification of training and trainees, the different levels of knowledge required by different people and the sustainability and replicability of training.

Follow up:

- Ad hoc training should be replaced by more systematic and coherent training for judges, prosecutors and law enforcement
- Implementation of the 2centre initiative should be supported

[16] Note: The terms of reference of the Project as agreed refer to the preparation of a model training manual and the actual training of judges and prosecutors. However, following the Octopus conference it was decided to pursue a more ambitious approach by developing a concept for institutionalising cybercrime training. For this reason this result and indicators have been reformulated.

- With regard to judges and prosecutors, the project rather than supporting ad hoc training events should develop a coherent concept aimed at institutionalizing training on cybercrime and electronic evidence.

2.7.2 Portugal – Training workshop for judges and prosecutors (Lisbon, 20 March 2009)

On 20 March 2009, the Project supported a training seminar on cybercrime held at the Centro de Estudos Judiciários (Center for Judiciary Studies) in Portugal for over 215 judges, prosecutors and lawyers.

The event improved knowledge of judges and prosecutors in matters related to cybercrime and raised awareness of the challenges that cybercrime poses for them.

According to the synopsis of the evaluation questionnaires (distributed to the participants by CEJ), 68% participants responded that the seminar improved their level of knowledge and professional capacity markedly and 27% very much.

In June, the law on the ratification of the Convention on Cybercrime and the Protocol was adopted by the Parliament of Portugal. In March 2010, Portugal ratified the Convention. This will further enhance the capacities of judges and prosecutors in Portugal to deal with cybercrime and electronic evidence and to cooperate internationally.

The event showed that the Center for Judiciary Studies could exercise a leading role in institutionalising the training of judges and prosecutors in cybercrime and electronic evidence.

2.7.3 Albania – Workshop for prosecutors (Duress, Albania, 16-17 April 2009)

Albania ratified the Convention on Cybercrime in 2002 without fully implementing its provisions into national legislation. In December 2008, the Parliament of Albania adopted amendments to the Criminal and Criminal Procedure codes to close these gaps. The authorities subsequently requested the PROSECO project and the Project on Cybercrime to provide training to Albanian prosecutors in view of applying this legislation in practice.

On 16-17 April 2009, a workshop was organised in Duress with the objective of promoting the application of Albania legislation in the prosecution and international cooperation against cybercrime. A private sector speaker from Microsoft also participated in this event.

The training focused on current challenges related to cybercrime and electronic evidence and the particular problems for prosecutors. The new legislative provisions were presented and discussed in detail. Discussions and feedback received indicated a strong interest by some and a reasonable interest by other prosecutors in this matter. As a result it can be expected that all participants are now familiar with these provisions and that some prosecutors are likely to get further involved and acquire additional knowledge.

Prosecutors are aware of the fact that they need to cooperate with the private sector, in particular internet service providers.

2.7.4 Germany – Contribution to ERA workshop on cybercrime (Trier, Germany, 14-15 May 2009)

On 14-15 May 2009, ERA organised the Conference on *"Criminal exploitation of new technologies. An effective response to cybercrime."* Under the topic on the legal framework

on cybercrime in Europe it was presented the progress made within the Project on cybercrime (Phase 1) in implementing the Convention on Cybercrime all over the world.

Over 50 participants – judges, prosecutors, governmental officers and representatives from the European Commission and Europol Liaison Bureau – participated in the event.

During the conference it was underlined that considering the current cybercrime trends and challenges, including for judges and prosecutors, more coordinated efforts and actions at the national and international level are needed.

As a follow up to the Conference, ERA with support of the European Commission's TAIEX programme is organising a series of seminar on the "Fight against cybercrime" with the purpose of assessing how European legislation in this field is applied in different Member States of the European Union and candidate countries and the perspectives for an effective Europe-wide campaign against cybercrime. Under the Project on Cybercrime the Council of Europe participated in some of these activities thus promoting the Convention on Cybercrime and its Additional Protocol.

2.7.5 Portugal/Europe – Meeting on institutionalising judicial training (Lisbon, 6 July 2009)

An informal meeting on "the future of cybercrime and training needs for judges and prosecutors" was held in Lisbon on 6 July 2009 in cooperation with the Center for Judiciary Studies, CEJ. The meeting was an excellent opportunity for participants (international experts and representatives from important private sector companies) to discuss on the needs and different national and international approaches to the training judges and prosecutors in cybercrime matters. The exchange of views helped preparing the concept paper on institutionalizing cybercrime training for judges and prosecutors. If furthermore confirmed the role that the CEJ could play in this respect.

2.7.6 Global – Workshop on the judicial training concept (Strasbourg, 3 – 4 September 2009)

Following the workshop at the Octopus Conference in March 2009, the meeting in Lisbon on 6 July and replies to a questionnaire received between June and August 2009, a draft concept paper was prepared that was discussed in detail and finalised at a workshop at the CoE in Strasbourg on 3-4 September 2009. The meeting was jointly organised by the Lisbon of Judicial Training Institutions of the CoE and the Project on Cybercrime. Representatives of eleven judicial training institutions, of the European Judicial Training Network as well as the private sector and academia participated.

The purpose of the concept is to help judicial training institutions develop training programmes on cybercrime and electronic evidence for judges and prosecutors and to integrate such training in regular initial and in-service training (that is, to institutionalise it). It will furthermore facilitate networking among judges and prosecutors to enhance their knowledge as well as consistent – rather than ad hoc – support to training initiatives by interested partners.

The concept consists of the following elements:

Objectives:

- To enable training institutes to deliver initial and in-service cybercrime training based on international standards

- To equip the largest possible number of future and practicing judges and prosecutors with basic knowledge on cybercrime and electronic evidence
- To provide advanced training to a critical number of judges and prosecutors
- To support the continued specialisation and technical training of judges and prosecutors
- To contribute to enhanced knowledge through networking among judges and prosecutors
- To facilitate access to different training initiatives and networks.

Measures in the following areas should help achieve these objectives:

1. Institutionalising initial training
2. Institutionalising in-service training
3. Standardised and replicable courses/modules
4. Access to training/self-training materials
5. Pilot centres for basic and advanced training
6. Enhancing knowledge through networking
7. Public private cooperation

Follow up:

- The Lisbon Network of the Council of Europe approved this concept in September 2009 and recommended that it be widely disseminated and implemented by judicial training institutions
- The implementation of this concept is primarily the responsibility of judicial training institutions but should be supported by public and private sector institutions and partners, including international organisations such as the CoE
- The Council of Europe and other bodies should promote the implementation of the concept throughout Europe and beyond. The Council of Europe should regularly assess the progress made
- The implementation of this concept in practice should also be supported by donors. Interested donors and organisations could partner up to develop projects to assist training institutions and other stakeholders that are prepared to assume responsibility for the measures proposed in this concept.

2.7.7 Concept for the training of judges and prosecutors (November 2009)

The Consultative Council of European Prosecutors welcomed the concept for the training of judges and prosecutors on cybercrime and electronic evidence (adopted by the Lisbon Network of judicial training institutions) and invited the relevant authorities in the member states to make the best use of it.

The concept was translated into several languages and has been widely distributed.

2.7.8 ERA - TAIEX seminar on the fight against cybercrime (Bucharest, 8-9 October 2009)

The event was organised within a series of events having the purpose to assess how the European legislation in this field is applied in different EU Member States and candidate countries and the perspectives for an effective Europe-wide campaign against cybercrime. The CoE contributed to these events.

Participants discussed the practical implementation of the Council of Europe Convention on Cybercrime and the Convention on child protection against sexual exploitation and sexual

abuse, Council Framework Decision 2005/222/JHA on attacks against information systems, and Council Framework Decision 2004/68/JHA on combating the sexual exploitation of children and child pornography.

Most of the interventions from the participants raised the question on how mutual legal assistance between judicial authorities in cybercrime cases could be speed up at the international level.

One of the conclusions of the meeting was that by implementing the Convention on Cybercrime and implicit the Council Framework Decision 2005/222/JHA on attacks against information systems, judges and prosecutors in Romania have not encountered specific problems that would be related to gaps in the legislation on cybercrime.

2.7.9 Training for judges on cybercrime and child abuse (6-10 December 2009, Cairo, Egypt)

Two training workshops for judges on cybercrime and child abuse (6-9 December 2009, Cairo, Egypt) and a round table discussion on a concept for the training of judges in cybercrime/electronic evidence in Egypt (10 December 2009, National Centre for Judicial Studies, Cairo) were organised by the CoE in cooperation with the National Centre for Judicial Studies of the Egyptian Ministry of Justice and Microsoft.

The objective of the training workshop was to provide judges with basic knowledge on cybercrime and electronic evidence.

The same 2-day module was delivered consecutively to two groups of judges and district attorneys on cybercrime and child abuse (in total 187 judges)

The Training workshop:

- The 2-day module was repeated based on MOJ request to benefit the largest possible number of judiciary
- The event was considered a great success and had very positive reviews from both MOJ and MCIT
- According to the Training Requirements and Evaluation Unit of the National Center for Judicial Studies Report most of the participants considered:
  - the training program was excellent and must be circulating among all judges and public prosecutors
  - trainers succeeded in dealing with all subject matters and deliver the information in a pragmatic way
- Among recommendations:
  - based on this course to organize advanced course
  - to study international treaties that deal with Internet and child sexual abuse and enforce such treaties
- The event was an example of cooperation between multiple local and international bodies, private and public, including the Egyptian Government (Egyptian National Centre of Judicial Studies, Ministry of Communication and IT, International Peace Movement, ICMEC, Inhope, Microsoft and the Council of Europe).

During the Round Table discussion with the National Centre of Judicial Studies (Ministry of Justice) was promoted the integration of cybercrime and electronic evidence matters into the curricula of judicial training institutions

Participants: Representatives of the National Centre for Judicial Studies (Cairo) Ministry of Communication and IT, the Council of Europe, Microsoft and the experts from the training workshop.

Round table:

- COE presented cybercrime training concept developed under the global Project on cybercrime
- Centre provided an assessment of the training workshop on cybercrime
- Further cooperation on training of judges in cybercrime/electronic evidence, including online child abuse, between the Council of Europe and the National Centre for Judicial Studies (Cairo) was discussed
- CoE invited the Centre for Judiciary Studies to attend and present at the Cybercrime Octopus Conference (23-25 March 2010)

Follow-up:

- The training concept for judges and prosecutors to be implemented in Egypt
- Consider the possibility that the centre, which seems to be extremely important in the region providing judicial training for Arab countries, Africa and other regions, to become a pilot centre on cybercrime training
- CoE will share curricula on cyber crime and the Training Manual on cybercrime when they become available.

2.7.10 Cybercrime training for law enforcement and judges (Islamabad, Pakistan, 23-24 Feb 2010)

The Federal Investigation Agency (FIA), Microsoft and the Council of Europe jointly organised two cybercrime training sessions for law enforcement officers in Islamabad on 23 and 24 February 2010. Furthermore, round table discussions were held on institutionalising cybercrime training with FIA as well as judicial training with the Federal Judicial Academy.

In addition, an exchange of views took place with the Pakistan Information Security Association (PISA).

These events will feed into ongoing legislative reforms and help bring the legislation of Pakistan further in line with the Budapest Convention on Cybercrime.

Follow up:

- Delivery of a two-weeks basic law enforcement training course in view of preparing for the creation of a cybercrime centre of excellence
- Assisting the Federal Judicial Academy in the preparation of a basic training course for judges
- Support to cybercrime legislation (transforming the Prevention of Electronic Crimes Ordinance into a proper law taking into account the Budapest Convention).

2.7.11 Octopus workshop on judicial training (Strasbourg, 23 March 2010)

The workshop discussed existing initiatives and good practices regarding the training of judges and prosecutors such as programmes developed in Netherlands, Portugal, France and Egypt and others including initial and in house training for judges and prosecution as well as cybercrime support infrastructures for judges or the creation of international initiatives such as the Global Prosecutors E-Crime Network (GPEN).

The workshop focused in particular on the concept for judicial training of judges and prosecutors prepared by the Council of Europe's Project on Cybercrime and Lisbon Network which will help institutionalise such training into the curricula of judicial training institutions, and recommended broad implementation.

The following challenges were identified during a discussion session with contributions received from the audience:

- It is necessary to have the right legislation in place before training is developed. At the same time, since the development of legislation may take a long time, training could also be delivered to judges based on good practices and experience of other countries. This will help provided judges with skills and awareness and make them informed stakeholders in the legislative process
- There is a lack of common standards in evidential rules in respect of electronic evidence and admissibility
- There is a general lack of understanding of technology across the board
- Judges and prosecutors need training on technical as well as legal issues
- Defence lawyers are often excluded from existing programmes.
- There is a lack of suitable training material available
- There are many national but few international solutions
- Shortage of qualified and experienced trainers
- Too much training consists only of Powerpoint or similar presentations
- Expensive "Face to Face" training is often the only choice available
- Current training is often too academic and not practical enough.

In terms of the way ahead, it was recommended to work on:

- Awareness raising at the introductory level for all players in the Criminal Justice System
- Develop sustainable and harmonised training programmes for lawyers (prosecution and defence) as well as LEA, judges and prosecutors
- Cooperation with Universities and the private sector in formulating courses that meet the needs defined by players in the Criminal Justice System
- Develop a glossary of internationally accepted terms
- Combine case based scenario training for teams (police, prosecutors and judges)
- Develop training materials based on common standards, such as the Budapest Cybercrime Convention.

2.8 Activities related to 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 Indicators: ▪ Up to 5 legal opinions on data protection standards in line with CETS 108 and 181 prepared and at least 5 draft laws available in non-European countries meeting these standards ▪ Accession requests by at least 3 non-European countries to CETS 108

Summary of progress made towards this expected result:

Specific activities under this component were limited between March and September 2009. However, data protection and privacy issues were raised on a number of occasions and the ground was prepared for future activities:

- The authorities of Morocco were encouraged in July 2009 to seek accession to the CoE's Convention on data protection (CETS 108) since new legislation is now in place in this country
- Following an exchange of letters, the Project on Cybercrime will participate in the meetings of the OECD's Working Group on Information Security and Privacy
- A presentation was made on "privacy and security: what are the issues?" at the meeting of the European Dialogue on Internet Governance (EuroDIG) in Geneva on 14 September 2009
- The issue of data protection in connection with cloud computing was raised in multiple events, including the Octopus Conference in March 2010.

In terms of data protection policies the decision of the CoE's Committee on Data Protection (T-PD) to work towards a modernisation of the data protection convention CETS 108 and of the CoE to encourage non-member States of the CoE to accede to this treaty (and its Protocol CETS 181) are positive developments. Data protection legislation and systems in line with this treaty and accession to this treaty should be of interest to non-European countries as it would indicate that they meet European data protection standards which in turn facilitates off-shoring of services from Europe as well as law enforcement cooperation with Europe.

2.8.1 Europe – EuroDIG (Geneva, 14-15 September 2009)

The 2nd European Dialogue on Internet Governance comprised a workshop on cybercrime and cybersecurity which was used by the Project on Cybercrime to point at the links and challenges related to the issues of "security and privacy" and to underline that measures against cybercrime (for example full implementation of the Convention on Cybercrime) would need to be combined with global trusted privacy and data protection policies/strategies as well as trusted authentication systems that protect privacy. Technological developments (IPv6, DNSSEC etc.) may enhance problems but also provide opportunities in this respect.

In terms of data protection policies the decision of the CoE's Committee on Data Protection (T-PD) to work towards a modernisation of the data protection convention CETS 108 and of

the Committee of Ministers to encourage non-member States of the CoE to accede to this treaty are positive developments. Data protection legislation and systems in line with this treaty and accession to this treaty should be of interest to non-European countries as it would indicate that they meet European data protection standards which in turn facilitates off-shoring of services from Europe as well as law enforcement cooperation with Europe.

Follow up:

- The Project on Cybercrime to support interested countries in the strengthening of their data protection legislation and to encourage their accession to treaty CETS 108 and Protocol CETS 181.

2.8.2 Octopus panel on security and privacy in the clouds (Strasbourg, 25 March 2010)

Cloud computing, with the migration of data and services from specific computers to servers "somewhere" in the clouds, entails tremendous opportunities but also far reaching security implications that are being discussed in many fora. This session focused on the following questions:

- How are personal data protected that are stored on servers in the "clouds"; what laws govern their protection?
- What does cloud computing mean for law enforcement access to computer data and systems in the "clouds" and for jurisdiction?
- Are current regulatory frameworks regarding data protection and law enforcement sufficient?

Discussion suggested that:

- The fact that the challenges related to cloud computing are discussed in multiple fora and by many organisations (such as ENISA, the Cloud Security Alliance, the OECD, the Council of Europe, industry and many others) is important in itself and will help define the questions and identify solution
- The proposal for international standards on privacy and personal data protection adopted by the 31st meeting of data protection commissioners (Spain, November 2009) may help advance the development of common global data protection standards
- The opening up to third countries of the Council of Europe's data protection Convention (CETS 108) and the decision to modernise this treaty offers an opportunity for countries to join an existing international instrument on data protection
- The Budapest Convention on Cybercrime – if fully implemented and applied efficiently – offers solutions to some of the law enforcement challenges
- The Cybercrime Convention Committee (T-CY) is currently analysing the question of trans-border law enforcement access to stored computer data.

In terms of the way ahead, it was recommended that:

- Existing instruments on cybercrime (Budapest Convention) and data protection (CETS 108) should be fully and efficiently implemented to help ensure security and privacy in the clouds
- The Cybercrime Convention Committee to continue its study on trans-border law enforcement access and the question of jurisdiction

- The Project on Cybercrime – in cooperation with public and private sector stakeholders could set up a working group – to carry out further research to identify good practices and possible solutions on security and privacy aspects of cloud computing
- The preparation of additional international standards or guidelines for cloud providers and law enforcement should be considered
- The establishment of globally trusted data protection standards and systems will need to be pursued.

2.9 Activities related to 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

Indicators:

- Comparative study on the implementation of art 9 (child pornography) of the Convention on Cybercrime
- Up to 10 events promoting the Convention on the Sexual Exploitation and Sexual Abuse of Children (CETS 201) and on Trafficking in Human Beings (CETS 197) in relation to the internet.

Summary of progress made towards this result:

- Between March 2009 and June 2010, the Project on Cybercrime organised or contributed to more than 10 events through which implementation of Article 9 of the Convention on Cybercrime and Convention on the Sexual Exploitation of Children (CETS 201) was promoted. This treaty entered into force on 1 July 2010
- Cooperation with APEC, the European Commission, the OECD, ECPAT, UNICEF, eNASCO and a range of other organizations and the private sector was sought to seek synergies and enhance the impact of the Project on Cybercrime in this respect.
- The comparative study on substantive criminal law provisions related to the sexual exploitation and abuse of children was launched. 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.

The following activities supported by the Project on Cybercrime contributed to this expected result:

2.9.1 Global – Octopus workshop on the sexual abuse of children (Strasbourg, 10-11 March 2009)

At the Octopus conference in March 2010 a specific workshop was held on criminalising child pornography and sexual exploitation and abuse of children on the Internet which concluded that Article 9 of the Convention on Cybercrime (CETS 185) and the Convention on the Sexual Exploitation and Sexual Abuse of Children (CETS 201) provide a comprehensive normative framework in this respect. However, only a few countries have so far fully implemented Article 9. Many other countries should therefore review and improve their current provisions in line with this Article. Countries should update their country profiles to facilitate such reviews. Consideration should also be given to the implementation of the new offences introduced by Convention 201. With regard to the obligations or liability of ISPs for child abuse materials there are differences regarding access, hosting and content providers. A number of issues require further debate.

2.9.2 APEC – Child protection online OECD/APEC symposium (Singapore, 15 April 2009)

The CoE was invited to the joint symposium of the Asia-Pacific Economic Cooperation and the OECD on initiatives among Member economies promoting safer Internet environment for children (15 April 2009, Singapore).

The objective of the event, gathering over 50 participants representing APEC economies, OECD, other organizations and stakeholders, was to promote a safer Internet environment for children.

The intervention of the Council of Europe in the session on best practices to address illegal/harmful content[17] underlined that Article 9 (together with the procedural law and international cooperation provisions) of the Convention on Cybercrime (CETS 185), and the Convention on the Protection of Children against Sexual Exploitation and Sexual Abuse (CETS 201) are instruments which provide the core elements of criminal legislation aimed at protecting children online.

In the concluding remarks of the session the chair encouraged APEC economies to use these instruments as a guideline for designing and harmonising legislation and use them as a framework for international cooperation.

2.9.3 Czech Republic/EU – Conference "Safer Internet for Children" (Prague, 20 April 2009)

The Ministerial Conference "Safer Internet for Children – fighting together against illegal content and conduct on-line" was organised under the Czech Presidency of the Council of the European Union by the Czech Ministry of Interior in co-operation with the European Commission. The CoE participated in this event through the Project on Cybercrime.

The Conference focused on the fight against illegal content and harmful conduct online (cyber bullying, grooming children). The main objective of the Conference was the adoption of a Ministerial Declaration concerning this issue and police cooperation.

Approximately 250 participants attended the Conference, including representatives of governments (Ministry of Justice, Ministry of Interior, Ministry of Youth and Sport, Ministry of Education, Ministry of Family) from European Union member states and Norway and Switzerland, representatives of private sector, NGO's and international organisations.

The European Commission presented the Safer Internet work programme for 2009 and pointed out that Russia was a priority country for the EU with regard to cybercrime. While presenting the new Safer Internet Programme for 2009-2013 (with a budget of €55 millions), it was underlined that the EC would strengthen cooperation with the Council of Europe.

The EC furthermore presented the EC proposal for an update of the Council Framework Decision on combating the sexual exploitation of children and child pornography (2004/68/JHA) which – in its explanatory memorandum – refers to Convention CETS 201 as the "highest international standard for protecting children against sexual abuse and exploitation to date".

[17] Presentations available on the APECTEL website http://www.apectelwg.org/

Participants supported this proposal in the Declaration adopted at the end of the Conference. The EC stressed that the CoE was an important partner as regards the fight against the sexual exploitation of children.

During a "high level panel", representatives of different countries presented their programmes and achievements regarding safer use of the Internet. The representative of the Ministry of Justice of the Netherlands and a Secretary of State from Norway expressed their support to the CoE Convention on the Protection of Children against Sexual Exploitation and Sexual Abuse. A representative of the Swiss government stressed the fruitful cooperation between his country and the CoE in the fields of cybercrime and protection of children.

By adopting the "Prague Declaration", participants committed to support politically and financially the implementation of the Safer Internet Programme for 2009 – 2013 at national level. It should be underlined that they also committed "to intensify cross-border cooperation, in particular by (…) taking into account the CoE Convention on Cybercrime and the CoE Convention on the Protection of Children against Sexual Exploitation and Sexual Abuse".

2.9.4 EU – Public Presentation on "Protecting children using the internet" (Brussels, 5 May 2009)

The CoE participated in the Public Presentation on "Protecting children using the internet" organised by the European Economic and Social Committee (EESC) on 5 May 2009, which brought together about 100 participants from across Europe. The objective was to promote a safer Internet environment for children.

The meeting underlined the need to implement the Convention on Cybercrime and provided an opportunity for the Council of Europe to promote its instruments on the protection of children against sexual exploitation and sexual abuse (CETS 201) as well as call for their ratification by those EU Member States that have not yet done so.

Increased international cooperation and coordinated partnerships to make the internet a safer place for young people and especially children were vigorously and unanimously requested by speakers and participants.

Follow up:

- As one of the rapporteurs concluded: Since several Member States have not yet ratified the Council of Europe instruments, *"political will is now most urgent as is the ratification of the Convention by those countries who have not yet endorsed it. Europe needs to put its own house in order so that we can work as a true EU block"*[18].

2.9.5 Arab region – Protection of children in cyberspace (Tunis, 16 May 2009)

The Council of Europe made a presentation on its work related to the Convention on Cybercrime at an event on the "Protection of children in cyberspace" organised by the Arab Information and Communication Technologies Organization (AICTO) and the ITU.

[18] Presentations and speeches are available at the EESC website:
http://www.eesc.europa.eu/sections/ten/index_en.asp?id=4300003tenen

Participants were mainly officials from AICTO member states and senior representatives of private IT companies and internet service providers. The CoE was the only European intergovernmental organisation speaking at the conference. The conference consisted of a number of presentations and panel discussions on the topics of "cybersecurity" and "protecting children in cyberspace".

People in the majority of Arab (Middle Eastern, North and East African) states participating in the event have (as yet) relatively little access to internet. The situation appears to be somewhat different in Tunisia and Egypt, where a growing part of, in particular, the urban population is using internet for educational, leisure and commercial purposes.

The positive impact of the internet in providing children with education tools and women with means of communication was underlined by many participants. Due to the low frequency of commercial transactions via the internet in the AICTO member states, identity theft and other types of internet based fraud was not yet a major source of concern.

The main concern of almost all Arab state representatives appeared to be how to protect families from "harmful" content by obliging internet service providers to use various state sponsored filtering systems to hinder access to certain types of sites.

Follow up:

- Continue to assist countries of the Arab region in the strengthening of legislation in line with the Convention on Cybercrime and the Convention on the Sexual Exploitation and Sexual Abuse of Children (CETS 201)
- Help ensure that measures against harmful content are not aimed at restricting the freedom of expression.

2.9.6 Europe – Conference "Protection of Children against Sexual Violence" (Berlin, 30 June 2009)

The international Conference "Protection of Girls and Boys against Sexual Violence in the New Media" (with the participation of the Deputy Secretary General of the Council of Europe) included discussions on the new German law on access blocking (adopted by the Parliament on 18 June 2009) and whether European standards in this respect should be developed.

Following an agreement with major service provides earlier in 2009, the law obliges all ISPs to block sites based on a list prepared by the Federal Criminal Police (BKA). However, it appears that provisions of the law will not be applied pending a review of the extent to which take down measures are feasible.

The meeting furthermore helped promote the Convention on the Protection of Children against Sexual Exploitation and Sexual Abuse and the Convention on Cybercrime.

2.9.7 Global study on compliance with CoE instruments (Strasbourg, July 2009 – September 2010)

The CoE is promoting criminal law measures to protect children from sexual exploitation and abuse online, as well as safe internet for children by multi-stakeholder cooperation based on common elements (strategies/specific actions/good practices), synergies and mechanisms for interaction.

As a follow up to the Octopus conference, a study was initiated under the Project on Cybercrime, which will analyse the compliance of European and selected non-European

countries with substantive criminal law provisions of CoE instruments, that is, Article 9 (child pornography) of the Convention on Cybercrime and with the Convention on the Sexual Exploitation and Sexual Abuse of Children (CETS 201). The comparative study on substantive criminal law provisions related to the sexual exploitation and abuse of children[19] is aimed at:

- Raising awareness of countries of the existing instruments already available to help them build a strategy to cope with sexual exploitation of children
- Promoting global standards for harmonizing legislation and a framework for effective and efficient international cooperation on cybercrime, including offences related to sexual exploitation and sexual abuse of children
- Serving as a database for legislation and help share good practices
- Preparing a future tool to monitor the legislation on child protection against sexual abuse and sexual exploitation

The conclusions of the study will be included as CoE contribution to the OECD ongoing study on protecting children online

2.9.8 Fighting against online child abuse images (Luxembourg, 16 September 2009)

The objectives of the 2nd meeting of Internet Focus Group "Fighting against online child abuse images" organised by the European Commission were to:

- Identify obstacles in cross border cooperation of LEAs investigating online child abuse
- Identify training offer for and needs of online child abuse investigators
- Formulate recommendations to the EC on the issue of notification and take-down of child abuse images
- Discuss the functionalities of the cyber crime platform and the INHOPE url database.

The discussions focused on:

- The Council of Europe 24/7 Network established under the Convention on Cybercrime, including the difficulties and lessons learnt identified under the discussion paper "The functioning of 24/7 points of contact for cybercrime (prepared by the Project on Cybercrime)
- Difficulties in cross border investigations
- Cooperation between LEAs and ISPs and good practices (e.g. Microsoft's "Cooperation procedure"), including in the training area
- New developments with regard to cybercrime training provided by different organizations: CoE, European Union, Europol etc.
- The Europol Cybercrime platform could help avoid overlapping investigations and uncoordinated international action

[19] In order to collect information a questionnaire was sent in November 2009.
44 countries responded: Armenia, Austria, Belgium, Bulgaria, Costa Rica, Croatia, Cyprus, Czech Republic, Denmark, Dominican Republic, Estonia, Finalnd, France, Georgia, Germany, Greece, Hungary, Ireland, Italy, Japan, Latvia, Liechtenstein, Lithuania, Luxembourg, Mexico, Moldova, Monaco, Montenegro, Norway, Philippines, Poland, Portugal, Romania, San Marino, Serbia, Slovak Republic, Slovenia, Spain, Switzerland, "The Former Yugoslav Republic of Macedonia", Turkey, United Kingdom, Ukraine
13 countries targeted in the first stage have not replied yet to the questionnaire:
Albania, Andorra, Azerbaijan, Bosnia and Herzegovina, Canada, Chile, Russian Federation, Iceland, Malta, Netherlands, South Africa, Sweden, United States of America.

- Need for a mechanism to allow sharing information regarding national investigations on child sexual abuse (e.g. establish a communication network for online child sexual abuse investigators).

Possible action for the European Commission to include a training program for online child abuse investigators, strengthening of the analytical capacity of Europol (AWF Twins), familiarise LEAs in some countries with cooperation and support given by Europol, Eurojust and Interpol, design an advanced procedure for notification and take-down, action with registrars.

2.9.9 Protecting Children from Sexual Offenders in the IT Era (Courmayeur, Italy, 11-13 Dec 09)

This conference was organised by the International Scientific and Professional Advisory Council (ISPAC) of the United Nations and focused on "Protecting Children from Sexual Offenders in the Information Technology Era".

During the event there were four workshops held simultaneously:

- technical solutions available to law enforcement and criminal justice
- status of scientific research and training of law enforcement staff
- collaboration between law enforcement/justice authorities and the private sector/industry
- victim protection.

In the session on action by international and regional institutions, the CoE representative underlined that the Convention on Cybercrime and the Convention on the Protection of Children against Sexual Exploitation and Sexual Abuse are global instruments, which provide the core elements of criminal legislation aimed at protecting children online.

Follow up:

- Raising awareness of countries and other stakeholders by participating in such events of the existing instruments already available to help build a strategy to cope with sexual exploitation of children

2.9.10 Safer Internet Day (Strasbourg, 8-9 February 2010)

The CoE, the International Centre for Missing and Exploited Children and Microsoft jointly organised a dinner debate in Strasbourg on 8 February 2010 to stimulate discussion around the value of partnerships in promoting online safety combined with a holistic approach that also includes strengthening relevant laws, empowering law enforcement and NGOs and deploying technology tools to achieve greater levels of safety.

This event was coordinated with the Safer Internet Programme of the European Commission and helped prepare for Safer Internet Day meeting in the Parliament of the European Union on 9 February.

2.9.11 Octopus workshop on the sexual exploitation of children (Strasbourg, 24 March 2010)

Presentations were made by representatives of the Council of Europe outlining initiatives and projects being implemented that address the issue of online child protection. It was underlined that the relevant instruments developed by the Council of Europe, namely the

Convention on the Protection of Children against Sexual Exploitation and Sexual Abuse (CETS 201) and the Convention on Cybercrime (CETS 185) are guidelines for action and assessment of progress made by countries. During the panel discussions with representatives from ECPAT International, Cyber Peace Initiative (Egypt), OECD, Interpol, EU Safer Internet Programme and eNACSO and other participants were outlined particular issues of interest. Many of the panellists described some of the initiatives that they have undertaken by their organizations at a local and national level to deal with the issue of child sexual exploitation.

Specific examples varied from the development of a child safety initiative in Egypt to the lack of quantifiable structured data to make adequate assessment of the scope of the problem at global or national level.

Most speakers outlined what direction and action their organizations are taking to address the issue at a national and international level. Law enforcement spoke on the issue of the use of technology to identify victims in an effort to identify potential perpetrators who prey on children.

Examples of good practices and initiatives to tackle this issue discussed were ECPAT, OECD, Cyber Peace initiatives, EU Safer Internet Programme, Interpol.

The Convention on the Protection of Children against Sexual Exploitation and Sexual Abuse (CETS 201) provides a comprehensive set of measures and offers benchmarks for determining progress made by countries. Together with the Budapest Convention on Cybercrime this treaty represents a comprehensive guideline for countries to develop a national strategy to cope with sexual exploitation and sexual abuse of children, including criminal law measures.

Interaction between the OECD and the Council of Europe in the preparation of their respective studies is a good example of cooperation. UNICEF is also working on a study and is open to cooperation.

Other governmental organizations discussed some of the ongoing programs of work that are undertaken to empower both the law enforcement and NGO community in an effort to effectively deal with child sexual exploitation.

Other organizations are conducting studies in an effort to better recognise the scope of the problem and identify the direction needed to be effective in dealing with the issue.

The discussion then turned to the question "take down or access blocking", this brought on a very spirited exchange between several members of the audience and panel. The discussion was welcomed and progressed to a useful exchange of thought and opinions and very worthwhile.

It was agreed that blocking should be used as preventive measure and not as the ultimate solution. Preference should be given to notice and take down. However, it is crucial to find the most effective technical methods in order to avoid abuse.

In terms of the way ahead, participants concluded:

- It is evidently clear that more must be done to identify, promote and support many of the ongoing initiatives being conducted by the organizations that presented at

the conference workshop. There was an overriding consensus that we are moving in the right direction but more has to be done to support these initiatives

- Specific example: More international organisations are supporting projects that aid in the identification of victim images
- There is a need for direction in the development and exchange of "best practices" on many issues pertaining to the child/victim issues
- It should be considered to engage the industry in more collaborative efforts to deal with the issue of child sexual exploitation. While it is recognized that industry has been helpful in these endeavours in the past and present, there is still a need to find better solutions and project to continue the efforts
- Better coordination among organizations and stakeholders with regard to different initiatives would help identify needs and solution. Linking of the studies in preparation by UNICEF, the OECD and the Council of Europe would serve as a good example
- The Convention on the Protection of Children against Sexual Exploitation and Sexual Abuse (CETS 201) should be used as guideline and – in conjunction with the Budapest Convention – as a tool for effective cooperation and criminal law measures.

The way ahead:

- Promote the Convention on the Protection of Children against Sexual Exploitation and Sexual Abuse (CETS 201) as benchmarks to measure progress made in the implementation of actions to protect children
- The Council of Europe – through the Project on Cybercrime – to continue supporting widely the strengthening of comprehensive legislation on protection of children against sexual exploitation and sexual abuse and to promote relevant instruments globally
- Promote a better coordination among organizations and stakeholders with regard to different initiatives
- Complete the study on substantive criminal law provisions related to the sexual exploitation and abuse of children.

3 Conclusion: progress towards the project 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

Indicators:

- At least 50 countries will be parties to the Convention on Cybercrime, including at least 8 non-European countries
- At least 25 countries will be parties to the Protocol on Xenophobia and Racism, including at least 5 non-European countries
- Cybercrime legislation in line with the Convention on Cybercrime will be available in at least 75 countries around the world
- Increase in the number of requests send/received by 24/7 points of contact and high-tech crime units as well as mutual legal assistance requests
- At least 5 draft laws on data protection in non-European countries in line with CETS 108 and 181
- Legal measures promoted against the sexual exploitation and abuse of children and trafficking in human beings on the internet
- Agreements concluded between law enforcement and internet service providers in at least 5 countries
- Concept for judicial training adopted and widely disseminated
- Enhanced cooperation between financial intelligence units, high-tech crime units and the private sector against criminal money on the internet.

The aim of the project is to promote broad implementation of the Convention on Cybercrime (CETS 185) and its Protocol on Xenophobia and Racism (CETS 189) and related international standards, that is, in particular the 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).

Progress towards the project objective during the first sixteen months was satisfactory with Azerbaijan, Germany, Moldova, Montenegro, Portugal, Serbia and Spain ratifying the Convention on Cybercrime, Montenegro, Portugal, Romania and Serbia ratifying the Protocol on Xenophobia and Racism and Chile having been invited to accede to the Convention on Cybercrime while the invitations for Argentina and Australia to accede were in progress. In a large number of countries, legislative reforms are underway, often with the support of the project. Countries such as Botswana, Colombia, Indonesia, Mauritius, Senegal and others seem to have made sufficient progress to seek accession to the Budapest Convention.

At the same time a major concern remains which can only be overcome by stronger political will of CoE member States: The fact that 18 CoE member States have not yet ratified the Convention and five member States have not yet signed it weakens the credibility of this important treaty in other regions of the world.

It is therefore essential to intensify the dialogue with member States and countries already invited to accede to complete the ratification/accession process.

As in phase 1, the project has been able to cooperate with a large number of public and private sector stakeholders which enhances markedly the impact of this project. Links

between measures against cybercrime and the promotion of fundamental rights and the rule of law have been reinforced.

Status of signatures and ratifications of the Convention on Cybercrime (June 2010)

Ratified (30):

- 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
- The „former Yugoslav Republic of Macedonia"
- Ukraine
- United States of America

Signed (16):

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

Not signed (5 CoE member States):

- Andorra
- Monaco
- Russian Federation
- San Marino
- Turkey

Invited to accede (5):

- Chile
- Costa Rica
- Dominican Republic
- Mexico
- Philippines

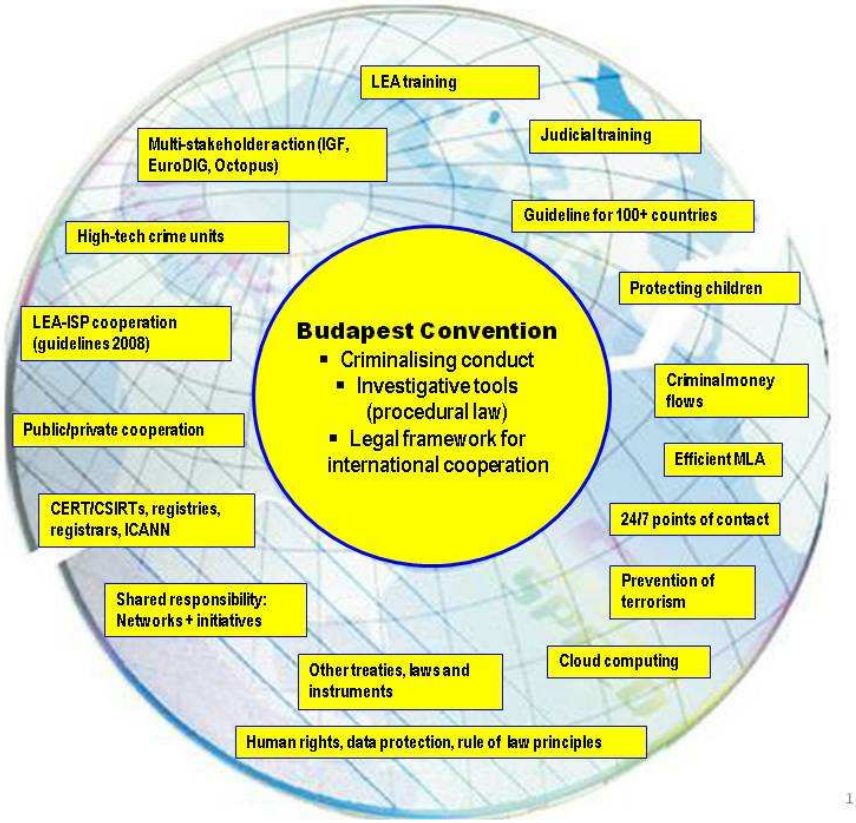
Tangible results have been achieved under each "expected result". The judicial training concept developed and widely disseminated during the first sixteen months of the project, the promotion of measures for the protection of children against sexual exploitation and abuse, the activities on international cooperation and law enforcement – service provider cooperation, and the initiation of activities related to criminal money flows on the internet as well as data protection are promising and are yielding results.

The project – in particular the partnership with Microsoft – is itself a good example of public/private cooperation. Microsoft not only provided voluntary contributions to the project in general but also logistical support and subject-matter expertise to a number of activities, helped disseminate the results of the project and promoted implementation of the Budapest Convention in events organised by Microsoft.

The Octopus conferences in March 2009 and March 2010 were highly successful, promoted interfacing among stakeholders, produced specific outcomes and generated visibility of efforts against cybercrime.

The project contributed significantly to the Cybercrime Convention Committee (T-CY), activities of the European Union, the United Nations Crime Congress and Crime Commission, and the work of other international organisations, and thus helped shape cybercrime policies at European and global levels.

In short, beyond the impact in terms of signatures, ratifications and accessions as well as the quality of implementation, the global Project on Cybercrime has been using the Budapest Convention as a vector to promote human rights and rule of law standards on the internet, to support the implementation of related European and international agreements, to create additional tools for training, institution building and public/private cooperation, and to provide a platform for multi-stakeholder cooperation.



Since the launching of Phase 1 in 2006, the project thus considerably enhanced the global value of the Budapest Convention.

The project was launched with initial contributions from Romania, Microsoft and McAfee as well as funding from the budget of the CoE (project DGHL/1429 on economic crime) and additional contributions by Estonia, Monaco and Microsoft in 2010. Nevertheless, it is important to underline that this global project remains largely under-resourced, and additional funds are urgently required if the project is to achieve its objective by its scheduled end in June 2011.

4 Workplan proposed for July to December 2010

Project priorities in the period July to December 2010 include:

- Policy dialogue with CoE member States in view of signatures and ratification of the Convention on Cybercrime
- Legislation – Continued support to the strengthening of legislation and the process of ratification/accession to the Convention on Cybercrime in particular with regard to CoE member States and countries already invited to accede
- Judicial training – Support to the implementation of judicial training concept and the delivery of training seminars
- Criminal money – Completion of the typology study on criminal money flows
- Children – Completion of the analysis of substantive criminal law provisions on the protection of children from sexual exploitation and abuse, and activities to promote the Convention on the Sexual Exploitation and Sexual Abuse of Children (CETS 201)
- jurisdiction, data protection and procedural safeguards (including support to the work undertaken by the Cybercrime Convention Committee)
- Initiation of a concept paper on cybercrime strategies for discussion at the 2011 Octopus Interface conference.

It should be noted that additional projects are in preparation, including a joint project of the European Union and the Council of Europe on "Regional Cooperation against Cybercrime" covering South-eastern Europe and Turkey as well as a sub-project of the EU and the CoE on cybercrime under the Eastern Partnership. Both projects are scheduled to start in autumn 2010 and will cover up to 14 European countries. They will complement the Global Project on Cybercrime.

Furthermore, and as follow up to discussions at the Octopus Interface conference in March 2010 and the meeting of the Cybercrime Convention Committee in June 2010, the possibility of setting up an agreement on action against cybercrime to assess needs, facilitate technical assistance and global capacity building, as well as to assess progress made by countries against cybercrime will need to be further explored. Such an agreement could help create a more sustainable basis and add an element of monitoring and accountability to global efforts against cybercrime.

List of activities foreseen July – December 2010 (subject to funding):[20]

Date	Place	Activity
1 July 2010	Brussels	Participation in the EU cybercrime experts group on statistics
2 July 2010	Paris	Contribution to the training course for judges at the Ecole National de la Magistrature
12-13 July 2010	Phnom Penh, Cambodia	Workshop on cybercrime legislation
25-27 August 2010	Mexico City, Mexico	Regional workshop on cybercrime legislation (for 7 countries of Latin America)
14-17 September 2010	Vilnius, Lithuania	Contribution to the Internet Governance Forum
7-8 October 2010	Moscow, Russian Federation	Meeting of the working group on criminal money flows (in cooperation with MONEYVAL and the MOLI-Russia project)
11-16 October 2010	Montreal, Canada	Participation in Digital Crime Consortium (Microsoft)
25-29 Oct 10	Kuala Lumpur, Malaysia	ASEAN Cybercrime Training Workshop for Judges and Prosecutors by the Judicial and Legal Training Institute (ILKAP)
25-27 Oct 10	Kuala Lumpur, Malaysia	Regional seminar on money laundering, trafficking and cybercrime (organised by France)
30 Nov–2 Dec 10	Abuja, Nigeria	Participation in West African Cybercrime Summit
30 Nov 2010	Brussels	Workshop on the impact of cloud computing
November 2010	Sankt Petersburg	Contribution to the MONEYVAL/Euro-Asia Group meeting on money laundering typologies
November 2010	Islamabad, Pakistan	Advice on cybercrime legislation and judicial training
November 2010	Phnom Penh, Cambodia	Follow up advice on cybercrime legislation
Nov/Dec 2010	Gabarone, Botswana	Decision-maker seminar on cybercrime
Week of 5 Dec 2010	Kyiv, Ukraine	Regional workshop on the sexual exploitation of children
December 2010 or January 2011	India	Training of judges

[20] As in the past, the project will attempt to respond to needs in a flexible and pragmatic manner.