COUNCIL OF EUROPE CONSEIL DE L'EUROPE

Economic Crime Division
Directorate General of
Human Rights and Legal Affairs
Strasbourg, 11 August 2008

Provisional/Public

Project on Cybercrime

Progress report

Status as at 31 July 2008

Project funded by the Council of Europe, Microsoft and Estonia

Contents

Contact

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

Executive Summary

This report summarises activities implemented under the Project on Cybercrime between September 2006 and July 2008.

Some 80 activities have been carried out under the project since its inception in September 2006 ranging from legislative reviews, training workshops and global conferences to contributions to events organised by other organisations.

The project relies 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 Convention on Cybercrime now serves as the primary reference standard for the development of cybercrime legislation in more than 90 countries. The project has been instrumental in this respect.

An increasing number of countries worldwide has legislation in line with the Convention. They are able to fully cooperate against cybercrime provided they request accession and are invited to accede to this treaty.

Important achievements during the first seven months of 2008 include the global Octopus Interface Conference (Strasbourg, 1-2 April 2008), the adoption of guidelines for law enforcement – Internet service provider cooperation, and the expansion of activities to Africa and the Caribbean. In Argentina and Indonesia new legislation on cybercrime was adopted by parliaments, and in Brazil the adoption of the new law is expected shortly. The Philippines were invited to accede to the Convention and the draft law is now before parliament. The Dominican Republic requested accession.

Slovakia and Italy ratified and Azerbaijan and Georgia signed the Convention in the first half of 2008. Other countries, in particular European member States, are expected to accelerate the ratification process. Only six of the 47 member States have not yet signed the Convention. In 2008, Croatia and Norway ratified the Protocol on Xenophobia and Racism which was also signed by South Africa.

Microsoft remained the main donor, contributing more than one third of the project budget to date. Estonia also made a voluntary contribution to the project in February 2008. Other public and private sector donors are invited to follow their example.

The project will end in February 2009. During the remaining seven months, the project will continue to support the strengthening of cybercrime legislation, disseminate the law enforcement – ISP guidelines, prepare and test training materials for judges, and strengthen the network of 24/7 points of contact. It will also contribute to the Internet Governance Forum in Hyderabad, India, in December.

The project feeds into to the Consultations of the Parties, that is, the Cybercrime Convention Committee (T-CY), and has been tasked by the T-CY to follow up on a number of decisions.

Experience to date clearly shows that the project has been able to produce results and make an impact, and that there is much demand for continued support of a similar nature.

A phase 2 project should:

- be aimed at the implementation of the Convention on Cybercrime and its Protocol
- also promote standards related to data protection, trafficking in human beings and the protection of children
- help make international cooperation (both 24/7 points of contact and judicial cooperation) more effective
- support the implementation of the guidelines on law enforcement – service provider cooperation
- support the training of judges
- strengthen cooperation with other organisations and initiatives, including training institutions and academia.

The budget required is estimated at Euro 1.4 million for a duration of 28 months. Donors are called upon to make this project possible through voluntary contributions.

Such a follow up project could be launched at the global Octopus Interface Conference on 10-11 March 2009 that is preceding the Cybercrime Convention Committee (T-CY) on 12-13 March.

1 Background

In 2001, the Convention on Cybercrime of the Council of Europe was adopted and opened for signature. This treaty – and the Protocol on Xenophobia and Racism committed through computer systems – helps societies cope with the challenges of cybercrime in that it provides for:

- the criminalisation of cyber-offences, and thus for a certain level of harmonisation between countries
- procedural measures to allow for effective investigations
- efficient international cooperation against cybercrime.

Although developed by the CoE, the Convention and its Protocol increasingly serve any country around the world as a guideline for the preparation of national legislation, and as a global framework for cooperation against cybercrime.

The Project against Cybercrime has been designed to support countries in their efforts to ratify or accede to as well as to implement the Convention and its Protocol. It was launched in September 2006 and will end in February 2009. The objective and expected outputs are:

Project objective:	To promote broad implementation of the Convention on Cybercrime (ETS 185) and its Protocol on Xenophobia and Racism (ETS 189)
Output 1:	Draft laws meeting the standards of ETS 185 and 189 available in at least 10 European and 5 non-European countries
Output 2:	Capacities of criminal justice systems strengthened to investigate, prosecute and adjudicate cybercrime
Output 3:	Capacities of criminal justice bodies to cooperate internationally re-enforced

Although this project was initially to have a budget of Euro 1.7 million, voluntary contributions from Microsoft, from Estonia, and the allocation from the CoE budget allowed this project to commence at a reduced scale.

Following a second progress report in December 2007, the present report summarises the activities and results achieved as at end-July 2008 and provides an updated list of activities for August 2008 to February 2009, that is, to the end of this project.

2 Activities

2.1 List of activities (September 2006 – July 2008)

Date	*Place*	*Description*
31 Aug - 1 Sep 2006 ✓	Geneva, Switzerland	Participation in the Meeting of the International Telecommunication Union on cybersecurity and spam: promotion of the Convention on Cybercrime as a guideline for the development of national legislation
17-19 Oct 2006 ✓	Rome, Italy	Support to the 2nd Training Conference of the G8 Network of 24/7 contact points
27-29 Nov 2006 ✓	Pitesti, Romania	Support to the National Cybercrime Training Conference in Romania
29-30 Nov 2006 ✓	Lisbon, Portugal	International seminar for Portuguese-speaking countries on "Meeting the challenge of cybercrime - Experience, good practice and proposals for improvement"
13-14 Feb 2007 ✓	Cairo, Egypt	Meetings and legislative advice to facilitate accession to the Convention on Cybercrime. Followed by a review of the draft law on cybercrime in April 2007
20-23 Feb 2007 ✓	New Delhi, India	Meetings and legislative advice to facilitate accession to the Convention on Cybercrime Followed by a review of the draft legislative amendments in March 2007
Feb 2007 ✓	Strasbourg	Analysis of the draft law on cybercrime of Pakistan
6-7 Feb 2007 ✓	Kyiv, Ukraine	Regional conference for countries of eastern Europe on cooperation against cybercrime (funded by the UPIC project on international cooperation in criminal matters)
27 Feb – 2 Mar 2007 ✓	Brasilia, Brazil	Meetings and legislative advice to facilitate accession to the Convention on Cybercrime
19–21 Mar 2007 ✓	Belgrade, Serbia	Regional conference for countries of south-eastern Europe on cooperation against cybercrime (funded by the PACO Serbia project on economic crime)
26-27 Mar 2007 ✓	Bucharest, Romania	Support to two training seminars for prosecutors (National Institute for Magistrates of Romania)
18-20 Apr 2007 ✓	South Africa	Meetings to promote the ratification of the Convention on Cybercrime and its Protocol and participation in the Symposium "Symposium on online security and the safety and welfare of South Africa's citizens" organised by Microsoft
23–24 Apr 2007 ✓	Philippines/ Asia and Pacific	Promotion of cybercrime legislation in line with the Convention on Cybercrime – Contribution to the Workshop on network security organised by the Asia-Pacific Economic Cooperation and ASEAN in Manila, Philippines
11 May 2007 ✓	Moscow, Russian Federation	Meeting on the implementation of the Convention on Cybercrime in the Russian Federation

14–15 May 2007✓	Geneva	Workshop on the Convention on Cybercrime within the framework of the WSIS follow up cluster of events at the ITU
May 2007✓	Strasbourg	Analysis of the draft law on cybercrime of the Philippines
18 June 2007✓	Dubai	Contribution to a regional meeting of states of the Gulf Cooperation Council (in cooperation with Microsoft)
11–12 June 2007✓	Strasbourg	Octopus Interface Conference on "Cooperation against cybercrime"
19-21 June 2007✓	Casablanca, Morocco	Training of prosecutors from northern Africa and the middle east – Contribution to the UNDP POGAR project
10 Sep 2007✓	New Delhi (India)	National conference on Cybercrime (in cooperation with ASSOCHAM)
12-14 Sep 2007✓	New Delhi (India)	Contribution to the Interpol Global Conference on Cybercrime
17 Sep 2007✓	Geneva (Switzerland)	ITU workshop
26-28 Sept 2007✓	Sao Paulo (Brazil)	ICCyber 2007: International Conference on Cybercrime
28 Sept 2007✓	Sao Paulo (Brazil)	Meeting with the Internet Steering Group of Brazil
28 Sept 2007✓	Sao Paulo (Brazil)	Training workshop for prosecutors
Oct 2007✓	Strasbourg	Launching of studies on cybercrime
1-2 Oct 2007✓	Colombia	National Workshop on Cybercrime Legislation
2 Oct 2007✓	Lyon (France)	Interpol European Working Party
5 Oct 2007✓	Geneva (Switzerland)	ITU High Level Expert Group meeting
9-11 Oct 2007✓	Washington DC (USA)	London Action Plan/ European Union Contact Network of Spam Authorities 3rd joint workshop
12 Oct 2007✓	Brussels	Meeting with eBay
22 Oct 2007✓	Paris	Study on cooperation between law enforcement and service providers: first meeting of the working group
24-26 Oct 2007✓	Heerlen (The Netherlands)	European Network Forensics and Security Conference
25-26 Oct 2007✓	Makati City (Philippines)	Legislators and Experts Workshop on Cybercrime
26-27 Oct 2007✓	Verona (Italy)	International conference "Computer crimes and cyber crimes: global offences, global answers"
29-31 Oct 2007✓	Jakarta (Indonesia)	Meetings on cybercrime legislation for Indonesia followed by a legislative analysis
5-9 Nov 2007✓	Bangkok (Thailand)	Policing Cyberspace International Summit
7-9 Nov 2007✓	Tomar (Portugal)	Contribution to the "Conference on Identity Fraud and Theft" organised by the authorities of Portugal within the context of the EU Presidency

7-9 Nov 2007✓	The Hague	Europol high-tech crime expert meeting
12-16 Nov 2007✓	Rio de Janeiro (Brazil)	Internet Governance Forum
15-16 Nov 2007✓	Brussels	European Commission expert conference on cybercrime
15-16 Nov 2007✓	Buenos Aires (Argentina)	Workshop on cybercrime legislation and accession to the Convention
19-20 Nov 2007✓	Washington DC (USA)	Organisation of American States
26-27 Nov 2007✓	Cairo (Egypt)	Regional conference on cybercrime
30 Nov-2 Dec✓	Courmayeur (Italy)	Contribution to United Nations ISPAC Conference on the Evolving Challenge of Identity-related Crime
8 Jan 2008✓	Geneva	Participation in ITU High Level Expert Group
29-30 Jan 2008✓	Kosovo	Legislative assistance workshop
7 Feb 2008✓	Düsseldorf, Germany	Study on law enforcement – service provider cooperation: 2nd meeting of the working group
11 Feb 2008✓	Brussels	Cyber Security Roundtable event 'Assessing the Threat of Cyber Security' (Security Defence Agenda, SDA)
19 Feb 2008✓	Tbilisi, Georgia	Legislative assistance workshop
20-21 Feb 2008✓	Montreux, Switzerland	McAfee cybersecurity meeting
20 Mars✓	Lille	2ème Forum International sur la Cybercriminalité
1-2 April 2008✓	Strasbourg	Octopus Interface Conference on cybercrime (to be followed by Cybercrime Convention Committee on 3-4 April 2007)
23-24 April 2008✓	Montenegro	Legislative assistance workshop
22 April 2008✓	Bosnia and Herzegovina	Legislative assistance workshop
9 April 2008✓	Kuala Lumpur, Malaysia	Meetings with the Government on cybercrime legislation and the Convention
10 April 2008✓	Singapore	Participation in Interpol-ASEAN cybercrime workshop
23 April 2008✓	Barcelona, Spain	CYBEX judicial training conference
16-17 April 2008✓	Dominican Republic	Workshop to review legislation and promote accession to the Convention (organised by Microsoft)
21-22 April 2008✓	Costa Rica	Meetings with government authorities on cybercrime legislation
13-15 May 2008✓	Port of Spain, Trinidad and Tobago	OAS/US DOJ regional workshop on cybercrime legislation in the Caribbean region
22 May 2008✓	Geneva	Participation in ITU High Level Expert Group
18-21 May 2008✓	Brisbane, Australia	Participation in AUSCERT cybercrime conference and meetings with Australian authorities
22 May 2008✓	Kuala Lumpur, Malaysia	IMPACT summit on cyberterrorism
26-27 May 2008✓	Tokyo, Japan	CECOS cybersecurity summit (Anti-Phishing Working Group)

28 May 2008✓	Brasilia, Brazil	Workshop on cybercrime legislation at the House of Representatives
4 June 2008✓	Vienna, Austria	OSCE: Presentation on cyberterrorism to the 32nd Joint Meeting of the Forum for Security Cooperation and the Permanent Council
4-6 June 2008✓	Reims, France	Cybercrime conference on a European reporting platform
9-10 June 2008✓	Egypt	Judiciary training workshop (in cooperation with Microsoft)
17-18 June 2008✓	The Hague	Europol meeting on the coordination of cybercrime training
18 June 2008✓	Luxembourg	Training of judges (in cooperation with Microsoft)
19 June 2008✓	Luxembourg	Conference "Cybercriminalité: réalités et solutions"
20 June 2008✓	London	Meeting on cooperation with the Crown Prosecution Service
23 June 2008✓	Ankara	Meeting on cybercrime legislation and accession by Turkey to the Convention on Cybercrime
26 June 2008✓	Geneva	HLEG meeting at the ITU
26/27 June 2008✓	Seoul, Korea	APEC meeting on cybercrime and terrorism
9-11 July 2008✓	Cotonou, Benin	Workshop for Western and Central African countries on cybercrime legislation and investigation (organised by the US DOJ)
22 July 2008✓	Buenos Aires, Argentina	Workshop on the new criminal legislation on cybercrime

2.2 Cooperation with countries and regions

2.2.1 Africa

Apart from cooperation with South Africa, Egypt and – to some extent – Morocco, cooperation between the CoE and Africa in cybercrime matters had been rather limited until mid-2008. The participation of representatives of the African Union Commission in the Octopus Interface Conference (Strasbourg, April 2008) was an important first step towards stronger cooperation.

From 9 to 11 April 2008, the US Department of Justice organised a regional workshop on cybercrime legislation and investigation for eleven countries of Western and Central Africa in Cotonou, Benin. The CoE contributed to this event.

The workshop proved to be very useful and timely in that it encouraged participants to further improve existing draft laws or to develop cybercrime legislation in line with the Convention on Cybercrime. Several countries indicated that accession to this treaty should be considered once legislation is in place or at an advanced stage.

Country	***Summary of recommendations made by participants***
1. Benin	Draft amendments to the Criminal Code and Criminal Procedure Code are before Parliament. Participants recommended that relevant provisions are reviewed to take into account the Convention on Cybercrime. The workshop was thus most timely.
2. Burkina Faso	A very early draft of a law on cybercrime is available. The criminal and criminal procedure codes will need to be reviewed in line with the Convention on Cybercrime.
3. Cameroun	A working group has developed a draft law with more than 100 articles. This draft should now be reviewed against the provisions of the Convention on Cybercrime, possibly with the support of the CoE
4. Congo (Brazzaville)	No legislation at present but review of criminal code and criminal procedure code underway. It was recommended that a working group be established to develop a specific law on cybercrime in line with the Convention with the support of the CoE. Accession to the Convention should be considered once the law is in place.
5. Gabon	No specific legislation in place at the moment. A special law on cybercrime should be developed in line with the Convention, an accession to the Convention should then be considered.
6. Ghana	A draft bill on cybercrime is available but should now be reviewed against the provision of the Convention. Accession to the Convention should be considered in the future.
7. Mali	No legislation available at present. A national law on cybercrime should be developed in line with international standards such as the Convention on Cybercrime.
8. Niger	A package of laws providing a legal framework for information and communication technologies has been prepared and is before Parliament. It is proposed that this package be analysed by the CoE. Accession to the Convention on Cybercrime should be considered
9. Nigeria	Several acts are in force covering a number of aspects related to cybercrime. A draft law on cybercrime is before the Parliament. This draft should be reviewed, possibly with CoE support to bring it fully in line with the Convention. An analysis of the draft had been provided by the CoE in January 2008.
10. Senegal	Existing and draft laws should be reviewed to cover gaps in national legislation. This should be guided by the Convention on Cybercrime.
11. Togo	No specific legislation in place. A working group should be established to develop a law on cybercrime in line with the Convention.

Immediately following the workshop a request for an analysis of a draft law was received from Niger.

A Pan-African conference is scheduled to take place in October 2008 in Abidjan (Ivory Coast) by the Organisation Internationale de la Francophonie in cooperation with the African Union Commission. This will allow follow up to the event in Benin.

Obviously, it is important that the momentum created through these events is supported through technical assistance. In July 2008, the African Union Commission and the CoE therefore developed a project proposal for a two-year project on cybercrime legislation in Africa which may help mobilise the necessary resources.

2.2.2 Arab region

The CoE contributed to a regional workshop on cybercrime for prosecutors of the Arab region (Casablanca, Morocco, 19 and 20 June 2007). This event was organised by the POGAR programme of the United Nations Development Programme. The event provided useful information regarding the state of cybercrime legislation in this region (Bahrain, Egypt, Jordan, Lebanon, Morocco, United Arab Emirates and Yemen) and generated interest in the Convention.

A Conference on Combating Cybercrime in countries of the Gulf Cooperation Council was held in Abu Dhabi on 18th June 2007. It was organised by the UAE Ministry of Justice in cooperation with Microsoft and with the participation of high-level officials. It was focusing on GCC approaches in the fight against cybercrime. A CoE consultant presented the Convention on Cybercrime which is reflected in the conclusions.

Some four hundred representatives from public and private sector institutions from the Arab region and other countries, and from non-governmental organizations and international bodies participated in the first regional conference on cybercrime held in Cairo on 26/27 November 2007. The Conference was held under the auspices of Ahmed Fathy Sorour, Speaker of Parliament of Egypt, and opened by Tarek Kamel, Minister of Communication and Information Technology. It was organized by the Egyptian Association for the Prevention of Information and Internet Crimes and supported by the Information Technology Industry Development Agency (ITIDA), the CoE, the United Nations Office on Drugs and Crime, Microsoft, Ain Shams University, IRIS, EASCIA and other partners.

In the declaration adopted at the closure of the Conference included a strong call on countries to implement the Convention on Cybercrime:

> *Participants note with appreciation the efforts underway in Egypt and other countries of the Arab region with regard to the strengthening of cybercrime legislation. These efforts should be given high priority and completed as soon as possible in order to protect societies in this region from the threat of cybercrime.*
> *The Budapest Convention (2001) on Cybercrime is recognized as the global guideline for the development of cybercrime legislation. Countries of the Arab region are encouraged to make use of this model when preparing substantive and procedural laws.*

2.2.3 Argentina

A CoE mission visited Buenos Aires on 15-16 November 2007. It consisted of a series of bilateral meetings with senior officials and counterparts and of a workshop organised with the support of the Law Faculty of the University of Buenos Aires.

The two main achievements were: strong support for the accession of Argentina to the Convention and a first review (followed by a discussion) of the cybercrime legislation with regard to the provisions of the Convention.

In spring 2008, the CoE was requested to review the draft laws amending the Criminal Code and the Criminal Procedure Code. On 5 June 2008, the Chamber of

Deputies (the Parliament) adopted the amendments to the Criminal Code which bring the substantive criminal law provisions much closer to the Convention on Cybercrime.

Discussions will now need to focus on amendments to the Criminal Procedure Code. On 22 July 2008, the CoE contributed to the "cybersecurity day" organised by the Ministry of Justice to disseminate information on the new law and to promote the reform of procedural law in line with the Convention on Cybercrime.

2.2.4 Australia

Participation of the CoE in the AUSCERT conference on 18-20 May 2008 helped establish a dialogue with the Australian authorities regarding possible accession of Australia to the Convention. This question is now under review at the Attorney General's Office in the light of possible amendments to national legislation that may become necessary.

2.2.5 Brazil

In February 2007, CoE helped the Federal Senate to review and improve the draft law on cybercrime. In June 2007, Senator Azeredo and his staff visited Strasbourg and participated in the Octopus Interface conference. At that stage the revised law was to be adopted by the Senate. However, in view of concerns expressed by service providers further hearings were to be organised.

In September, the CoE participated in an international conference on cybercrime investigations and cyber-forensics (ICCYBER, Sao Paulo, 26-28 September). That visit was also used for a round table discussion with the Internet Steering Group of Brazil which provided an opportunity for a dialogue between service providers, government and a representative of the Senate on the draft law.

The visit was furthermore used for a training workshop for specialised cybercrime prosecutors in Sao Paulo.

The dialogue with Brazilian authorities continued in 2008 with frequent exchanges on provisions of the draft law. A strong delegation from Brazil participated in the Octopus Interface Conference in Strasbourg in April 2008. The CoE contributed to a workshop organised by the Chamber of Deputies (Parliament) in May 2008.

On 9 July 2008, the Senate adopted the draft bill and submitted it to the Chamber of Deputies for adoption. If adopted, Brazilian legislation will be largely in line with the Convention on Cybercrime.

The next step would now be to encourage Brazilian accession to the Convention. Further discussions on this question are expected to take place in the second half of August.

2.2.6 Caribbean region

A "Cybercrime Legislation Drafting Workshop" for countries of the Caribbean was organised by the US Department of Justice and the Organisation of American States was held in Port of Spain, Trinidad and Tobago (13-15 May 2008). The CoE's Project on Cybercrime contributed to this event.

Several countries of this region are fairly advanced in terms of cybercrime legislation. The Commonwealth Model Computer Crime Law of 2002 – which is based on the Convention on Cybercrime – has been instrumental in this respect. Bahamas and Barbados seem to meet most requirements of the Convention already, and Dominica, Jamaica and St Vincent and the Grenadines have draft laws to that effect. All other participating countries appear to be committed to follow their example.

Country	***Status of legislation***
1. Antigua and Barbuda	A draft computer misuse act was developed in 2006 but was not further pursued
2. Bahamas	The Electronic Communications and Transactions Act 2003, and the Computer Misuse Act 2003 seem to bring the legislation the Bahamas largely in line with the Convention on Cybercrime
3. Barbados	The necessary legislation is in place and seems to fully meet the requirements of the Convention on Cybercrime, although the mutual legal assistance act would need to be amended in case of accession to the Convention
4. Belize	No legislation in place at present
5. Dominica	A draft law has been prepared – similar to Barbados – which would fully meet the requirements of the Convention. Further amendments to the MLA act would be required in case of accession
6. Grenada	No legislation in place but a draft is to be developed on the basis of the examples of Barbados and the Dominican Republic
7. Haiti	No legislation in place but a working group has been tasked to commence work on a cybercrime law
8. Guyana	No legislation in place but propose to start work following the workshop
9. Jamaica	A draft law has been prepared which would fully meet the requirements of the Convention
10. St Kitts and Nevis	Work on a draft law is underway and my be ready for submission to Parliament by the end of 2008
11. St Vincent and Grenadines	A draft law has been developed which seems to comply with the Convention
12. Surinam	No legislation in place but need to develop a cybercrime law in line with the Convention has been recognised
13. Trinidad and Tobago	A number of bills related to cybercrime (electronic transaction bill, data protection bill, child protection act) are expected to be passed in 2008. However, the computer misuse act of 2000 would need to be amended to close gaps and fully meet international standards

2.2.7 Colombia

In Colombia an interagency working group led by the Ministry of Foreign Affairs is working on a draft law on cybercrime. On 1-2 October 2007 a workshop was organised in Bogota to review this draft law with the help of CoE experts. This workshop was highly productive and resulted in specific recommendations for improvement. The working group subsequently prepared a revised version of the law (sent to the CoE on 23 November 2007) and will now engage in a dialogue with the Congress on this matter.

As a result of the workshop, the Colombian authorities will also consider acceding to the Convention.

In September 2008 the Colombia will host a regional workshop of the Organisation of American States and the CoE on cybercrime legislation for Latin American countries. This is expected to add impetus to the reform of cybercrime legislation within Colombia.

2.2.8 Dominican Republic

In May 2007, the Dominican Republic adopted Law 53/07 on cybercrime which brings the substantive and procedural law of this country in compliance with the Convention on Cybercrime. In April 2008, the Dominican Republic expressed their willingness to accede to the Convention on Cybercrime, and the procedure in line with article 37 is now underway.

On 16 April 2008, a conference was held in Santo Domingo with the support of Microsoft on the "integration of the Dominican Republic in the Convention on Cybercrime". This event provided clear indications that Law 53/07 is applied in practice as reflected in a number of investigations, prosecutions and cases before court.

2.2.9 Georgia

A workshop on cybercrime legislation was held in Tbilisi on 19 February 2008. An concrete outcome of this event was the signing of the Convention on Cybercrime by Georgia on 1 April 2008. Follow up will now be required in order to bring Georgian legislation in line with the Convention.

2.2.10 Egypt

In February 2007, a CoE mission had visited Cairo and in May 2007 the CoE submitted a written analysis on the compliance of the Draft Law of Egypt "Regulating the Protection of Electronic Data and Information and Combating Crimes of Information" with the requirements of the CoE Convention on Cybercrime.

In order to add momentum, the CoE supported a Conference on Cybercrime in Cairo on 26-27 November 2007 (see above).

However, it seems that the Egyptian authorities are now considering creating separate laws on data protection and on cybercrime.

In June 2008, the CoE contributed to two training workshops for judges organised by the Ministry of Justice and Microsoft. The objective of the event was to provide judges with an introduction to cybercrime and cybercrime-related investigation. The training was designed as two identical one-day training sessions. Some 120 judges participated in total.

2.2.11 India

Following a mission to New Delhi from 21 to 23 February 2007, a detailed analysis of the draft amendments to the Information Technology Act was sent to the Standing Committee on Information Technology of the Parliament in March 2007. The Parliament subsequently organised further hearings and sent its report back to the Government in the beginning of September. The report reflects some of the observations made by CoE experts and makes reference to the Convention on Cybercrime. It is now up to the Government whether to accept these changes and incorporate them into a new version.

In order to continue the dialogue in this matter, the project supported a national conference on cybercrime which was held in Delhi in September 2007 in cooperation with the Associated Chamber of Commerce and Industries of India (ASSOCHAM). Microsoft and eBay also supported this event.

In December 2008, India will host the Internet Governance Forum which will be held in Hyderabad (3-6 December 2008). This event may help may encourage the finalisation of the draft law and discussions on the accession to the Convention by India.

2.2.12 Indonesia

A CoE mission visited Jakarta from 29 October to 1 November 2007. The visit was facilitated by Microsoft Indonesia. It focused on the "Draft Act on Information and Electronic Transactions" with its Chapter VII on Prohibited Actions and Chapter XI on Interrogation, Prosecution and Examination in the Session of Court.

Following the visit, the CoE prepared a written analysis a written analysis of the draft Act against the provisions of the Convention in December 2007 and also translated the Convention into Bahasa.

In March 2008, the Indonesian Parliament adopted the Act on Information and Electronic Transactions which brings Indonesian legislation closer to the Convention on Cybercrime. A number of proposals made by CoE experts were taken into account.

Important progress was thus made in Indonesia. A detailed analysis should now be carried out to see to what extent the new law and other legislation in force cover the provisions of the Convention. Such an analysis could point at further work required and also initiate discussions on a possible accession of Indonesia to the Convention.

2.2.13 Nigeria

Representatives of Nigeria participated in the Octopus Conference in June 2007.

In December 2007 the CoE prepared an analysis of the draft law on cybercrime. This review suggests that with some adjustments to most articles this draft could become a solid law fully in line with the Convention.

In July 2008 this was further discussed with representatives of Nigerian authorities who pledged to consider a further review of the draft law in cooperation with the CoE.

2.2.14 Philippines

In April 2007, the CoE participated in a meeting on cybersecurity organised by the Asia Pacific Economic Cooperation (APEC) and ASEAN in Manila. In the course of this event, the CoE was requested by the authorities of the Philippines to review the draft law on cybercrime.

In early June, a detailed analysis was sent to Manila, and in the same month the Philippines participated in the Octopus Conference on Cybercrime in Strasbourg.

As a result, in September 2007 the Philippines sent a letter to the Secretary General of the CoE requesting accession to the Convention on Cybercrime. In May 2008, the Philippines were formally invited to accede to the Convention.

On 25-26 October 2007 in Makati City (Manila), a workshop was organised by the Department of Justice, the Commission for Information and Communication Technology (CICT) of the Philippines and the CoE with the support of Microsoft in which some 60 representatives from public and private institutions participated. Workshop discussions resulted in a number of proposals for further improvements.

By June 2008, a draft of the law was before Parliament for review. However, at the same time the Department of Justice and the CICT were in the process of preparing a consolidated version of the draft taking into account suggestions by the CoE (including comments sent November 2007 and June 2008) and other stakeholders for consideration by Parliament.

2.2.15 Romania

Support to the National Cybercrime Training Conference in Romania (Pitesti, 27-29 November 2006): The project provided limited co-financing to a conference in Romania organised by the Ministry of Interior for police investigators, prosecutors and judges (Pitesti, Romania, 27-29 November 2006). Some 100 investigators, prosecutors and judges from different regions of Romania have been trained in order to allow them to implement the cybercrime legislation adopted in 2004 when Romania ratified the Convention on Cybercrime. This event received strong international backing as reflected in the participation of foreign law enforcement officials (in particular the USA), representatives from the private sector (including Microsoft), from EUROPOL and the CoE. Romania has taken important steps against cybercrime in terms of adopting legislation (in 2004), and establishing specialised services within the Ministry of Interior and the Prosecution. Further training, in particular of judges, will be required.

The training conference at the National Institute of Magistrates (26-27 March 2007, Bucharest, Romania) was a follow up to the one held in 2006. Participants were judges, prosecutors and those experts that were selected to work as trainers in further cybercrime training activities. The presentation of the CoE expert was related to the Convention on Cybercrime with a focus on the substantive criminal law provisions.

A further training event for judges and prosecutors is envisaged for January 2009.

2.2.16 Russian Federation

The Russian Federation has not yet signed the Convention due to concerns related to Article 32. A CoE mission visited Moscow in May 2007 to provide explanations regarding this article and subsequent discussions took place in Strasbourg. These clarifications seemed satisfactory and should help the Russian authorities make progress towards signature and ratification of the Convention.

2.2.17 Serbia

The CoE provided intensive supports to Serbia in view of the preparation of cybercrime legislation, the strengthening of law enforcement and criminal justice capacities to investigate and prosecute cybercrime, the promotion of international cooperation and accession to the Convention on Cybercrime.

These activities were not funded by the Project on Cybercrime but by the PACO Serbia project against economic crime of the CoE and the European Agency for Reconstruction which ended in May 2008.

Activities included the organisation of a regional conference on cybercrime (see below), the preparation of a "Manual Tool on the Investigation of Cybercrime" for the law enforcement and the judiciary, an expertise on the harmonisation of the provisions of the Serbian Criminal Code and Criminal Procedure Code with international standards in the field of cybercrime followed by a roundtable with working group members and relevant Serbian counterparts to present and discuss the results, the participation of Serbian experts and practitioners in the Octopus Conference on Cybercrime organised by the CoE in June 2007, two one-week technical trainings on cybercrime for a total of 80 practitioners and the participation of six representatives (from the Ministries of Interior and Justice, the Administration for the Prevention of Money Laundering (FIU), District Court and Prosecution Office) in the international seminar on combating the financing of terrorism (Switzerland, 15 – 17 October 2007).

Additional specialised training sessions were organised for practitioners on topics such as forensic investigation, computer emergency response team and investigation child exploitation between January and April 2008.

2.2.18 South Africa

In April 2007, a CoE mission visited South Africa to discuss the state of implementation of the Convention on Cybercrime and to contribute to a symposium on internet safety and child exploitation organised by Microsoft.

South Africa participated in the elaboration of these instruments and signed the Convention in November 2001. However, the Protocol has not yet been signed and the Convention not yet ratified. The visit helped to put these back on the agenda of the Department of Justice so that ratification of the Convention and signature of the Protocol can be expected in the near future.

The South African authorities are of the opinion – confirmed by a number of successful investigations – that the minimum legal basis is available following the adoption of the Electronic Communication and Transactions Act 25 of 2002 and the

Regulation of Interception of Communications and Provision of Communication-related Information Act 70 of 2002:

Chapter XIII of the Electronic Communication and Transactions Act 25 of 2002 criminalises "unauthorized access to, interception of or interference with data" – this includes misuse of devices (Section 86), "computer-related extortion, fraud and forgery" (Section 87) and "attempt, and aiding and abetting". While the ECTA defines these criminal offences, many other provisions of this Act remain to be implemented, including the appointment of cyber inspectors (Chapter XII) with far reaching investigative powers. In practice the SAPS applies the Criminal Procedure Code and other Acts to investigate cybercrime. The main provision missing appears to be the possibility of expedited preservation of data.

Child pornography is covered by the Film and Publications Act 1996. It includes the impression that a person is a minor as well as morphed images.

These provisions should allow South Africa to ratify the Convention and the Protocol but over time the legislation may nevertheless need to be improved.

In April 2008, the Minister of Justice visited the CoE in Strasbourg and signed the Protocol on Xenophobia and Racism. This will now allow the authorities to move towards ratification of both instruments.

2.2.19 South-eastern Europe

A regional conference on cybercrime was held in Belgrade from 19 to 21 March 2007 within the framework of the PACO Serbia project on Economic Crime. Representatives from 16 countries and from international organisations and private sector bodies participated. Participants discussed the current state of cybercrime legislation, the functioning of international cooperation against cybercrime, including the creation of 24/7 points of contact, questions related to the investigation and prosecution of cybercrime as well as to public-private partnerships.

On 17-18 December 2007, a regional workshop on cybercrime legislation and the training of judges was organised in Plovdiv, Bulgaria, with the participation of judges, prosecutors and ministerial officials from Bulgaria, Romania, Serbia and "the former Yugoslav Republic of Macedonia". It encouraged countries to further improve their legislation. With regard to the training of judges the workshop concluded that:

> The training needs of judges and the types of training to be delivered should be identified and defined more precisely (initial for many or advanced training for a few, national or international, external or national or in-house expertise, external trainers or training of trainers).

It was agreed, among other things, that the CoE – in cooperation with other organisations – should organise further events for judges and develop training materials for standard courses.

With regard to legislation, as a follow up to the workshops in Belgrade workshop (March 2007) and Plovdiv (December 2007), legislative assistance workshops were held in:

- Kosovo (January 2008)
- Bosnia and Herzegovina (April 2008)
- Montenegro (April 2008).

2.2.20 Ukraine

Within the framework of the Project on International Cooperation in Criminal Matters in Ukraine (UPIC) of the CoE and the European Commission, the CoE organised an international conference on cooperation against cybercrime in Kyiv, Ukraine on 6-7 February. Representatives from Estonia, France, Italy, Latvia, Lithuania, the Russian Federation, the Netherlands, Romania and Ukraine, international organisations and private sector bodies participated in this event.

In Ukraine the harmonisation of national legislation with the Convention still needs to be completed with regard to some substantive and procedural provisions. The rights, authorities and obligations of both law enforcement authorities and service providers, including the liability of legal persons and provisions for the expedited preservation of data, would need to be further clarified in order to facilitate public-private cooperation. The issues in question have been identified and should be addressed by the Ukrainian authorities responsible.

With regard to the investigation and prosecution of cybercrime, there is an obvious need for specialisation and the establishment of cybercrime or high-tech crime units as reflected in the examples of France, Italy and Romania presented during the conference. In Ukraine, a wide range of cybercrime have been investigated and referred to court. However, the capacities of existing units would need to be further strengthened.

The establishment of 24/7 points of contact is considered a very useful way of facilitating international cooperation as shown by the experience of the G8 24/7 Network and as required under Article 35 of the Convention on Cybercrime. However, by July 2008, Ukraine had not yet established such a contact point although it is already party to the Convention.

2.3 Cooperation with other organisations

2.3.1 Global: Octopus Interface conference on "Cooperation against Cybercrime" (Strasbourg, June 2007)

More than 140 cybercrime experts from some 55 countries, international organisations and the private sector met at the CoE in Strasbourg from 11 to 12 June 2007 to:

- analyse the threat of cybercrime
- review the effectiveness of cybercrime legislation
- promote the use of the Cybercrime Convention and its Protocol as a guideline for the development of national legislation and encourage wide and rapid ratification and accession to these treaties

- strengthen cooperation among different initiatives by enabling stakeholders to make better use of existing opportunities and to explore new ones.

A comprehensive set of recommendations was adopted at the closure of the Conference. The event provided a platform for a wide range of organisations and initiatives to share experience and good practices. These included the Internet Governance Forum, Digital Rights Europe, European Commission, ENISA, Organization of American States, Interpol, Asia Pacific Economic Cooperation, InHope, International Centre for Missing and Exploited Children, Organisation of the Islamic Conference, and the United Nations Development Programme. Private sector initiatives and representatives included Microsoft, Anti-Phishing Working Group, FIRST/CERT USA, London Action Plan and others.

One workshop was organised jointly with the G8 High-tech Crime Subgroup with the participation of 24/7 points of contact from more than 25 countries.

The event added considerable momentum and credibility to the anti-cybercrime efforts of the CoE.

2.3.2 Global: Octopus Interface conference on "Cooperation against Cybercrime" (Strasbourg, 1-2 April 2008)

On 1-2 April 2008, preceding the 3rd meeting of the Cybercrime Convention Committee (T-CY) on 3-4 April, a follow up global conference was held at the CoE in Strasbourg.

More than 210 participants from 65 countries and a wide range of private sector, public, civil society and international organisations took part in this event.

The Conference:

- discussed current and expected cybercrime threats and trends such as malware, identity theft and other forms of fraud, botnets and denial of service attacks, child pornography and abuse, and the implications of social networks and of technologies such as Voice over Internet Protocol and next generation networks
- reviewed the effectiveness of cybercrime legislation. In this connection, a clear global trend was noted in that countries all over the world are strengthening their legislation using the Convention on Cybercrime as a guideline
- discussed measures to enhance the effectiveness of international cooperation, including 24/7 points of contact and improved coordination at national levels. It was agreed that the CoE and the G8 High-tech Crime Subgroup maintain a joint directory of contact points (the merger of the Directory was subsequently approved by the Cybercrime Convention Committee on 3-4 April)
- adopted guidelines for the cooperation between law enforcement and internet service providers in the investigation of cybercrime. These guidelines can now be disseminated all over the world in order to help law enforcement and ISPs structure their cooperation
- underlined the need to ensure an appropriate balance between the need to enhance security of information and communication technologies and the need to strengthen the protection of privacy, personal data, freedom of expression and other fundamental rights.

The increased number of participants, countries and other institutions is an indicator of the level of cooperation that the Project on Cybercrime has been able to generate. The Conference helped intensify existing cooperation with countries and organisation, and initiate new cooperation, for example, the African Union Commission.

The conference received wide media coverage which shows that the topics covered were highly relevant. The media coverage in turn helped further promote measures to enhance the security of ICT and the Convention on Cybercrime.

The adoption of the guidelines on law enforcement – Internet service provider cooperation was one of the main results of the Conference. These guidelines had been drafted between October 2007 and March 2008) by a working group consisting of industry (Microsoft, eBay, EuroISPA, service provider associations of France and Germany and others) and law enforcement representatives (from France and Germany). The draft was discussed in detail during the Conference and finalised and adopted by the Conference on 3 April.

2.3.3 Anti-Phishing Working Group

The Anti-Phishing Working Group has been participating in a number of activities carried out under this project (meeting on identity theft in Portugal in November 2007, Octopus Interface Conferences in June 2007 and April 2008). The CoE in turn co-sponsored the "Counter e-Crime Operations Summit" of the APWG in Tokyo, Japan, on 26-27 May 2008. This provided an excellent opportunity to further strengthen cooperation with the private sector in activities related to the Convention on Cybercrime.

It also helped promote the ratification of the Convention on Cybercrime by Japan. Japan signed the Convention in 2001 but amendments to cybercrime legislation are part of a law package that is still before Parliament. However, the authorities remain committed to ratifying the Convention.

2.3.4 Asia and Pacific Economic Cooperation and ASEAN

The CoE was invited to present the Convention on Cybercrime at an APEC/ASEAN workshop on cybersecurity during the 35th meeting of the telecommunication working group of the APEC in Manila, Philippines, April 2007. This generated interest among countries of South-east Asia with an immediate request for legislative assistance from the Philippines. This later on resulted in a request for accession to the Convention by the Philippines.

It opened the door for further cooperation with ASEAN and its member states. In April 2008, for example, discussions were held with the authorities of Malaysia. An ASEAN workshop on cybercrime legislation – with CoE participation is foreseen for October 2008.

The CoE also contributed to a cybercrime training workshop organised by ASEANAPOL in Singapore on 10 April 2008.

Cooperation with APEC continues. In June 2008, the CoE sent a speaker to an APEC event on cyberterrorism in Seoul, Korea.

2.3.5 European Network Forensics and Security Conference

The CoE was invited to participate with a keynote speaker in this first conference organised by Zuyd University, Netherlands, from 24 to 26 October 2007 which gathered many experts from the law enforcement, academics, senior managers from companies such as Capgemini or Symantec and other high-tech firms.

2.3.6 European Union (Portuguese Presidency) and European Commission

From 7 to 9 November 2007, the Ministry of Interior of Portugal held a conference on "Identity fraud and theft – the logistics of organised crime" (Tomar, Portugal) within the framework of the Portuguese EU Presidency. The CoE was invited to sponsor a workshop on "Cybercrime and identity theft". The conference showed the importance of the Convention on Cybercrime for the investigation and prosecution of identity theft involving computer systems. It provided an opportunity to remind EU member States to speed up the ratification of the Convention as less than half of them have actually done so to date.

Participation in this event was also important in view of the proposal of the European Commission to develop legislation on identity theft (see Communication on Cybercrime of May 2007) and the activities of the United Nations Office on Drugs and Crime regarding identity theft.

The Communication on Cybercrime of the European Commission (May 2007) and the Council Conclusions of 8/9 November 2007 expressing strong support to the Convention on Cybercrime in Europe and elsewhere around the world is a good basis for stronger cooperation between the CoE and the European Commission.

> *2827th Council meeting*
> *Justice and Home Affairs*
> *Brussels, 8-9 November 2007*
>
> *4) Underlines the confidence placed in the Council of Europe Convention of 23 November 2001 on Cybercrime, supports and encourages implementation of the measures thereof and calls for the widest possible participation by all countries;*
> *5) Attaches the greatest importance to promoting cooperation with non-member countries in preventing and combating cybercrime, more specifically , given the pivotal role of the Council of Europe Convention on Cybercrime by supporting the introduction of that globally oriented legal framework, in liaison with the Council of Europe, especially in countries where development and technical assistance is being provided;*

The CoE participated in the cybercrime conference organised by the European Commission in Brussels on 15-16 November. The meeting underlined the need to implement the Convention. It also referred to the need for law enforcement – service provider cooperation in cybercrime investigations (and the respective study underway under the auspices of the CoE) and the network of 24/7 contact points.

The European Commission in turn participated actively in the Octopus Interface Conference in April 2008, and invited the CoE to it's the EC meeting on cybercrime on 25-26 September 2008.

This indicates that the European Commission and the CoE increasingly coordinate their activities related to cybercrime.

2.3.7 Europol

Europol participated in the Octopus Conference in June 2007 and in April 2008. The cybercrime threat assessment released by Europol in August 2007 ("High-tech Crimes within the EU") includes a recommendation regarding the implementation of the Convention on Cybercrime and acknowledges the Octopus Interface conferences as a platform for cooperation among different stakeholders.

The CoE participated in the annual Europol High Tech Crime Expert meeting in The Hague from 6 to 8 November 2007 which gathered i.a. experts from most of the EU member States, the EC, USA, Interpol, private companies (Microsoft, eBay, Paypal, Skype) and specialised telecom companies (KPN).

The CoE also participated in the meeting on coordination of cybercrime training within the European Union held in The Hague on 17-18 June 2008.

2.3.8 24/7 Network of contact points and G8 High-tech Crime Working Group

The Convention on Cybercrime foresees the establishment of contact points which should be available 24 hours a day, 7 days a week in order to facilitate international cooperation in cybercrime investigations. The respective provision of the Convention is based on the experience of the G8 Network of Contact Points which was created in 1997 and currently comprises some 50 countries.

The project supported the 2nd Training Conference of the G8 Network of 24/7 contact points (Rome, 17-19 October 2006) and sponsored the participation of representatives from Bulgaria, Romania, Turkey and Ukraine in this event. The Conference included a session on the Convention on Cybercrime and thus helped promote this treaty among some 50 European and non-European countries. The meeting furthermore helped clarify that the 24/7 contact points of the G8 network should be consistent with those established under the Convention. The meeting thus strengthened the common understanding of the G8 and the CoE on this question.

The Octopus Interface Conferences of June 2007 and April 2008 also included workshops for contact points which were jointly organised with the G8 High-tech Crime Working Group and which resulted in a proposal to merge the directories of contact points of the CoE with that of the G8. This proposal was agreed upon in November 2007 and confirmed by the Cybercrime Convention Committee (T-CY) in April 2008. Specific details and procedures now need to be elaborated regarding the maintenance of the directory.

The T-CY also tasked the Project on Cybercrime to prepare a study on the effectiveness of 24/7 points of contact as well as on a checklist for expedited preservation requests.

2.3.9 IMPACT

The International Multi-lateral Partnership against Cyber-Terrorism (IMPACT) is an initiative of the Prime Minister of Malaysia. The first meeting of IMPACT was held in Kuala Lumpur, Malaysia, from 20 to 22 May 2008. The CoE was invited to present the Convention on Cybercrime.

IMPACT is to have four functions:

- Training & Skills Development – In collaboration with leading global ICT companies, IMPACT will conduct highly specialised training, seminars etc. for the benefit of member governments

- Centre for Security Certification, Research & Development – MPACT will function as an independent, internationally-recognised, voluntary certification body for cyber-security. In consultation with member governments and leading ICT companies, IMPACT will extract and formulate a checklist of some of the global best practices for the purpose of creating an international benchmark

- Global Emergency Response Centre – IMPACT will build up its expertise to be the foremost cyber-threat resource centre for the global community. IMPACT will establish an emergency response centre to facilitate swift identification and sharing of available resources to assist member-governments during emergencies

- Centre for Policy, Regulatory Framework & International Co-operation – Working with partners such as Interpol, EU, ITU etc., the Centre contributes towards formulation of new policies and work towards harmonisation of national laws to tackle a variety of issues relating to cyber threats e.g. cyber crimes. Provides advisory services to member-governments on policy and regulatory matters.

The meeting comprised some 150 participants from 30 different countries and the private sector representing a diverse set of institutions. It included Ministers, or Secretaries of State from Algeria, Brunei, Cambodia, Ghana, India, Iran, Laos, Malaysia (Prime Minister), Myanmar, Philippines, Singapore, Tunisia and Vietnam. The private sector was strongly represented, including senior private sector representatives from Google, Kaspersky Lab, ICANN, F-Secure and others. Apart from the International Telecommunication Union, only the CoE participated as an international organisation.

Some concern was expressed regarding the notion of "cyber-terrorism" and it was proposed to replace it with the term "cyber-threats". While the further course of action and the working procedures of this initiative remain to be defined, there was broad consensus that with regard to legislation, IMPACT intends very much to rely on the Convention on Cybercrime.

2.3.10 International Telecommunication Union

The World Summit on the Information Society tasked the ITU among other things with facilitating follow up on matters related to cybersecurity. The CoE thus contributed to the follow up meeting held in Geneva in May 2007. This involved a specific workshop on the Convention on Cybercrime and the facilitation of panel discussions.

During the same event, the Secretary General of the ITU presented his Global Cybersecurity Agenda and, among other things called for the development of model laws to ensure interoperability in the absence of international legal frameworks. The CGA is silent about the Convention on Cybercrime.

In October 2007, the ITU established a High-level Expert Group to advise the Secretary General of the ITU with regard to the cybersecurity strategy. The CoE was invited to participate in the work of the HLEG. The group completed its work in June 2008. The technical reports prepared by this group make extensive reference to the Convention on Cybercrime and suggest that countries use it as a guideline for their own legislation and consider accession to it.

During its last meeting on 26 June 2008 – as the group could not reach consensus on the overall recommendations – the chairman of the HLEG was tasked to prepare a report with his recommendations to be addressed to the Secretary General of the ITU.

2.3.11 Internet Governance Forum

The CoE actively participated in the 2007 IGF event (Rio de Janeiro, 12 – 16 November 2007) with two meetings specifically dedicated to cybercrime:

- a best practice forum on the Convention
- a workshop on legislative responses to current and future cyber threats.

The CoE made use of high profile experts from Europe, Asia, South-America and Africa to make presentations or participate as key persons in open discussions. This resulted in having the Convention not profiling itself as a "European" one only but as a global instrument supported on all continents. Both activities gathered a total of about 300 participants from all over the world.

The next IGF will be held in Hyderabad, India, from 3-6 December 2008. The CoE proposed a number of workshops and best practice fora on topics related to cybercrime, international cooperation, freedom of expression, data protection and law enforcement – service provider cooperation.

2.3.12 Interpol

The CoE and Interpol cooperated on a number of occasions. Among other things, the CoE participated in the October meeting of the European Working Group on High-tech Crime in Lyon.

An important event was the 7th International Conference on Cybercrime, a global meeting organised by Interpol in New Delhi, India, from 12 to 14 September to which the CoE contributed. The meeting adopted a set of recommendations of which the first one was related to the Convention on Cybercrime:

The delegates at the 7th International Conference on Cyber Crime recommend:

- That the Convention on Cyber Crime of the Council of Europe shall be recommended as providing the international legal and procedural standard for fighting cyber crime. Countries shall be encouraged to join it.

2.3.13 London Action Plan

The CoE took part in the 3rd Joint LAP-CNSA (EU Contact Network of Spam Authorities) Workshop organised in Washington DC from 9 to 11 October 2007. In particular, a session on "cross-border enforcement cooperation - leveraging resources of international enforcement networks" moderated by the US Federal Trade Commission allowed the CoE to make a presentation on the Convention focusing on its provisions facilitating cooperation at the international level. Other bodies represented in the panel included the US Department of Justice, Office of the Privacy Commissioner of Canada, CNSA and Microsoft.

The Committee of Ministers of the CoE approved on 7 November 2007 the request for CoE observer status to the LAP. In the coming months, this will allow CoE to develop closer cooperation and activities with the LAP: awareness raising among private companies and internet service providers, exchange of good practices, trainings for law enforcement and judiciary, implementation of procedures enhancing international cooperation.

The LAP intends to discuss the guidelines on law enforcement – service provider cooperation at its meeting in Germany in October 2008.

2.3.14 Organisation of American States

The OAS had supported the implementation of the Convention on Cybercrime among its 34 member states for some years. The CoE participated in the meeting of the Group of Experts on High-tech Crime in Washington on 19-20 November 2007. The meeting provided clear indications of the progress made in this region (in countries such as Argentina, Brazil, Colombia).

Moreover, basic agreement was reached to hold joint OAS/CoE events on cybercrime legislation for OAS countries in 2008.

As follow up, the CoE contributed to the OAS/USDOJ workshop in the Caribbean (May 2008). The methodology used during this event permitted to the legislation of participating countries in some detail and identify needs for further reform. Based on this experience, a joint OAS/CoE workshop on cybercrime legislation for 18 countries of Latin America is scheduled for 3-5 September 2008 in Bogota, Colombia.

Thus, discussions on OAS/CoE cooperation have led to specific activities and support to OAS member states.

2.3.15 POLCYB

The Society for the Policing of Cyberspace (POLCYB), was incorporated as a not-for-profit society in June 1999. Based in British Columbia, Canada, its goal is to enhance international partnerships among public and private professionals to prevent and combat crimes in cyberspace (see http://www.polcyb.org)

The 7th Annual Policing Cyberspace International Summit 2007, which took place in Bangkok, Thailand from 5 to 9 November 2007, was organised by POLCYB in co-operation with the International Law enforcement Academy (ILEA), Bangkok and the CoE. The Summit was also supported by the private sector.

The Summit brought together over 100 participants working both in the public sector, in particular law enforcement, and in the private sector to discuss "International policing and policy perspectives on countering cybercrime." During the first three days discussions centred on a number of matters such as international collaboration, digital evidence prosecutions, child exploitation, investigations, malware and emerging technologies. Discussions on digital evidence training took place during the last 2 days.

The importance of the Convention on cybercrime was recognised during the discussions and it was agreed that there was a great need to improve the laws and procedures of States in particular in the light of the standards contained in the Convention on cybercrime.

The next POLCYB meeting will be held in November 2008, again in Bangkok.

2.3.16 United Nations Office on Drugs and Crime

The CoE and UNODC cooperated constructively with each other. Among other things, the CoE facilitated the participation of UNODC in the conference on identity theft organised by the authorities of Portugal (Tomar, November 2007) and contributed to an event on identity theft held in Courmayeur, Italy, at the end of November 2007. In turn, the CoE was invited to participate in a core group of experts on identity theft of UNODC (Courmayeur, Italy, 29 November – 2 December 2007). UNODC furthermore participated in the working group preparing guidelines for law enforcement – ISP cooperation.

There is certainly scope for even further cooperation with UNODC in cybercrime matters in2008.

2.4 Studies

In October 2007, five studies were launched under the Project on Cybercrime. They were completed in time for the Octopus conference and the Cybercrime Convention Committee April 2008:

1. Cybercrime situation report ("Current threats and trends and the adequacy of the international response")	The study provides an up-to-date analysis of current cybercrime threats and trends.
2. Study on cybercrime legislation ("Legislation implementing the Convention on Cybercrime: comparative analysis of good practices and effectiveness")	The study serves as a resource for countries that are in the process of strengthening their national legislation against cybercrime in line with the Convention. The study was carried out by a research institute in Verona, Italy.
3. Study on the role of service providers ("Cooperation between service providers and law enforcement against cybercrime: towards common guidelines?")	The study was aimed at facilitating the cooperation between service providers and law enforcement in the prevention and investigation of cybercrime. It included a proposal for common guidelines for such cooperation for further discussion at the cybercrime conference on 1-2 April 2008. The guidelines were discussed, finalised and adopted on that occasion.
4. Study on international cooperation ("The effectiveness of international cooperation against cybercrime: examples of good practice")	The study is to help countries make better use of the international cooperation provisions of the Convention on Cybercrime, including Article 35 on 24/7 points of contact. It was carried out by an expert from Portugal. A follow up report will be prepared in the second half of 2008 focusing on the effectiveness of 24/7 points of contact.
5. Study on data protection ("Investigating cybercrime and the protection of personal data and privacy")	The purpose of the paper is to give guidance to countries as to how to make cybercrime investigations compatible with data protection and privacy concerns (in particular when implementing the procedural provisions of the Convention on Cybercrime). The study was carried out by a researcher from the Netherlands. The question of data protection and privacy is again moving higher on the agenda, and this study is thus very timely.

These studies fed into discussions at the Octopus Conference and the T-CY meeting in the first week of April 2008 and are used within the framework of different project activities. In particular the guidelines on law enforcement – service provider cooperation are a very practical result; and they are already being disseminated in different countries and fora.

3 Results

Project objective: *To promote broad implementation of the Convention on Cybercrime (ETS 185) and its Protocol on Xenophobia and Racism (ETS 189)*

The Project on Cybercrime since its inception in September 2006 helped establish the Convention as the primary reference standard for cybercrime legislation globally. This is reflected among other things in the recognition that the Convention received at the Internet Governance Forum, Interpol, Europol, the European Union and the European Commission, the Organisation of American States, Asia Pacific Economic Cooperation, the United Nations Office on Drugs and Crime, the African Union Commission and others. Furthermore this is reflected in the ever stronger cooperation with the private sector (in particular Microsoft) and other initiatives such the Anti-Phishing Working Group, the London Action Plan, POLCYB, ICCYBER or AusCERT.

The first six months of 2008 have seen a further confirmation of this trend with activities now also covering countries of the Caribbean and Africa.

The Project interacts very well with the Cybercrime Convention Committee (T-CY) in that it provides substantive inputs and ensures follow up to T-CY decisions. The global Octopus Interface conferences are organised back-to-back with T-CY meetings.

3.1 Output 1: Legislation

Legislation implementing the Convention on Cybercrime and its Protocol on Xenophobia and Racism (draft laws meeting the standards of ETS 185 and 189 available in at least 10 European and 5 non-European countries)

In Argentina and Indonesia cybercrime laws were adopted by Parliament in the first half of 2008, and in Brazil the adoption of the new law is expected shortly. The Philippines were invited to accede in May 2008 and the draft law is now before Parliament. The Dominican Republic adopted a law in 2007 and requested accession to the Convention during the Octopus Interface Conference in April 2008. These are major achievements.

Since the inception of the project, the Convention on Cybercrime was presented to representatives from more than 150 countries around the world through different types of meetings.

Specific advice on draft laws was provided to:

- Argentina
- Brazil
- Colombia
- Egypt
- India
- Indonesia
- Nigeria
- Pakistan
- Philippines
- Serbia.

A further request for a legislative analysis was received from Niger in July 2008.

A regional workshop in the Caribbean helped review the legislation of 14 countries of that region in some detail, and a similar event in Benin allowed a review of the legislation of 11 African countries.

In order to facilitate the analysis of cybercrime legislation against the provision of the Convention, "profiles" have been prepared for more than 40 countries of which 30 had been published by July 2008. The profiles for European countries that have ratified the Convention were reviewed in November 2007 and now serve as bases for in-country workshops which are aimed at further improving cybercrime legislation.

The Dominican Republic and Sri Lanka adopted new legislation in 2007 with the Dominican Republic following very closely the Convention. Legislative work guided by the Convention is furthermore underway in many other countries.[1] Interest for assistance to the review of legislation has also been expressed by many other countries from around the world.

In sum, the legislative processes that the project was able to support and initiate since its launching in 2006 exceeded expectations, in particular considering that with many of the non-European countries, the CoE had little contact before. The Convention is used as a guideline or "model law" now in more than 90 countries.

In terms of additional ratifications by European countries, the progress made has been less satisfying although legislative work is underway in many of them. While in 2006 seven countries deposited the instrument of ratification, in 2007 only three additional countries became parties to the Convention. In the first half of 2008 Slovakia and Italy also ratified and Azerbaijan and Georgia signed it.

Nevertheless, almost half of the European Union member States still need to ratify this Convention. The call for ratification of the EU Justice and Home Affairs Council of November 2007 may help accelerate this process. Six member States of the CoE have not yet signed the Convention.

Ratification of the Convention on Cybercrime since November 2001

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

Regarding the Protocol on Xenophobia and Racism the number, four additional countries ratified this instrument in 2007. In the first half of 2008, Croatia and Norway also became parties and the total number now stands at 13, while 20 others have signed it.

[1] Countries such as Botswana, Sri Lanka and Thailand adopted legislation without support from this project but with assistance from public institutions (such as the US Department of Justice) or the private sector (in particular Microsoft).

One could argue that the pace of implementation of the Convention is as fast if not faster than that of other CoE conventions in the criminal field[2], that the implementation of procedural law measures (of which the Conventions contains more than other international treaties) takes time, and that countries are expected to have the legislation in place and adopted by parliaments by the time of ratification. On the other hand, it also appears that in some countries the question of cybercrime – in spite of its significance – is not given the necessary priority.

Status of signatures and ratifications of the Convention on Cybercrime (July 2008)

Ratified (23):

- Albania
- Armenia
- Bosnia and Herzegovina
- Bulgaria
- Croatia
- Cyprus
- Denmark
- Estonia
- Finland
- France
- Hungary
- Iceland
- Italy
- Latvia
- Lithuania
- Netherlands
- Norway
- Romania
- Slovakia
- Slovenia
- The „former Yugoslav Republic of Macedonia"
- Ukraine
- United States of America

Signed (22):

- Azerbaijan
- Austria
- Belgium
- Canada
- Czech Rep
- Georgia
- Germany
- Greece
- Ireland
- Japan
- Luxembourg
- Malta
- Moldova
- Montenegro
- Poland
- Portugal
- Serbia
- South Africa
- Spain
- Sweden
- Switzerland
- United Kingdom

Not signed (6 CoE member States):

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

Invited to accede (3):

- Costa Rica
- Mexico
- Philippines

Request for accession (1):

- Dominican Republic

3.2 Output 2: Criminal justice capacities

Strengthening of capacities for the investigation, prosecution and investigation of cybercrime

In terms of capacity building for more effective investigations, prosecution and adjudications, the focus of the project has been on creating the legal basis in line with the procedural law provisions of the Convention.

[2] With the exception of the Criminal Law Convention on Corruption which had 32 ratifications six years after it was opened for signature.

Several hundred police officers and prosecutors participated in activities around the world where the procedural provisions of the Convention were explained. The project contributed to a number of training events specifically aimed at forensic investigators and others at prosecutors.

A particular problem identified in different countries is related to the need for law enforcement to cooperate with service providers in the investigation of cybercrime. The guidelines adopted in April 2008 will be most useful in this respect.

While law enforcement officers of many countries have made much progress in developing their subject-matter skills and while this is also partly true for prosecutors, the judiciary is clearly lacking behind. Steps have therefore been taken by the project to develop training modules for judges. A first training event was held in Bulgaria in mid-December 2007. In June 2008, training seminars for judges were held in Cairo (Egypt) and in Luxembourg. Another national training event for judges on cybercrime is due to take place in Istanbul in October 2008, and a further event for judges and prosecutors in Ohrid ("the former Yugoslav Republic of Macedonia") in November 2008. The preparation of a training manual for judges is in preparation. The project will furthermore cooperate with a European Commission-funded project carried out by CYBEX in Spain and aimed at development a standard course for judges.

3.3 Output 3: International cooperation

Capacities of criminal justice bodies to cooperate internationally re-enforced

The capacity of countries to cooperate internationally will be largely enhanced once they become parties to the Convention.

The regional conferences organised in Serbia and Ukraine, the global Octopus Conferences held in Strasbourg in June 2007 and April 2008 had a strong focus on international cooperation against cybercrime. Participation of the CoE in a large number of events organised by other organisations helped explain the relevant provisions of the Convention further.

In October 2007, a study was launched to document good practices in the implementation of the international cooperation provisions of the Convention. A follow up report on the effectiveness of the network of 24/7 contact points will be prepared in the 2nd half of 2008 for discussion at a workshop in November 2008.

The project contributed to the strengthening of the 24/7 points of contact in line with Article 35 of the Convention and the experience of the G8 High-tech crime subgroup.

The risk of competing networks or a multiplication of contact points and networks was reduced by reaching an understanding in November 2007 with the G8 subgroup to merge the directories of contact points of the CoE and the G8. This was confirmed by the T-CY and practical steps now need to be agreed upon.

4 The way ahead

In addition to the Cybercrime Convention Committee (T-CY), the Project against Cybercrime is the most important resource that the CoE has at its disposal to support the implementation of the Convention.

Results so far show that the project has been very effective and pragmatic, and that much has been achieved with limited resources.

The momentum created by the project now provides unique opportunities to make an impact around the world by the scheduled end of the project in February 2009.

A proposal for a follow up project is in preparation. This proposal should be finalised by September 2008 and circulated in view of securing funding. Additional country-specific or regional projects should also be developed.

A global Octopus Interface Conference is scheduled to be held on 10-11 March 2009: it will permit an assessment of the current project and the launching of follow up activities.

4.1 Focus during the remainder of the project

The thematic focus during the remainder of the project (August 2008 – February 2009) will be:

- Further support to the strengthening of cybercrime legislation
- Dissemination of the law enforcement – ISP guidelines
- Preparation and testing of training materials for judges
- Strengthening of 24/7 contact points.

4.1.1 Support to the strengthening of legislation in view of implementing the Convention and permitting accession

Activities in this respect include the following:

- In countries were legislative reforms are underway, the process will be supported if appropriate (such as in Argentina, Brazil, Colombia, Philippines and others).
- Legislative analysis will be provided on request. For example, a review of the draft law of Niger will be completed by September 2008
- A legislative review workshop event will be organised in Colombia in early September for 18 countries of Latin America in cooperation with the Organisation of American States
- A cybercrime conference will be organised in Turkey in cooperation with Microsoft in October 2008 in view of promoting the implementation of the Convention in Turkey
- A similar workshop is envisaged for ASEAN countries in Kuala Lumpur in October 2008
- The project will contribute to the Internet Governance Forum in India in December 2008.

4.1.2 Strengthening of capacities for the investigation, prosecution and investigation of cybercrime

Activities in this respect include the following:

- The guidelines for the cooperation between law enforcement and service providers adopted in April 2008 will be disseminated, for example at the Internet Governance Forum in December 2008, at the London Action Plan meeting in October 2008 and through other events. This will support the implementation of the procedural provisions of the Convention
- The question of data protection/privacy in the investigation of cybercrime will also be tabled at the Internet Governance Forum in December 2008 based on the study prepared in early 2008
- The CoE will contribute to the training of investigators and prosecutors through this project and activities organised by other organisations. Training workshops for judges and prosecutors are foreseen in November 2008 (Ohrid, "the former Yugoslav Republic of Macedonia") and January 2009 (Romania)
- Materials will finalised for the training of judges and cooperation with other organisations and projects will be sought in view of developing a standardised replicable training course.

4.1.3 International cooperation

Activities in this respect include the following:

- An analysis of the effectiveness of 24/7 points of contact will be prepared and an international workshop on this question will be carried out in November 2008. The results will feed into the work of the Cybercrime Convention Committee in March 2008.
- In cooperation with the G8 High-tech Crime Subgroup, the project will help maintain the Directory of Contact Points.
- In countries that have ratified the Convention but have not yet established such contact points (Armenia, Bosnia and Herzegovina and Ukraine) their creation will be promoted.

4.2 List of activities proposed (August 2008 – February 2009)

Date	***Place***	***Description***
Aug 2008 – Feb 2009	Misc	Legislative analysis
Aug - Sep 2008	Strasbourg	Study on "jurisdiction"
Aug – Oct 2008	Strasbourg	Finalisation of materials for the training of judges
Aug – Oct 2008	Strasbourg	Study on the effectiveness of 24/7 points of contact
20-22 Aug 2008	Rio, Brazil	International Lawyers Association Conference
26 Aug 2008	Belo Horizonte, Brazil	Training workshop for prosecutors
27-28 Aug 2008	Brasilia, Brazil	Meetings with public authorities on cybercrime legislation

3-5 Sep 2008	Bogota, Colombia	OAS/CoE regional conference on cybercrime legislation for 18 OAS member States
16 – 18 Sep 2008	Geneva	IGF Preparatory meeting
25 – 26 Sep 2008	Brussels	European Commission meeting on cybercrime
6-8 October 2008	Spain	Conference on Electronic Evidence and the fight of Cybercrime
20 – 21 Oct 2008	Strasbourg	European Dialogue on Internet Governance
10 – 12 Oct 2008	Abidjan, Ivory Coast	Organisation Internationale de la Francophonie: Pan-African conference on cybercrime
23 Oct 2008	Athens, Greece	Eurojust: Strategic meeting on cybercrime
23-24 Oct 2008	Istanbul, Turkey	Conference on cybercrime
30-31 Oct 2008	Kuala Lumpur	EC/ASEAN workshop on cybercrime legislation
11-12 Nov 2008	Minsk, Belarus	Workshop on cybercrime legislation and investigation
13 Nov 2008	Barcelona	ISMS forum "Threats to Information Security"
17 Nov 2008	"the former Yugoslav Republic of Macedonia"	Training workshop for judges and prosecutors
18-19 Nov 2008	"the former Yugoslav Republic of Macedonia"	Regional workshop on 24/7 points of contact
3 – 6 Dec 2008	India	Participation in Internet Governance Forum
Jan 2009	Romania	Training workshop for judges and prosecutors

This list will be updated in the light of emerging needs and opportunities.

4.3 Relationship with the Cybercrime Convention Committee (T-CY)

In line with Article 46 (Consultations of the Parties) the Cybercrime Convention Committee (T-CY) was established in 2006 and since held three meetings (the last one in April 2008). In June 2007 and in April 2008, the T-CY followed immediately the global conferences on Cooperation against Cybercrime that were organised by the Project. This link has been beneficial for both the T-CY and the Project, and there is an understanding that this practice should continue. At its 3rd meeting:

> 41. The T-CY welcomed the results of this global Conference and took note of the several reports prepared under the Project. It welcomed the organization of the Project's global conference immediately prior to the T-CY and recommended that this practice be continued in the future if possible.

The next meeting of the T-CY is thus scheduled for 12-13 March 2009, following the global conference on 10-11 March.

The T-CY also requested states to consider voluntary contributions to the Project:

> 39. The project is currently funded from the budget of the Council of Europe and voluntary contributions from Estonia and Microsoft. The T-CY called on other States

and bodies to make additional contributions available so that the Project can be fully implemented.

The 3rd meeting of the T-CY in April 2008 tasked the Project with the following:

> 16. The T-CY requested the Project on cybercrime to prepare, in co-operation with the Committee of experts on the operation of European Conventions on co-operation in criminal matters (PC-OC) and the G8 Network:
>
> - a report dealing in particular with the nature, role, powers, legal basis and institutional e-mail addresses of contact points and to submit it to the next meeting of the T-CY.
>
> 27. The T-CY took note of a proposal by Romania concerning the preparation by the T-CY of a checklist for use between the 24/7 contact points for requests for expedited preservation of computer data and requested the Project on cybercrime to present a draft for consideration by the T-CY at its next meeting.
>
> 29. The T-CY recognized that many jurisdictional difficulties arose owing to the ease by which servers could be changed rapidly from country to country or make use of Bots. The T-CY agreed that further consideration should be given to questions of jurisdiction in the light of technological developments and invited the Project on cybercrime to submit a report on this matter to the next meeting of the T-CY.

The Project will carry out these activities as requested by the T-CY during the remaining months.

4.4 Towards a follow up project

The current project will end in February 2009. Experience to date clearly shows that the project has been able to produce results and make an impact, and that there is much demand for continued support of a similar nature.

Initial discussions suggest that such a Phase 2 project should again be aimed at the implementation of the Convention on Cybercrime and its protocol on xenophobia and racism, but also related instruments such as standards on data protection and the protection of children from exploitation and human beings from trafficking.

It should help make international cooperation more effective based on the analyses carried out under the current project.

With regard to law enforcement capacities, it should focus on the implementation of the guidelines on law enforcement – service provider cooperation.

The training of judges should be supported on the basis of the materials developed under the current project.

Regarding the training of judges, prosecutors and law enforcement, opportunities need to be explored in view of institutionalising such training in a sustainable manner through partnerships between public and private sectors and academia.

The structure would be as follows:

Project objective	To promote broad implementation of the Convention on Cybercrime (ETS 185) and its Protocol on Xenophobia and Racism (ETS 189) and related international standards
Output 1	Legislation and policies: Cybercrime policies and legislation strengthened in accordance with the Convention on Cybercrime and its Protocol
Output 2	International cooperation: Capacities of 24/7 points of contact, prosecutors and of authorities for mutual legal assistance strengthened
Output 3	Investigation: Law enforcement – service provider cooperation in the investigation of cybercrime improved on the basis of the guidelines adopted in April 2008
Output 4	Training: Judges and prosecutors trained in the prosecution and adjudication of cybercrime, and recommendations available regarding the institutionalisation of such training
Output 5	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
Output 6	Exploitation of children and trafficking in human beings: Enhanced knowledge of standards against the sexual exploitation and abuse of children and trafficking in human beings on the internet

The project should last at least until mid-2011 (that is 28 months) and the budget is estimated at Euro 1.4 million. While up to Euro 400,000 could be envisaged to be funded from the CoE Programme of Activities (Project 1429), the remainder (Euro 1 million) would need to be mobilised in the form of voluntary contributions.[3]

A project of this nature cannot be carried out without staff. Member States should therefore be encouraged to second a qualified cybercrime expert to the CoE.

4.5 Cooperation with Microsoft

Project activities to date were funded by voluntary contributions from Microsoft and the budget of the CoE (Project 143/1429 on Economic Crime) as well as from a voluntary contribution form Estonia in 2008. As indicated in the previous report, cooperation with Microsoft went beyond providing financing:

- Representatives of Microsoft offices around the world facilitated contact to stakeholders and provided information regarding the legislative and institutional framework
- In a number of instances, they provided additional support locally to meetings organised by public authorities and the CoE
- They promoted the implementation of the Convention through events organised by Microsoft; and the CoE was invited to participate in a number of these. In the first six months of 2008 this included a high-profile event in the Dominican Republic and training workshops for judges in Egypt and Luxembourg
- Microsoft provided expertise to training events organised under the PACO Serbia project against economic crime

[3] See Appendix for a project outline.

- They made use of the Convention in order to analyse the legal framework of countries of Asia and the Pacific
- They carried out a number of activities related to child protection and promoted the implementation of Article 9 on child pornography of the Convention on Cybercrime and now also take into account the new Convention on the sexual exploitation and abuse of children (ETS 201)
- Microsoft supported the study on law enforcement-service provider cooperation and facilitated the participation of other service providers in the working group that prepared draft guidelines for such cooperation.

The cooperation between Microsoft and the CoE has been very pragmatic and result-oriented. A continuation of this partnership beyond 2008 should be in the interest of both parties.

5 Appendix: Follow up project proposal

Global Project on Cybercrime (Phase 2)

Outline

Version 11 August 2008

Project title	Global Project on Cybercrime, Phase 2 (DGHL/2009/2079)
Project area	A global project to support countries in implementation of the Convention on Cybercrime (ETS 185) and its Protocol on Xenophobia and Racism (ETS 189)
Budget	Up to EURO 1.4 million (threshold EURO 500,000)
Funding	CoE (Project 1429 - economic crime) Voluntary contributions and secondments
Implementation	Economic Crime Division (Directorate General of Human Rights and Legal Affairs, CoE)
Duration	28 months (1 March 2009 – 30 June 2011)

BACKGROUND AND JUSTIFICATION

Computer networks are turning the world into a global information society in which any kind of information is available to internet users almost anywhere and in which electronic commerce may soon exceed hundreds of billions of Euros. However, this process is accompanied by an increasing dependency on such networks and a growing vulnerability to criminal intrusion and misuse. Networks facilitate illegal access to information, attacks on private or public computer systems, distribution of illegal content as well as cyber-laundering and possibly cyber-terrorism. Online fraud (often involving phishing and other methods of identity theft, fake websites, advance fee fraud, auction fraud, stock market manipulation, credit card and other financial crime) is expanding rapidly as cybercrime is increasingly aimed at generating illegal proceeds and as offenders are increasingly organising to commit crime on the Internet.

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

- effective criminalisation of cyber-offences. 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, and between State institutions and the private sector
- efficient mutual legal assistance regimes, allowing direct cooperation among multiple countries.

The Convention on Cybercrime (ETS 185) of the CoE helps countries respond to these needs. It was opened for signature in November 2001 and by July 2008 had been ratified by 23 and signed by another 22 countries. The Additional Protocol on the Criminalisation of Acts of a Racist and Xenophobic Nature Committed through Computer Systems (ETS 189) of January 2003 had been ratified by 13 and signed by another 20 States.

From September 2006 to February 2009, the CoE implemented the first phase of the Project on Cybercrime in order to support countries worldwide in the implementation of the Convention. The project was funded by the CoE and contributions from Microsoft and Estonia.

During this period the project helped establish the Convention as the primary reference standard for cybercrime legislation globally. This is reflected among other things in the recognition that the Convention received by a wide range of international and regional organisations and the ever stronger cooperation with the private sector (in particular Microsoft) and other initiatives.

The project helped create a momentum of cooperation against cybercrime at all levels. Several Interface conferences and a large number of other meetings were organised or supported. It provided specific legislative advice and helped shape cybercrime legislation in a wide range of European and non-European countries. The project familiarised hundreds of law enforcement and criminal justice officers around the world with the investigative tools provided by the Convention. In this connection, modules for the training of judges were prepared. Guidelines were developed to help law enforcement and internet service providers structure their cooperation in the investigation of cybercrime. The need to protect personal data and privacy while enhancing the security of cyberspace was underlined. A particular need was expressed by stakeholders to strengthen the protection of children against their sexual exploitation on the internet. The project promoted effective international cooperation and in particular the creation of 24/7 points of contact and stronger cooperation with the G8 High-tech Crime Subgroup and Interpol.

The present project is designed to follow up on this and build on the momentum created. It is to serve as a resource allowing the CoE to support European and non-European countries in a pragmatic and flexible manner.

OBJECTIVE, EXPECTED OUTPUTS AND ACTIVITIES

Project objective	To promote broad implementation of the Convention on Cybercrime (ETS 185) and its Protocol on Xenophobia and Racism (ETS 189) and related international standards
Output 1	Legislation and policies: Cybercrime policies and legislation strengthened in accordance with the Convention on Cybercrime and its Protocol
	• Up to 10 in-country law drafting/review workshops in European and non-European countries
	• Up to 3 international workshops on cybercrime legislation (as part of global conferences)
	• Up to 12 legal opinions on draft laws
	• Participation in different events to promote implementation and accession of the Convention
	• Preparation of country profiles and other documentation on cybercrime legislation
Output 2	International cooperation: Capacities of 24/7 points of contact, prosecutors and of authorities for mutual legal assistance strengthened
	• Maintenance of the directory of contact points (in cooperation with the G8)
	• Study on the effectiveness of contact points

	• Development of a cooperation manual on mutual legal assistance in cybercrime matters
	• Up to 5 training events for contact points, prosecutors and authorities for MLA
	• Up to 3 international workshops for contact points, prosecutors and MLA authorities (as part of global conferences)
Output 3	Investigation: Law enforcement – service provider cooperation in the investigation of cybercrime improved on the basis of the guidelines adopted in April 2008
	• Documentation and dissemination of good practices
	• Up to 7 in-country events on law enforcement – service provider cooperation
	• Up to 3 international workshops on LE/ISP cooperation (global conference)
Output 4	Training: Judges and prosecutors trained in the adjudication of cybercrime
	• Analysis of existing training materials, institutions (including academia) and of opportunities for partnerships and institutionalisation of training
	• Preparation and dissemination of training materials
	• Up to 7 national/regional training events for judges and prosecutors (training of trainers)
Output 5	Data protection and privacy: Data protection and privacy regulations in connection with cybercrime investigations improved in line with CoE and other relevant international standards
	• Up to 7 in-country workshops to review regulations and practices on data protection/privacy
	• Participation in events to promote data protection and privacy regulations
	• Studies and analyses on data protection and privacy regulations and practices
	• Up to 3 international workshops (as part of global conferences)
Output 6	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
	• Up to 5 in-country workshops to review regulations and practices on the sexual exploitation and abuse of children and trafficking in human beings on the internet
	• Participation in events to promote the Convention on the exploitation and abuse of children (CETS 201) and on trafficking in human beings (CETS 197)
	• Studies and analyses
	• Up to 2 international workshops (as part of global conferences)

BUDGET

Overall project budget (September 2006 – February 2009)

The total budget of the project has been estimated at Euro 1.4 million. The threshold to launch implementation at a reduced scale would be Euro 500,000.

Overall estimated project budget (March 2009 to June 2011) in Euro

	Euro		Percent
Output 1 - Legislation and policies			
In-country workshops (10)	150,000		
Legal opinions, studies and analyses	42,000		
International workshops (part of global conf.)	98,000		
Participation in events to promote the Convention	40,000		
		330,000	24%
Output 2 - Points of contact and MLA authorities			
Maintenance of directory	20,000		
Country-specific support	50,000		
Studies and analyses	30,000		
Cooperation manual	30,000		
Regional and international events (5)	170,000		
		300,000	21%
Output 3 - Law enforcement - ISP cooperation			
In-country events (5)	70,000		
Studies, analysis and sharing of good practices	28,000		
International workshops (part of glob conf.)	56,000		
		154,000	11%
Output 4 - Training of judges			
Preparation and dissemination of materials	40,000		
In-country and regional training events (7)	140,000		
		180,000	13%
Output 5 - Data protection and privacy regulations			
Legal opinions, studies and analyses	42,000		
In-country workshops (5)	72,000		
International workshops (part of glob conf.)	56,000		
		170,000	12%
Output 6 - Exploitation of children and trafficking			
In-country workshops (5)	84,000		
Studies and analyses	25,000		
Participation in events	25,000		
International workshops (part of glob conf.)	40,411		
		174,411	12%
Sub-total	1,308,411		93%
Overheads (7%)	91,589		7%
Grand total	1,400,000		100%

This estimate includes cost for a project manager (part-time), a long-term adviser or seconded expert (full-time) and an assistant (full-time). Administrative cost would be covered from the overheads.

IMPLEMENTATION ARRANGEMENTS

The project serves as a resource to support:

- activities carried out by the CoE
- activities carried out by other partners through CoE expertise
- the participation of officials from different countries in specific activities carried out by other organisations or partners.

The project is implemented by the Economic Crime Division of the Directorate General of Human Rights and Legal Affairs of the CoE by making use of the expertise available in countries which are party or signatory to the convention. Close cooperation with public and private sector partners will be sought.

CONTACT

For any additional information please contact:

Economic Crime Division
Directorate General of Human Rights and Legal Affairs
Council of Europe
F-67075 Strasbourg Cedex (France)

Tel +33 3 9021 4506
Fax +33 3 8841 3955
Email alexander.seger@coe.int