www.coe.int/cybercrime

COUNCIL OF EUROPE CONSEIL DE L'EUROPE

Strasbourg, 15 June 2009 ECD/567(2009)1

Project on Cybercrime

Final report

(September 2006 – February 2009)

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

Project funded by Estonia, Microsoft and the Council of Europe

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

Disclaimer

Executive summary

This report summarises activities implemented and the results achieved under the Project on Cybercrime between September 2006 and February 2009 when it was completed.

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

The project was possible due to voluntary contributions from Microsoft and Estonia which complemented Council of Europe funding.

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

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

- Albania: Amendments to substantive and procedural criminal law adopted in 2008
- Argentina: Amendments to substantive criminal law adopted in 2008
- Azerbaijan: Signed Convention on Cybercrime in 2008
- Brazil: Draft amendments approved by Federal Senate in 2008 and now before the Chamber of Deputies
- Chile: Request for accession received in February 2009
- Colombia: Amendments to substantive criminal law adopted in January 2009
- Dominican Republic: Legislation adopted and entered into force in 2008; Dominican Republic invited to accede to the Convention in 2008
- Georgia: Signed Convention on Cybercrime in 2008
- Germany: Amendments to legislation and ratification law adopted by Parliament in 2008
- India: Amendments to Information Transaction Act adopted by Parliament in December 2008
- Indonesia: Act on Information and Electronic Transactions adopted by Parliament in 2008
- Italy: Ratified Convention on Cybercrime in 2008
- Philippines: Draft law before Parliament and Philippines invited to accede to the Convention on Cybercrime in 2008
- Serbia: Legislative amendments and ratification law adopted by Parliament in early 2009
- South Africa: Signed the Protocol to the Convention on Xenophobia and Racism in 2008
- Sri Lanka: Cybercrime Act adopted and entered into force in 2008.

The project thus helped establish the Convention as the primary standard of reference globally.

Results also include:

- the preparation of guidelines for law enforcement – Internet service provider cooperation which were adopted by the global conference in Strasbourg in April 2008 and which have since been made use of by the European Union and different countries
- the promotion of the training of judges and prosecutors
- the establishment of 24/7 points of contact in countries that are parties to the Convention
- the strengthening of multi-stakeholder cooperation, among other things through the global Octopus conferences.

The project furthermore fed into the Consultations of the Parties, that is, the Cybercrime Convention Committee (T-CY).

Results show that the pragmatic approach of the project has been very effective and that much has been achieved with limited resources (approximately Euro 1.1 million in total). The funds entrusted to this project have been used in an efficient manner and yielded a high return on investment.

The project ended in February 2009. Building on its achievements, the Global Project on Cybercrime (Phase 2) was launched in March 2009. The Government of Romania, Microsoft and McAfee have agreed to provide initial funding. It is hoped that other donors will follow their example and join this undertaking.

1 Background

In 2001, the Convention on Cybercrime of the Council of Europe (CoE) 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.

Although developed by the CoE, it was always intended for the Convention and its Protocol to apply at a world-wide level. These instruments now serve an increasing number of countries around the world as a guideline for the preparation of national legislation, and as a global framework for cooperation against cybercrime.

The Project on Cybercrime was 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 ended in February 2009. The project was based on the following assumptions:

- Societies worldwide are dependent on ICT and thus vulnerable to cybercrime
- They need to develop a consistent and comprehensive legal basis to criminalise conduct, to provide criminal justice authorities with efficient tools for investigation and to engage in efficient international cooperation
- A globally harmonised approach is necessary given the transnational nature of cybercrime
- Multi-stakeholder action and in particular public-private cooperation is essential to counter cybercrime
- The Convention on Cybercrime provides a basis for such an approach.

The objective and expected outputs of the project were:

Project objective:	To promote broad implementation of the Convention on Cybercrime (CETS 185) and its Protocol on Xenophobia and Racism (CETS 189)
Output 1:	Draft laws meeting the standards of CETS 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

Voluntary contributions from Microsoft, from Estonia, and allocations from the CoE budget provided sufficient funding to permit the implementation of and participation in more than 110 activities in the course of 30 months.

The present report documents activities implemented and results achieved in the course of this project.

2 Activities

2.1 List of activities (September 2006 – February 2009)

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 Convention on Cybercrime
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	Contribution to United Nations ISPAC Conference on the

	(Italy)	Evolving Challenge of Identity-related Crime
8 Jan 2008✓	Geneva	Participation in ITU High Level Expert Group
29-30 Jan 2008✓	Kosovo[1]	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"

[1] All the reference to Kosovo, whether to the territory, institutions or population, in this text shall be understood in full compliance with United Nations Security Council Resolution 1244 and without prejudice to the status of Kosovo.

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
Aug - Dec 2008✓	Strasbourg	Study on "jurisdiction"
Aug – Dec 2008✓	Strasbourg	Finalisation of materials for the training of judges
Aug – Dec 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
Sep 2008✓	Strasbourg	Analysis of the draft law of Niger
Oct 2008✓	Strasbourg	Analysis of the draft law of Benin
25 – 26 Sep 2008✓	Brussels	European Commission meeting on public-private cooperation against cybercrime
30 Sep 2008✓	Brussels	NATSEC cyber security conference
6-8 October 2008✓	Spain	Conference on Electronic Evidence and the Fight against Cybercrime
7-8 Oct 2008✓	Sofia	ITU cyber security workshop
20 – 21 Oct 2008✓	Strasbourg	European Dialogue on Internet Governance
23 Oct 2008✓	Athens, Greece	Eurojust: Strategic meeting on cybercrime
23-24 Oct 2008✓	Istanbul, Turkey	Conference on cybercrime
27-28 Oct 2008✓	Sri Lanka	Workshop on cybercrime and 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 (PROSECO funded)
17-20 Nov 2008✓	Bangkok	POLCYB conference on policing in cyberspace
18-19 Nov 2008✓	"the former Yugoslav Republic of Macedonia"	Regional workshop on 24/7 points of contact (PROSECO funded)
18 – 20 Nov 2008✓	Abidjan, Ivory Coast	Organisation Internationale de la Francophonie: Pan-African conference on cybercrime
27-28 Nov 2008✓	Kuala Lumpur	EC/ASEAN/CoE workshop on cybercrime legislation
1 – 3 Dec 2008✓	Kenya	US DOJ workshop on cybercrime
15 Dec 2008✓	Abu Dhabi	Cybercrime workshop
30 Jan 2009✓	Washington, USA	Global Network Initiative workshop
3-5 Feb 2009✓	Redmond, USA	High-level visit to Microsoft

10 Feb 2009✓	Rome, Italy	Participation in G8 High-tech Crime Subgroup
18 Feb 2009✓	Brussels, Belgium	Participation in 6th Worldwide Security Conference (East-West Institute)

2.2 Cooperation with countries and regions

2.2.1 Africa

Cooperation with countries of Africa in the course of this project showed that the process of strengthening of legislation has been initiated in a large number of countries, but that this process is rather slow and sometimes incoherent, and not necessarily taking into account international standards. Although there are exceptions, the ability of the majority of African countries to investigate, prosecute and adjudicate cybercrime and cooperate internationally is limited.

There is a serious risk that African countries develop legislation that is not compatible or harmonised with that of other countries, in particular that of countries providing servers and services with which cooperation would be most necessary.

The fact that many countries are working on their legislation is an opportunity that should be made use of through a specific technical cooperation project along the lines of a (yet unfunded) proposal developed by the Secretariat of the African Union Commission and the CoE in July 2008.

2.2.1.1 Benin

Following a regional workshop for countries of West Africa organised by the US Department of Justice in Cotonou in July 2008 (in which the CoE participated), the authorities of Benin submitted a draft law covering substantive law provisions to the CoE for analysis. The study was sent to Benin in October 2008, but it is unclear what follow up was given to it.

2.2.1.2 Egypt

In Egypt, legislation was under preparation in 2007 to strengthen legal provisions related to cybercrime, but it seems that in 2008 these efforts slowed down as priority was given to other acts.

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 for countries of the Arab region. However, it appears 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.

The further training of judges and the protection of children against exploitation and abuse on the Internet are certainly fields for further cooperation. However, it would be important to take up efforts again to strengthen the legal basis with regard to cybercrime and the protection of personal data, not only but also given that European and other countries are outsourcing services to Egypt. Egypt will host the Internet Governance Forum in November 2009 and this may provide an opportunity to reinforce cooperation.

2.2.1.3 Niger

In 2006, Niger had developed a comprehensive set of draft laws for a regulatory framework related to information and communication technologies, including cybercrime. In September 2007, at the request of the authorities, the CoE provided an analysis of the parts related to cybercrime which was found to largely reflect the provisions of the Convention on Cybercrime. Again, it is unclear what follow up has been given.

2.2.1.4 Nigeria

In Nigeria, different legal acts are in force and institutional capacities are in place to investigate cybercrime to some extent. In 2007, efforts were underway to further strengthen the legal basis, and in December 2007 the CoE prepared an analysis of the draft law on cybercrime. That review suggested 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. However, no follow up was given to that.

Cybercrime is not only a challenge for Nigeria itself but cybercrime and related fraud originating from Nigeria is a major concern for many other countries around the world. It would therefore be essential that Nigeria brings its legislation in line with the Convention on Cybercrime and strengthens is ability to cooperate with other countries by considering accession to this treaty.

2.2.1.5 South Africa

Cooperation with South Africa led to this country to sign the Protocol on Xenophobia and Racism in April 2008 during a visit of the Minister of Justice of South Africa to the Council of Europe. South Africa had signed the Convention on Cybercrime already in 2001 but a policy decision had been taken to submit both instruments together to the Parliament for ratification. Following the signature of the Protocol, the review of national legislation in terms of its compliance with both instruments is now underway in South Africa.

In April 2007, a CoE mission had 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. The visit helped to put the question of the signing of the Protocol and ratification of the Convention back on the agenda of the Department of Justice.

At that time, the South African authorities were 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.

Although South Africa already is in a position to investigate, prosecute and adjudicate cyber-related offences on the basis of existing laws to some extent, ratification and full implementation of the Convention and its Protocol would send an important signal to other countries of southern Africa, and it would enhance the ability of South Africa to cooperate internationally.

2.2.1.6 Regional activities in Africa

Through the Project on Cybercrime, the CoE contributed to or participated in several regional events:

- From 9 to 11 July 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.

- A similar regional workshop for countries of Eastern Africa was organised by the US Department of Justice in November 2008 in Nairobi, Kenya, to which the CoE contributed through the Project on Cybercrime.

- A Pan-African conference took place in November 2008 in Yamoussoukro (Ivory Coast) by the Organisation Internationale de la Francophonie in cooperation with the African Union Commission and the International Telecommunication Union. A Council of Europe speaker presented the Convention on Cybercrime on that occasion.

The Benin regional workshop (July 2008) was indicative of the efforts underway and for what national technical level experts believe was necessary:

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.

2.2.2 Arab region

Cooperation with countries of the Arab region indicated interest to strengthen legislation, institutions and practices to cope with cybercrime, but actual results remained limited.

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. In December 2008, the CoE through the Project on Cybercrime contributed again to a similar event in Abu Dhabi.

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.*

There are thus prospects for further cooperation, but the national authorities would need to define the course of action they would like to follow and for which they would need support.

2.2.3 Asia

Cooperation with Asian countries under the Project on Cybercrime has been very encouraging and produced good results:

- Several countries adopted legislation reflecting the requirements of the Convention on Cybercrime (such as India, Indonesia and Sri Lanka)
- In the Philippines a draft law is before Parliament, and in 2008 the Philippines was invited to accede to the Convention on Cybercrime
- Cooperation has been initiated with other ASEAN countries and needs for legislative reforms have been identified.

2.2.3.1 India

In December 2008, the Parliament of India adopted amendments to the Information Technology Act 2000. These amendments, although they will need to be complemented by a range of secondary regulations to be issued by the Executive, largely reflect the provisions of the Convention on Cybercrime.

Under the Project on Cybercrime, the CoE had visited New Delhi in February 2007 and 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 returned its report to the Government in the beginning of September. The report reflected the observations made by CoE experts and referred to the Convention on Cybercrime.

In order to continue the dialogue in this matter, the project supported a national conference on cybercrime 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. It preceded the global Interpol meeting on cybercrime in New Delhi.

In December 2008, India hosted the Internet Governance Forum in Hyderabad (3-6 December 2008). The Council of Europe had prepared a number of workshops and fora but had to cancel its participation following the Mumbai attacks at the end of November.

In December 2008, the Parliament of India adopted and on 5 February 2009 the President of India signed the amendments to the Information Technology Act.

By February 2009 accession to the Convention remained under consideration by the Government of India.

There are thus prospects for further cooperation with India. Accession to the treaty would be of great benefit for India as well as for other parties to the Convention. Further activities may focus on the question of law enforcement – service provider cooperation, and the training of judges and law enforcement.

2.2.3.2 Indonesia

In 2008, Indonesia adopted legislation which addresses many requirements of the Convention on Cybercrime, and in early 2009, the authorities prepared further amendments to bring Indonesian legislation fully in line with this treaty. They furthermore expressed a strong interest in acceding to the Convention.

A CoE mission had 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 taking into account proposals made by CoE experts.

Indonesia participated in an ASEAN/European Commission workshop for ASEAN countries in November 2008. The analysis of legislation during that event confirmed compliance with many provisions and identified issues that remained to be covered. In February 2009, the Indonesian authorities sent further draft amendments to the Council of Europe to close the remaining gaps for review.

Important progress was thus made in Indonesia and there are very good prospects for further cooperation as well as accession by Indonesia to the Convention on Cybercrime.

2.2.3.3 Japan

Japan signed the Convention on Cybercrime in 2001, but legislation to fully implement the treaty has been pending in Parliament since 2004. The obstacles are unrelated to cybercrime provisions, but are nevertheless part of the same package of laws.

During a meeting in Tokyo in May 2008, representatives of the Government confirmed that Japan remained committed to become a party to the Convention on Cybercrime.

2.2.3.4 Pakistan

In February 2007, the Project on Cybercrime prepared an analysis of the Electronic Crime Bill 2006. This Bill was subsequently adopted in the form of a Presidential Decree not reflecting the comments made. The transformation of the decree into a proper law may provide a further opportunity to ensure that the legislation of Pakistan is compatible with international standards.

2.2.3.5 Philippines

Cooperation with the Philippines under the Project on Cybercrime resulted in an invitation to the Philippines to accede to the Convention and a draft law meeting the requirements of this treaty.

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.

Since late 2008 a draft law is before Parliament for consideration and it is hoped that the Parliament will deal with it in due course.

As the Philippines have already been invited to accede, the adoption of the law could lead to early accession to the Convention, and this would not only allow the Philippines to cooperate with other parties but also encourage a similar process in other countries of this region.

2.2.3.6 Sri Lanka

In July 2008, the Computer Crimes Act no 24 of 2007 entered into force in Sri Lanka which brings the legislation of the country largely in line with the Convention on Cybercrime.

In October 2008, the Information and Communication Technology Agency of Sri Lanka and the CoE through the Project on Cybercrime organised a joint workshop in Colombo to raise awareness among judges, prosecutors and law enforcement of this Act

Discussions during this event showed that the Computer Crimes Act and other laws in force cover the provisions of the Convention on Cybercrime. Senior officials underlined that the Government would consider seeking accession to this treaty.

There are thus prospects for further cooperation with Sri Lanka which may focus on further training of judges, prosecutors and law enforcement to enable them to fully implement this new legislation.

2.2.3.7 Regional: ASEAN

In November 2008, the ASEAN Secretariat, the European Commission funded APRIS II Project and the CoE's Project on Cybercrime organised a joint workshop on cybercrime legislation for ASEAN countries. This event added impetus to the reforms underway in Indonesia and the Philippines and helped identify the needs for legal reforms in other member states of ASEAN.

The workshop was an excellent example of cooperation among different organisations. Follow up events should be organised in 2009 and 2010 to further embed capacity building and cooperation against cybercrime within ASEAN.

Country	***Summary of discussions***
Brunei Darussalam	In Brunei Darussalam cybercrime legislation is largely inspired by identical legislation of Singapore, which in turn took its inspiration from the UK Computer Misuse Act. Regarding substantive law most of the substance of the Cybercrime Convention is covered, either by specific laws or by traditional criminal law on the basis of case law. Regarding criminal procedural law, further amendments are needed. A Bill is planned to amend criminal law, including amendments relating to cybercrime and investigative powers. In order to keep the amendments in line with the Cybercrime Convention it is recommended to hold a workshop on the matter in 2009.
Cambodia	Cambodia has not yet addressed the issue of cybercrime in its domestic law. In the Country Report, prepared for the 7th Senior Officials Meeting on Transnational Crime, Vientiane Lao, June 25-28, 2007 a separate chapter has been included on cybercrime, recognising that Cambodia suffers from cybercrime and that it has to adopt laws against cybercrime. So far, no specific Bills have been launched in this area. It further remains unclear to what extent existing criminal law and criminal procedural law are capable to deal with any of the issues as incorporated in the Cybercrime Convention, or whether mutual assistance is possible. It is therefore recommended to hold a workshop in Cambodia to initiate the necessary steps to develop legislation in line with the Cybercrime Convention
Indonesia	In Indonesia the Electronic Information and Transaction Act was adopted in Spring 2008. Indonesia thus made good progress in the elaboration of cybercrime law taking into account previous advice of the Council of Europe. Most of the substantive law issues are covered. The same conclusion can be drawn for criminal procedural law. Indonesia could thus already now seek accession to the Convention. Additional bills will be elaborated in the near future to cover specific issues in particular with regard to procedural law. Once these bills are adopted, Indonesia could accede to the Budapest Convention. However, special attention should be paid to international co-operation. Indonesia is only able to provide mutual assistance on the basis of bilateral agreements. Data protection legislations should also be developed in parallel to further cybercrime regulations.
Laos	In Laos specific substantive or procedural law provisions related to cybercrime are currently not available. An e-commerce act is being finalized. This provides an opportunity for elaborating consistent and comprehensive legislation on cybercrime in line with the Budapest Convention. A workshop could be organized in 2009 in order to initiate a process of legislative reform.
Malaysia	In Malaysia, the Computer Crimes Act of 1997 and the Communication and Multimedia Act of 1998 provide the main legal measures related to cybercrime. These meet a range of requirements but some substantive (such as system interference) and procedural law issues (such as expedited preservation) seem not be covered. Currently, the authorities are carrying out a study to identify needs for reform (to cope with issues such as phishing, illegal access, DDOS attacks etc), and the Convention on Cybercrime serves as a guideline in this respect. Once the study is completed and the reform of legislation is completed Malaysia should be able to accede to the Convention. A workshop could be organized in 2009 to discuss the results of the study.
Philippines	In the Philippines a draft law is currently before the Parliament. This draft is in line with the Convention on Cybercrime and has been reviewed on several occasions in cooperation with the Council of Europe. Some possible gaps were identified during

	the workshop and will be taken into account as the bill is further improved. The Philippines were invited to accede to the Budapest Convention in May 2008. In order to ensure the adoption of the law, some members of Congress and Senators could be invited to participate in the Global conference on cybercrime organized by the Council of Europe in March 2009. Subsequently a workshop for congressmen and senators could be held in the Philippines for a detailed discussion about the draft law in order to promote its speedy adoption. Once adopted, the Philippines will be ready to accede to the Convention.
Singapore	Singapore's cybercrime legislation is largely inspired by the UK Computer Misuse Act. On substantive law most of the substance of the Cybercrime Convention is covered, either by specific provisions or by traditional criminal law on the basis of case law. Where criminal procedural law is concerned, search and seizure of computer systems are covered, likewise the power to order the production of data. Domestic law does not provide for a legal power to intercept traffic data or the content of telephone or internet communication. No power has been defined in relation to the expedited provisional provisions of articles 16 and 17 of the Cybercrime Convention. This will also limit the possibilities of international cooperation (articles 29 or 30). Mutual assistance to other countries is rendered on the basis of (bilateral) treaties but Singapore can co-operate on the basis of the principle of reciprocity. The current legislation should therefore be reviewed in the light of the Budapest Convention.
Vietnam	In Vietnam a few substantive law provisions are available in the penal code and general procedural provisions can be applied to some extent. Amendments to the penal code are before the National Assembly for adoption in May 2009. These include some additional provisions on cybercrime. A specific law on cybercrime covering substantive and procedural law provisions may need to be considered in the future. One or several workshops could be organized in 2009 in order to analyse existing and draft provisions, raise awareness among decision makers and prepare the ground for further reforms of cybercrime legislation. The Convention on Cybercrime should be considered in this respect; it would also serve as a basis for international cooperation. A high tech crime unit may be established in the Ministry of Public Security in 2009. Training of its staff would be required. The Interpol office and the VN-Cert are already available for international cooperation.

2.2.4 Australia

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

2.2.5 Europe

In Europe, six additional countries ratified and three signed the Convention on Cybercrime in the course of the project. In more than 30 European countries work on cybercrime legislation was underway between 2006 and February 2009, and altogether Europe experienced a considerable improvement in terms of legislation, enforcement and international police and judicial cooperation against cybercrime. At the same time the pace of ratifications was slower than expected.

The Project on Cybercrime not only focused on supporting legislative work in view of signature and ratification, but also reviewed the legislation of countries that were already parties to the Convention without having fully implemented all its provisions.

The Project furthermore promoted the establishment of 24/7 points of contact (by February 2009 all parties but Ukraine had one), and initiated work on the training of judges and prosecutors.

2.2.5.1 Belarus

Belarus is a non-member State of the Council of Europe and has shown interest in acceding to the Convention on Cybercrime. For that reason, the Project on Cybercrime contributed to a workshop organised by the Organisation for Cooperation and Security in Europe (OSCE) with the Ministry of Interior of Belarus in Minsk on 12 November 2008.

The Ministry of the Interior (MoI) has overall responsibility not only for operational activities managed by the "high-tech crime department" but also for the initiation of improvements in the legislative framework. Representatives from the Prosecutor's Office, National Law Drafting Center, the Parliament and the Ministry of Foreign Affairs participated.

It was underlined that before seeking accession to the Convention national legislation should be brought in line with its treaty. A comparative analysis on the basis of a country profile could be a starting point. The workshop also discussed questions of international cooperation, the establishment of a 24/7 point of contact and law enforcement – Internet service provider cooperation.

2.2.5.2 Georgia

A workshop on cybercrime legislation was held in Tbilisi on 19 February 2008. A concrete outcome of this event was the signing of the Convention on Cybercrime by Georgia on 1 April 2008.

In October 2008 (in the aftermath of the Russia/Georgia conflict), during meetings in Tbilisi, the Georgian authorities underlined the need to strengthen the legislative and institutional framework against cybercrime. In cooperation with the European Commission a proposal for a "Project on Cybercrime in Georgia" was subsequently finalised. The project is to commence in June 2009.

2.2.5.3 Romania

The project provided limited co-financing to the National Cybercrime Training Conference in Romania (Pitesti, 27-29 November 2006). Some 100 investigators, prosecutors and

judges from different regions of Romania were trained in order to allow them to implement the cybercrime legislation adopted in 2003. In 2004 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 2003), and establishing specialised services within the Ministry of Interior and the Prosecutor's Office. Further training, in particular of judges, will be required.

The Project funded an expert for a training conference at the National Institute of Magistrates (26-27 March 2007, Bucharest, Romania). Participants were judges, prosecutors and experts that were selected to work as trainers in further cybercrime training activities.

Romania in turn contributed significantly to the Project on Cybercrime by making speakers available from the Ministry of Justice, the Prosecutor's Office, the Ministry of Interior and the Judiciary.

2.2.5.4 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. By the end of Phase 1 of the Project in February 2009, this dialogue had not yet led to a successful conclusion.

2.2.5.5 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.

By February 2009, a package of laws had been passed by the Serbian Parliament which allows for the ratification of six treaties in April 2009, including the Convention on Cybercrime and the Protocol on Xenophobia and Racism.

2.2.5.6 Ukraine

Ukraine ratified the Convention on Cybercrime in 2006, but it appears that some provisions have not yet been fully implemented and that thus further efforts are required. This applies to Article 35 as by February 2009 Ukraine remained the only party to the Convention without a 24/7 point of contact, but also to procedural law. It seems that the lack of specific provisions causes difficulties in the relationship between law enforcement and Internet service providers. The adoption of the fully revised Criminal Procedure Code (which had been pending for several years) would certainly create a more favourable context, although the draft does not contain the type of specific provisions required.

These issues were already pointed out during an international conference on cooperation against cybercrime in Kyiv, Ukraine on 6-7 February 2007 organised within the framework of the Project on International Cooperation in Criminal Matters in Ukraine (UPIC) of the CoE and the European Commission. 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.

The conference noted inter alia that in Ukraine the harmonisation of national legislation with the Convention still needed 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 conference also underlined the need for the establishment of a 24/7 point of contact. The issues in question thus had been identified already in February 2007. Efforts should be undertaken in 2009 to resolve these.

It seems that in December 2008, an internal decision had been taken to establish a 24/7 point of contact within the State Security Service. This decision had not been communicated to the Council of Europe by February 2009. It should also be mentioned that the national Interpol office has a functioning contact point and is connected to the I 24/7 Network.

2.2.5.7 Regional and other activities in South-eastern Europe

Through the Project on Cybercrime as well as sister projects such as PACO Serbia and the PROSECO project on networking among prosecutors several regional and country-specific events on cybercrime were organised in 2007 and 2008. These

- helped strengthen legislation in countries that were not parties to the Convention but also in countries that had already ratified the Convention. By February 2009:
  - Legislation had been passed by Parliament in Serbia to allow ratification (see above)
  - A draft law had been prepared in Montenegro in view of future ratification
  - The Parliament of Albania had passed (in December 2008) amendments to criminal legislation to fully implement the Convention and its Protocol

- The preparation of further amendments had been initiated in "the former Yugoslav Republic of Macedonia"

- led to the creation of 24/7 points of contact in Bosnia and Herzegovina and Serbia and the review of the effectiveness of contact points in other countries of this region

- provided initial training for judges and prosecutors and pointed at the need for comprehensive further training

- underlined the need for public-private cooperation, in particular between law enforcement and Internet service providers.

Activities included a regional conference on cybercrime 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 (March 2007) and Plovdiv (December 2007), legislative assistance workshops were held in:

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

In November 2008, a regional training workshop for judges and prosecutors was held in Ohrid, "the former Yugoslav Republic of Macedonia", within the framework of the PROSECO project, back to back with an international workshop to review the functioning of 24/7 points of contact.

2.2.6 Latin America and Caribbean

2.2.6.1 Argentina

On 5 June 2008, the Chamber of Deputies (the Parliament) adopted amendments to the Criminal Code which bring the substantive criminal law provisions of Argentina much closer to the Convention on Cybercrime.

On 15-16 November 2007, a CoE mission had visited Buenos Aires for 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. This resulted in 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 then requested to review the draft laws amending the Criminal Code and the Criminal Procedure Code.

Following the adoption of the substantive law provisions in June 2008, the focus shifted to the 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.

While the reform of the procedural law continues Argentina could already now consider seeking accession to the Convention.

2.2.6.2 Brazil

In Brazil, draft legislative amendments have been prepared which would bring Brazilian legislation in line with the Convention on Cybercrime. They were approved by the Federal Senate on 9 July 2008, but have since been pending in the Chamber of Deputies (Parliament). The question of accession to the Convention on Cybercrime is still under consideration.

The CoE, through the Project on Cybercrime, has been interacting with the Brazilian authorities since February 2007, when the 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 2007, 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.

In August 2008, the Project on Cybercrime supported a training workshop for judges and prosecutors in Belo Horizonte, contributed to a panel on cybercrime during the meeting of the International Lawyers Association in Rio and had meetings with different ministries, the Federal Senate and the Chamber of Deputies in Brasilia. As a result, the Ministry of External Relations established a working group to review the question of accession to the Convention.

2.2.6.3 Colombia

Colombia made considerable progress by adopting substantive criminal legislation in line with the Convention on Cybercrime in January 2009.

In Colombia an interagency working group led by the Ministry of Foreign Affairs had been working on a draft law on cybercrime since 2006. 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 for further comments).

In September 2008 the Colombia hosted a regional workshop of the Organisation of American States and the CoE on cybercrime legislation for Latin American countries. This added impetus to the reform of cybercrime legislation within Colombia.

On 5 January 2009, the Congress adopted amendments to the Criminal Code of Colombia which brought the substantive legislation of Colombia in line with the Convention on Cybercrime.

Accession to the Convention on Cybercrime is under consideration.

2.2.6.4 Costa Rica

Costa Rica was invited to accede to the Convention on Cybercrime in 2005 but has not yet completed the accession process. A CoE mission visited Costa Rica on 21-22 April 2008. The analysis of legislation suggests that further improvements would be required before Costa Rica could accede to the Convention. This was confirmed during the regional OAS/CoE workshop in Bogota (Colombia) in September 2008 in which Costa Rica participated.

2.2.6.5 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, during the global Octopus Conference in Strasbourg, the Dominican Republic expressed their willingness to accede to the Convention on Cybercrime.

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.

In November 2008, the Dominican Republic was invited to accede to the Convention on Cybercrime.

2.2.6.6 Regional: 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

2.2.6.7 Regional Latin America

Following the example of the event for the Caribbean region, a "Cybercrime Legislation Drafting Workshop" for countries of Latin America was organised jointly by the Organisation of American States, the Council of Europe and the US Department of Justice in Bogota, Colombia (Port of Spain, Trinidad and Tobago (13-15 May 2008). The CoE's Project on Cybercrime contributed to this event. More than 60 representatives from 17 countries of Latin America[2] participated.

By the end of the workshop, draft profiles had been prepared for each of the 17 countries analyzing existing or draft national legislation against the provisions of the Convention and identifying needs for further legislative work.

In general terms, a considerable number of provisions are already in place in different countries. Regarding substantive criminal law, that is, the conduct to be criminalized, several countries cover child pornography on the internet in the comprehensive manner of Article 9 of the Convention on Cybercrime. The illegal access to computer systems (Article 2) and data interference (Article 4) are also provided for in one way or the other in most countries.

On the other hand, the legislation of several countries was unclear with regard to the difference between data interference (Article 4) and system interference (Article 5), and thus it is not certain whether a botnet or denial of service attack would constitute a criminal offence. The same is true for the misuse of devices, that is, the production, sale or distribution of tools for illegal access (hacking tools), illegal interception, and data or system interference.

In terms of procedural law (expedited preservation, search and seizure, production orders and other measures in Articles 16 to 21) most countries seem to rely on omnibus provisions applying to real-life situations. These appear to work to some extent but limit the effectiveness of investigations and the gathering and use of electronic evidence in the course of criminal proceedings.

Further work is thus required in most countries:

Country	***Status of legislation***
1. Argentina	Substantive legislation was adopted in June 2008. Current procedural may meet minimum requirements, but specific provisions should be prepared in connection with reforms of the CPC. Thus, most of the requirements of the Convention are to some degree covered under Argentinean legislation. The provisions which are missing would not prevent Argentina to seek accession.
2. Bolivia	Some substantive law provisions will be implemented under a draft law (e.g. definitions, illegal interception, computer sabotage and additional provisions on infringements of the copyright). The existent legislation criminalizes illegal access (combined with data interference) to computer data, data interference, computer forgery, infringements of the copyright) and some acts related to child pornography. Computer fraud and misuse

[2] Argentina, Bolivia, Brazil, Chile, Colombia, Costa Rica, Dominican Republic, Ecuador, El Salvador, Guatemala, Honduras, Mexico, Nicaragua, Panama, Paraguay, Peru and Uruguay.

	of devices are missing. Most of the procedural law provisions seem not to be in place and interception is prohibited expressly by Constitution.
3. Brazil	The draft law adopted by the Federal Senate in July 2008 and since pending with the Chamber of Deputies would help Brazil cover the minimum requirements of the Convention. Additional complementary laws are also in preparation.
4. Chile	The basic provisions are in place but should be updated. This applies in particular to procedural law.
5. Colombia	The draft law [subsequently adopted in January 2009] brings substantive criminal law in line with the Convention. Further work on procedural law would be required.
6. Costa Rica	Some substantive law provisions seem to be covered, but most need to be reviewed. Most procedural provisions seem to function efficiently.
7. Dominican Republic	The law adopted in 2007 covers all provisions. Secondary regulations on expedited preservation are in preparation.
8. Ecuador	Some provisions appear to be in place, but further work is required on the basis of the Convention on Cybercrime.
9. El Salvador	It seems that two draft laws are in Congress that are based on the Convention on Cybercrime.
10. Guatemala	Most of the substantive law and procedural law provisions have not been implemented yet.
11. Honduras	During the time of the workshop, Honduras was in the process of reforming its criminal legislation. The draft law contained a number of provisions, but further improvements were required.
12. Mexico	Current substantive and procedural criminal legislation covers only few provisions. During the workshop it was proposed that an interagency working group should be established to elaborate a draft law on cybercrime and e-commerce.
13. Nicaragua	Although most of the substantive law and procedural law provisions are provided in the national legislation, they should be reconsidered in order to implement the standards of the Convention.
14. Panama	In general, the substantive law provisions (except Article 6) seem to be covered while the procedural law provisions would need further consideration.
15. Paraguay	Substantive law provisions are partially covered while procedural law provisions need further consideration in order to implement the requirements of the Convection.
16. Peru	Several substantive law provisions are in place but should be reviewed. Procedural provisions seem to be function although they should also be reviewed.
17. Uruguay	Most of the substantive and procedural law provisions required by the Convention do not have a correspondent under the current national law of Uruguay.

2.2.7 Global events

In the course of the project, two global events were organised in order to permit an "interfacing" of representatives of public and private sector institutions across geographic regions on issues covered under the Project on Cybercrime. Both meetings were highly successful, and the Octopus conferences now seem to be a fixture among international events on cybercrime.

2.2.7.1 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.

2.2.7.2 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, botnCETS 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 was 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, with 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 Cooperation with other organisations

2.3.1 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.

2.3.2 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 was held in November 2008 in Kuala Lumpur, Malaysia.

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

In June 2008, the CoE sent a speaker to an APEC event on cyberterrorism in Seoul, Korea. Further cooperation with APEC should be sought in the future.

2.3.3 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.

2.3.4 European Union 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 2007. 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. At the meeting on cybercrime organised by the EC in Brussels on 25-26 September 2008, participants agreed on a set of recommendations on law enforcement – ISP cooperation based on the guidelines adopted by the Octopus conference in April 2008. These recommendations were subsequently adopted by the 2987th Justice and Home Affairs Council meeting (Brussels, 27-28 November 2008). The "Council Conclusions on a Concerted Work Strategy and Practical Measures Against Cybercrime" specifically underline the cooperation between the EC and the Council of Europe and again supports the Convention on Cybercrime.

In 2008, the Council of Europe – through the Project on Cybercrime – cooperated actively with the French EU Presidency and participated, among other things, in the meeting preparing the "European Reporting Platform" (Reims, 5-6 June 2008).

In February 2009, a coordinating meeting of the European Commission, the Council of Europe, Interpol, Europol and UNODC took place in Brussels.

In sum, cooperation between the European Commission/European Union and the Council of Europe regarding cybercrime improved considerably in the course of the project.

2.3.5 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.

The Project on Cybercrime thus was a valuable vehicle to strengthen cooperation between Europol and the Council of Europe.

2.3.6 G8 High-tech Crime Subgroup

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. However, by February 2009, specific details and procedures regarding the merger of the directory and the role of the Council of Europe had not yet been agreed upon.

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.

Between September 2008 and February 2009, the Project on Cybercrime carried out this study, a draft of which was shared with the G8 High-tech Crime Subgroup in Rome on 10 February 2009. Feedback suggested that further discussions are necessary regarding the effectiveness of contact points as well as their responsibilities which seem to be broader under the Convention on Cybercrime than in the practice of the G8 HTCSG.

2.3.7 Global Network Initiative

The GNI was initiated by companies in the ICT sector in response to increasing government pressure in different regions of the world to comply with domestic laws and policies in ways that may conflict with the internationally recognized human rights of freedom of expression and privacy.

The Project on Cybercrime was invited to participate in a round table discussion in Washington DC on 30 January 2009 to present the law enforcement – ISP cooperation guidelines and other relevant tools of the Council of Europe as a means to ensure due process and the rule of law in cybercrime investigations involving service providers.

Further cooperation with the GNI could be sought, for example, in connection with the Internet Governance Forum.

2.3.8 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 later on decided 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.

2.3.9 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 made extensive reference to the Convention on

Cybercrime and suggested 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. The chairman's report (September 2008) is a reflection of the difficulty of the HLEG process to come to a consensus.

2.3.10 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 Council of Europe was strongly involved in the preparatory process of the Hyderabad (India) IGF fro 3-6 December 2009. However, due to the Mumbai attacks, the Council of Europe was unable to participate.

The IGF has proven to be an important platform generating multi-stakeholder action.

2.3.11 Interpol

The CoE and Interpol cooperated on a number of occasions. Among other things, the CoE participated in the October 2006 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 2007 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.

Given that cybercrime units in different countries make increasing use of Interpol's I 24/7 network for efficient police cooperation, cooperation between the Council of Europe and Interpol will certainly be further strengthened in the future.

2.3.12 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. This will allow the 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.

2.3.13 Organisation for Economic Cooperation and Development (OECD)

Cooperation between the OECD and the Council of Europe has been limited during the Project on Cybercrime. However, during the OECD Ministerial Conference on the Future of the Internet Economy in Seoul on 16-17 June 2008, the Deputy Secretaries General of both organizations agreed to intensify cooperation in cybercrime matters in the future in areas such as malware and botnCETS, the online protection of children and data protection.

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 analyse 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 was held on 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 Project on Cybercrime also contributed speakers to the POLCYB meeting in November 2008 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 in 2008.

There is certainly scope for further cooperation with UNODC in cybercrime matters in the future.

2.4 Discussion papers

In the course of the project a series of discussion papers and studies were launched under the Project on Cybercrime. They fed into the global Octopus conferences, the Cybercrime Convention Committee and many other activities:

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?") and guidelines adopted	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 was 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. The study was presented at the cybercrime conference on 1-2 April 2008. A follow up report was prepared in the second half of 2008/early 2009 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 presented at the cybercrime conference on 1-2 April 2008. The question of data protection and privacy is again moving higher on the agenda, and this study was thus very timely.
6. Study on jurisdiction ("Cybercrime and internet jurisdiction")	The purpose of the study was to prepare an inventory of current problems related to jurisdiction in cybercrime matters and to suggest possible solutions.
7. Study on the functioning of 24/7 points of contact	The study analyses the functioning and effectiveness of the 24/7 network of contact points against the requirements as defined in Art 35 of the Convention on Cybercrime.
8. Study on identity theft ("Internet related identity theft")	The study identifies the legal issues involved with regard to identity theft on the Internet, the relevance of the Convention on Cybercrime in this respect and possible additional solution. The study was presented at a conference on identity theft held in Tomar, Portugal, in November 2007 but has been widely used in other fora since.

3 Cooperation with the T-CY and donors

3.1 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 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 carried out these activities as requested by the T-CY

3.2 Cooperation with Estonia

Project activities were funded by voluntary contributions from Microsoft and the budget of the CoE (Project 143/1429 on Economic Crime) as well as a voluntary contribution form Estonia in 2008.

Estonia has been very supportive to CoE activities against cybercrime, and this support has been highly relevant in particular in the light of the cyber-attacks that Estonia was subjected to in May 2007.

Estonia also set an example to other bi-lateral donors and encouraged them to support future project activities.

3.3 Cooperation with Microsoft

Cooperation with Microsoft (and with industry in general) under this project is based on:

- a shared interest in enhancing the security of information and communication technologies
- the Convention on Cybercrime which (a) calls for cooperation with the private sector and which (b) is recognised and supported by industry since 2004 when major companies publicly expressed their support[3]
- thus on an understanding that countries should strengthen their cybercrime legislation in a harmonised manner using this treaty as a guideline
- approval by the Committee of Minister of the CoE of contributions from specific private sector donors to this project[4]
- the understanding that such contributions are not linked to any conditions.

Following the support expressed by Microsoft during the Octopus 2004 conference, and the fact that funding from other sources was not made available in the course of 2005, discussions with Microsoft led to contributions which allowed the Project on Cybercrime to be launched in September 2006.

As indicated in earlier reports, 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 2008, this included a high-profile event in the Dominican Republic and training workshops for judges in Egypt, Luxembourg and Turkey
- Microsoft provided expertise to training events organised under the PACO Serbia project against economic crime
- Microsoft participate actively in the global Octopus conferences
- 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 (CETS 201), such as during a workshop in South Africa in April 2007
- 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.

---

[3] In conjunction with the 2004 Octopus conference major companies (including Microsoft, Ebay, Symantec and others) published an open letter to the US Government to ratify the Convention. A number of companies support the Convention as a matter of corporate policy. In 2008, for example, McAfee announced their "Cybercrime Initiative" with explicit reference to the Convention on Cybercrime.

[4] In 2006, contributions from Microsoft and in February 2009 contributions from McAfee were approved by the Committee of Ministers.

Cooperation between Microsoft and the CoE has been very pragmatic and result-oriented.

In February 2009, the Deputy Secretary General of the Council of Europe accepted an invitation to Microsoft Headquarters in Redmond. The visit resulted in a common understanding at senior level of priority areas for future cooperation, ranging from measures against cybercrime, the protection of children from abuse, the protection of fundamental rights on the Internet and the need to find solutions to questions related to national jurisdictions versus borderless crime and the question of cloud computing.

This successful partnership is thus to continue in the future. It serves as an example of good practice for cooperation between the Council of Europe and industry in the information technology as well as other sectors.

4 Results

4.1 Project objective

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

The Project on Cybercrime between September 2006 and February 2009 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, but also McAfee, Symantec or Ebay, with associations of Internet service providers and other initiatives such the Anti-Phishing Working Group, the London Action Plan, POLCYB, ICCYBER or AusCERT. It is telling that the private is pro-actively supporting the Convention on Cybercrime.

The Project interacted well with the Cybercrime Convention Committee (T-CY) in that it provided substantive inputs and ensured follow up to T-CY decisions. The global Octopus Interface conferences were organised back-to-back with T-CY meetings.

The achievement of the project objective is in particular reflected in concrete results under each of the three outputs.

4.2 Output 1: Legislation

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

Since 2006, a global trend towards stronger cybercrime legislation using the Convention on Cybercrime can be noted. This trend has been supported by the Project on Cybercrime. The Convention on Cybercrime was presented to representatives from more than 150 countries around the world through different types of meetings.

In order to facilitate the analysis of cybercrime legislation against the provision of the Convention, "profiles" have been prepared for more than 90 countries. They served as bases for regional and country-specific workshops on cybercrime legislation and helped share good practices. In addition, detailed analyses of draft laws were provided to Argentina, Benin, Brazil, Colombia, Egypt, India, Indonesia, Niger, Nigeria, Pakistan, Philippines and Serbia.

As a result, more than 100 countries around the world either have cybercrime legislation in place or are in the process of preparing legislation using the Convention on Cybercrime as a guideline or "model law". Examples are:

- Albania: Amendments to substantive and procedural criminal law adopted in 2008
- Argentina: Amendments to substantive criminal law adopted in 2008
- Azerbaijan: Signed Convention on Cybercrime in 2008
- Brazil: Draft amendments approved by Federal Senate in 2008 and now before the Chamber of Deputies
- Colombia: Amendments to substantive criminal law adopted in January 2009
- Dominican Republic: Legislation adopted and entered into force in 2008; Dominican Republic invited to accede to the Convention in 2008
- Georgia: Signed Convention on Cybercrime in 2008
- Germany: Amendments to legislation and ratification law adopted by Parliament in 2008
- India: Amendments to Information Transaction Act adopted by Parliament in December 2008
- Indonesia: Act on Information and Electronic Transactions adopted by Parliament in 2008
- Italy: Ratified Convention on Cybercrime in 2008
- Philippines: Draft law before Parliament and Philippines invited to accede to the Convention on Cybercrime in 2008
- Serbia: Legislative amendments and ratification law adopted by Parliament in early 2009
- South Africa: Signed the Protocol to the Convention on Xenophobia and Racism in 2008
- Sri Lanka: Cybercrime Act adopted and entered into force in 2008.

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.

Nevertheless, in terms of actual ratifications/accessions to the Convention, the progress made has been less satisfying although legislative work is underway in countries. Between September 2006 and February 2009:

- seven countries deposited the instrument of ratification of the Convention on Cybercrime: Armenia, Iceland, Italy, Latvia, Netherlands, Slovakia and the USA
- three additional countries signed the Convention: Azerbaijan, Georgia and Liechtenstein
- two additional countries were invited to accede: Dominican Republic and Philippines, while the request for accession by Chile was received and being processed in February 2009.

Status of signatures and ratifications of the Convention on Cybercrime (February 2009)

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
- Liechtenstein
- Luxembourg
- Malta
- Moldova
- Montenegro
- Poland
- Portugal
- Serbia
- South Africa
- Spain
- Sweden
- Switzerland
- United Kingdom

Not signed (5 CoE member States):

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

Invited to accede (4):

- Costa Rica
- Dominican Republic
- Mexico
- Philippines

Request for accession (1):

- Chile

By February 2009 almost half of the European Union member States (13 out of 27) had not yet ratified this Convention. The call for ratification of the EU Justice and Home Affairs Council of November 2007 and again in November 2008 may help accelerate this process. Six member States of the CoE (Andorra, Monaco, Russia, San Marino and Turkey) had not yet signed the Convention.

Regarding the Protocol on Xenophobia and Racism, four additional countries ratified this instrument in 2007. In 2008, Croatia and Norway also became parties and the total number stood at 13, while 21 others had signed it by February 2009.

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[5], that the implementation of procedural law measures (of which the Convention on Cybercrime contains more than other international treaties) takes time, that countries are expected to have the legislation in place and adopted by parliaments by the time of ratification, and that EU Member States had . 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.

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

4.3 Output 2: Criminal justice capacities

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

Results have been achieved in the following areas under this output:

1. Implementation of the procedural law tools of the Convention

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.

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.

The Project on Cybercrime furthermore contributed to efforts for the harmonisation of law enforcement training (working group led by Europol) and the creation of centres of excellence for training in cybercrime investigations and forensics (2Centre initiative supported by the public and private sector).

2. Law enforcement – ISP cooperation

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 developed under the Project on Cybercrime and adopted in April 2008 can be considered a major achievement in this respect. These guidelines served as a basis for the draft agreement between the French service provider association and the Ministry of Interior, the Government of Romania recommended their use by different public and private institutions in Romania, and they served as a basis for the EU Justice and Home Affairs Council of November 2008. They were circulated in a large range of other countries.

3. Training of judges

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 promote the training of 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. The project contributed to national training event for judges on cybercrime in Turkey in October 2008, and a further event for judges and prosecutors in Ohrid ("the former Yugoslav Republic of Macedonia") in November 2008. A draft training manual for judges was prepared. The project furthermore cooperated with a European Commission-funded project carried out by CYBEX in Spain and aimed at development a standard course for judges. In this context the Council of Europe contributed to a training event in Madrid in October 2008.

The ground has thus been prepared to move towards institutionalising cybercrime training for judges in the future.

4.4 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. By February 2009, fifty countries had either signed/ratified this treaty or been invited to accede. Once they are all full parties, the value of the Convention as a framework for international cooperation will be greatly enhanced.

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 further explain relevant provisions of the Convention.

The Project promoted the creation of 24/7 points of contact in a number of countries. By February 2009, Ukraine was the only country that had not yet established such a mechanism. 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.

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 was prepared between September 2008 and February 2009. The report documented lessons learnt and brought a number of issues to the forefront that need to be addressed to make these contact points and international cooperation in general more efficient.

5 Overall conclusions

In addition to the Cybercrime Convention Committee (T-CY), the Project against Cybercrime was the most important resource that the CoE had at its disposal to support the implementation of the Convention and its Protocol between September 2006 and February 2009.

Results show that the pragmatic approach of the project has been very effective and that much has been achieved with limited resources. Approximately Euro 1.1 million was spent in total. The funds entrusted to this project have been used in an efficient manner and yielded a high return on investment.

The main result of the project is that over a period of 30 months it has been possible to create and sustain a global momentum towards:

- the strengthening of cybercrime legislation in a harmonised manner, including measurable results in terms of laws adopted
- improving public-private (in particular law enforcement – ISP) cooperation in the investigation of cybercrime
- closer cooperation among a multitude of stakeholders.

The Convention on Cybercrime has been established as the primary reference standard globally.

By the end of this project a follow up "Global Project on Cybercrime Phase 2" had been designed to build on the achievements to date (see Appendix). The project is to last from 1 March 2009 to 30 June 2011 with a budget of Euro 1.4 million. Its objective is to promote broad implementation of the Convention on Cybercrime (CETS 185) and its Protocol on Xenophobia and Racism (CETS 189) and related international standards. In addition to what has been covered during the first phase it will put a stronger focus on the implementation of the LEA – ISP guidelines, on promoting financial investigations, on the training of judges, on data protection and privacy and the protection of children.

The Government of Romania as well as Microsoft and McAfee have agreed to provide initial funding and support. It is hoped that other donors will join this effort.

6 Appendix

Project on Cybercrime
www.coe.int/cybercrime

COUNCIL OF EUROPE CONSEIL DE L'EUROPE

Global Project on Cybercrime (Phase 2)

Summary

Version 9 Mar 2009

Project title	Global Project on Cybercrime, Phase 2 (DGHL/2009/2079)
Project area	A global project to support countries worldwide in the 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	Council of Europe (Project 1429 - economic crime) Contributions from Romania, Microsoft, McAfee and other private and public sector donors
Implementation	Economic Crime Division (Directorate General of Human Rights and Legal Affairs, Council of Europe)
Duration	28 months (1 March 2009 – 30 June 2011)

BACKGROUND AND JUSTIFICATION

Computer networks have turned the world into a global information society in which any kind of information is available to internet users almost anywhere and which provides unique opportunities for people to develop their economic potential and exercise their fundamental rights and freedoms. However, this process is accompanied by an increasing dependency on information and communication technologies (ICT) and a growing vulnerability to criminal misuse and attacks. ICT facilitate illegal access to information, attacks on private or public computer systems, distribution of illegal content as well as cyber-laundering, terrorism and other forms of serious crime. Online fraud is expanding rapidly as cybercrime is increasingly aimed at generating illegal proceeds and as offenders are organising to commit crime on the Internet. This is true for all societies, including developing countries which are relying on ICT without the necessary legal and institutional framework.

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

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

The "Budapest" Convention on Cybercrime (ETS 185) of the CoE helps countries respond to these needs. It was opened for signature in November 2001 and by December 2008 had been ratified by 23 and signed by another 23 countries. These include non-European countries such as Canada (signed), Japan (signed), South Africa (signed) and the USA (signed and ratified). Costa Rica, the Dominican Republic, Mexico and the Philippines have been invited to accede. The Additional Protocol on the Criminalisation of Acts of a Racist and Xenophobic Nature Committed through Computer Systems (ETS 189) of January 2003 had been ratified by 13 and signed by another 21 States. Equally important is that a large number of countries worldwide is using the convention as a guideline or model law for the strengthening of their cybercrime legislation.

From September 2006 to February 2009, the CoE implemented the first phase of the Project on Cybercrime 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 and other initiatives.

The project helped create a momentum of cooperation against cybercrime at all levels. Several Octopus 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 in Africa, Asia, the Caribbean and Latin America. More than 100 countries now use the Convention as a guideline for their legislation. 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. 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.

Issues identified during phase 1 of the project included:

- The need for public-private cooperation, in particular the cooperation between law enforcement and internet service providers. In response, guidelines were developed to help law enforcement and ISPs structure their cooperation in the investigation of cybercrime
- The need to protect personal data and privacy while enhancing the security of cyberspace
- The need for a further strengthening of measures to protect children from exploitation and abuse on the internet.

The present project (phase 2) is designed to follow up on this and to 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
Activities	• 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 of and accession to 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
Activities	• 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
Activities	• 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	Financial investigations: enhanced knowledge among high tech crime units and FIUs to follow money flows on the internet
Activities	• Study on typologies of criminal money flows on the internet and techniques of financial investigations
	• Up to 2 international workshops
Output 5	Training: Judges and prosecutors trained in the adjudication and prosecution of cybercrime
Activities	• 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 6	Data protection and privacy: Data protection and privacy regulations in connection with cybercrime investigations improved in line with CoE and other relevant international standards
Activities	• 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 2 international workshops (as part of global conferences)
Output 7	Exploitation of children and trafficking in human beings: Enhanced knowledge of standards against the sexual exploitation and abuse of children and trafficking in human beings on the internet
Activities	• 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 sexual 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

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

The distribution by project component (expected output) is estimated as follows:

	Percent
Output 1 - Legislation and policies	24%
Output 2 - Points of contact and MLA authorities	19%
Output 3 - Law enforcement - ISP cooperation	11%
Output 4 - Financial investigations	4%
Output 5 - Training of judges	13%
Output 6 - Data protection and privacy regulations	9%
Output 7 - Exploitation of children and trafficking	12%
Sub-total	93%
Overheads (7%)	7%
Grand total	100%

IMPLEMENTATION ARRANGEMENTS

The project serves as a resource to support:

- activities carried out by the CoE
- activities carried out by other partners with CoE inputs
- 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