Project on Cybercrime
www.coe.int/cybercrime

COUNCIL OF EUROPE CONSEIL DE L'EUROPE

Economic Crime Division
Directorate General of
Human Rights and Legal Affairs
Strasbourg, 12 December 2007
Final/public

Project on Cybercrime

Progress report

Status as at 30 November 2007

Project funded by the Council of Europe and Microsoft

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

This technical report does not necessarily reflect official positions of the Council of Europe or of the donors funding this project

1 Background

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

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

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

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

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

Although this project was initially to have a budget of Euro 1.7 million, voluntary contributions from Microsoft of Euro 270,000 (US$ 350,000 in 2006 and 2007) and the allocation of so far Euro 360,000 from the Council of Europe budget (2006-2008) allowed this project to commence at a reduced scale.

Following a first progress report in March 2007, the present report summarises the activities and results achieved as at end-November 2007 and provides an updated list of activities for December 2007 to June 2008.

2 Activities

2.1 List of activities

Date	***Place***	***Description***
Sep 2006 – Feb 2007		
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
March - November 2007		
19–21 Mar 2007 ✓	Belgrade, Serbia	Regional conference for countries of south-eastern Europe on cooperation against cybercrime (funded by the PACO Serbia project on economic crime)
26-27 Mar 2007 ✓	Bucharest, Romania	Support to two training seminars for prosecutors (National Institute for Magistrates of Romania)
18-20 Apr 2007 ✓	South Africa	Meetings to promote the ratification of the Convention on Cybercrime and its Protocol and participation in the Symposium "Symposium on online security and the safety and welfare of South Africa's citizens" organised by Microsoft
23–24 Apr 2007 ✓	Philippines/ Asia and Pacific	Promotion of cybercrime legislation in line with the Convention on Cybercrime – Contribution to the Workshop on network security organised by the Asia-Pacific Economic Cooperation and ASEAN in

		Manila, Philippines
11 May 2007 ✓	Moscow, Russian Federation	Meeting on the implementation of the Convention on Cybercrime in the Russian Federation
14–15 May 2007✓	Geneva	Workshop on the Convention on Cybercrime within the framework of the WSIS follow up cluster of events at the ITU
May 2007✓	Strasbourg	Analysis of the draft law on cybercrime of the Philippines
18 June 2007✓	Dubai	Contribution to a regional meeting of states of the Gulf Cooperation Council
21 June 2007✓	Morocco	Meetings to discuss cybercrime legislation and accession to the Convention on Cybercrime
11–12 June 2007✓	Strasbourg	Octopus Interface Conference on "Cooperation against cybercrime"
19-20 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

5-9 Nov 2007✓	Bangkok (Thailand)	Policing Cyberspace International Summit
7-9 Nov 2007✓	Tomar (Portugal)	Contribution to the “Conference on Identity Fraud and Theft” organised by the authorities of Portugal within the context of the EU Presidency
7-9 Nov 2007✓	The Hague	Europol high-tech crime expert meeting
12-16 Nov 2007✓	Rio de Janeiro (Brazil)	Internet Governance Forum
15-16 Nov 2007✓	Brussels	European Commission expert conference on cybercrime
15-16 Nov 2007✓	Buenos Aires (Argentina)	Workshop on cybercrime legislation and accession to the Convention
19-20 Nov 2007✓	Washington DC (USA)	Organisation of American States
26-27 Nov 2007✓	Cairo (Egypt)	Regional conference on cybercrime
30 Nov-2 Dec✓	Courmayeur (Italy)	Contribution to United Nations ISPAC Conference on the Evolving Challenge of Identity-related Crime

2.2 Cooperation with countries and regions

2.2.1 Arab region

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

One immediate result was a request for a review of the draft legislation of Morocco which is now underway.

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

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

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

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

2.2.2 Argentina

A CoE mission visited Buenos Aires on 15-16 November 2007. It consisted of a series of bilateral meetings with senior officials and counterparts and – on 16 November – of a workshop organised with the support of the Law Faculty of the University of Buenos Aires. This event gathered about 40 experts/professionals (mainly from the Ministry of Foreign Affairs, Federal Prosecution Office, Law enforcement and judicial institutions, criminal lawyers, University Professors, the Parliament, working group members drafting the legislation and private sector/service providers).

The two main achievements were: strong support for the accession of Argentina to the Convention (which everybody estimates possible in the first half of 2008) and a first systematic review (followed by a discussion) of the cybercrime legislation with regard to the provisions of the Convention.

At the end of November 2007, the Senate passed the substantive criminal law amendments related to cybercrime.

As a direct follow-up, the Ministry of Justice will shortly send a request to the CoE for a legal expertise of the bill on cybercrime with the amendments introduced by the Senate before it is reviewed and adopted by the Chamber of Deputies. With regard to procedural law, a proposal for amendments to the criminal procedure law of Argentina has been prepared by a working group and can now also be reviewed.

2.2.3 Brazil

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

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

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

2.2.4 Colombia

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

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

2.2.5 Egypt

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

However, between May and November 2007 not much progress seems to have been made regarding this law. In order to add momentum, the CoE supported a Conference on Cybercrime in Cairo on 26-27 November 2007 (see above). The dialogue with the Ministry of Information and Communication Technology on this law should continue.

2.2.6 India

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

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

In terms of follow up, the dialogue with the Government, specifically the Ministry of ICT should be continued and direct assistance should be offered to those responsible for the re-drafting. The next Internet Governance Forum which will be held in India in December 2008 may facilitate progress towards accession to the Convention by India.

2.2.7 Indonesia

A CoE mission visited Jakarta from 29 October to 1 November 2007. The visit was facilitated by Microsoft Indonesia.

Discussions with representatives of the Department for ICT, the Parliament and a range of other stakeholders indicated that existing legislation (Penal Code, Criminal Procedure law, Law on Telecommunications, and others) can be used only to a limited extent to investigate and prosecute cybercrime. Efforts underway to develop a more coherent legal framework against cybercrime include in particular 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.

At the request received in the course of the visit, the CoE prepared a written analysis of the draft Act against the provisions of the Convention in November 2007.

The CoE also commissioned the translation of the Convention on Cybercrime into Bahasa in order to help stakeholders get a better understanding as to what is required.

2.2.8 Nigeria

Representatives of Nigeria participated in the Octopus Conference in June 2007. Further contacts resulted in a request for an analysis of the draft law which was initiated at the end of November 2007.

2.2.9 Philippines

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

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

As a result, in September 2007 the Philippines sent a letter to the Secretary General of the Council of Europe requesting accession to the Convention on Cybercrime. The consultations according to Article 37 of the Convention are now underway.

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 of the Philippines and the Council of Europe with the support of Microsoft in which some 60 representatives from public and private institutions participated.

The draft Bill discussed during the workshop was an updated version of the one reviewed by Council of Europe experts in April/May 2007, and already constitutes a very good basis. Workshop discussions resulted in a number of proposals for further improvements. Should these proposals be taken into account, the Philippines will have a law on cybercrime which could set an example for other countries of Asia.

2.2.10 Romania

Support to the National Cybercrime Training Conference in Romania (Pitesti, 27-29 November 2006): The project provided limited co-financing to a conference in

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

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

2.2.11 Russian Federation

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

2.2.12 Serbia

The Council of Europe provides 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 are not funded by the Project on Cybercrime but by the PACO Serbia project against economic crime of the Council of Europe and the European Agency for Reconstruction. They are nevertheless implemented as a contribution to the objectives of this project.

Activities during the period reviewed included i.a. 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).

In the coming months, additional specialised training sessions will be organised for practitioners on topics such as forensic investigation, computer emergency response team (CERT) and Child Exploitation Tracking System (CETS).

2.2.13 South Africa

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

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

The South African authorities are of the opinion – confirmed by a number of successful investigations – that the minimum legal basis is available following the adoption of the Electronic Communication and Transactions Act 25 of 2002 and the Regulation of Interception of Communications and Provision of Communication-related Information Act 70 of 2002:

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

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

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

Representatives from South Africa participated in the Octopus Conference in Strasbourg in June and informed that Convention would now be submitted to Parliament to approve ratification, while signature of the Protocol would be processed through a separate procedure.

2.2.14 South-eastern Europe

A regional conference on cybercrime was held in Belgrade from 19 to 21 March 2007 within the framework of the PACO Serbia project on Economic Crime.

Representatives from 16 countries and from international organisations and private sector bodies participated. Participants discussed the current state of cybercrime legislation, the functioning of international cooperation against cybercrime, including the creation of 24/7 points of contact, questions related to the investigation and prosecution of cybercrime as well as to public-private partnerships.

These issues were discussed against the background of the Council of Europe's Convention on Cybercrime (ETS 185) and the Additional Protocol on the Criminalisation of Acts of a Racist and Xenophobic Nature Committed through Computer Systems (ETS 189). From the then 19 Parties to the Convention, nine took part in the Conference, that is, Albania, Bosnia and Herzegovina, Bulgaria, Croatia, France, Hungary, Romania, Slovenia and "the former Yugoslav Republic of Macedonia‟.

In Serbia, action is being taken to amend criminal legislation, and the process of ratification of the Convention is expected to be completed in the very near future. The other countries participating in or contributing to the Conference were encouraged to ratify the Convention as soon as possible, namely Germany, Italy, Moldova, Montenegro, Turkey and the United Kingdom.

Discussions on the state of cybercrime legislation showed that a range of substantive and procedural measures have been introduced in participating countries in recent years which meet many of the requirements of the Convention, as reflected in the example of Romania. The harmonisation of national legislation with the Convention still needs to be completed in some of the countries. This is particular true for international cooperation and procedural law provisions. The Council of Europe was requested to support workshops on cybercrime legislation in Albania, Bosnia and Herzegovina, Bulgaria and "the former Yugoslav Republic of Macedonia".

With regard to the investigation, prosecution and adjudication of cybercrime considerable progress has been made in terms of specialisation and skills. Good practice includes the examples of France, Italy, Romania and the United Kingdom. Important efforts are also underway in Serbia – where a cybercrime prosecutor and court department have been appointed and the creation of a cybercrime investigation unit is underway – and other countries of South-eastern Europe. Further training and specialisation is required not only for investigators but also for prosecutors and judges.

The establishment of 24/7 points of contact was considered a very useful way of facilitating international cooperation as shown by the experience of the G8 24/7 Network and as required under Article 35 of the Convention on Cybercrime. Such contact points have been created in most of the participating countries, including Bulgaria, Croatia, France, Hungary, Italy, Romania, Slovenia, "the former Yugoslav Republic of Macedonia‟ and the United Kingdom. Serbia has designated a temporary contact point. The establishment of a contact point is underway in Albania. Bosnia and Herzegovina is encouraged to make a decision in the very near future.

The need for public-private partnerships was clearly recognised by all participants. Presentations by representatives of the Association of Internet Service Providers of Serbia and Microsoft pointed at the opportunities that such partnerships can offer to both public and private institutions.

In sum, participants underlined the need for a clear legal basis and effective cooperation against cybercrime at all levels – national, inter-agency, public-private and international – and the importance of the Convention on Cybercrime and its

Protocol in this respect. The exchange of experience and the contacts established during the Conference helped enhance such cooperation.

2.2.15 Ukraine

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

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

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

The establishment of 24/7 points of contact is considered a very useful way of facilitating international cooperation as shown by the experience of the G8 24/7 Network and as required under Article 35 of the Convention on Cybercrime. In Ukraine such a contact point does not yet exist but should be established as soon as possible in order to meet the requirements of the Convention.

2.3 Cooperation with other organisations

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

More than 140 cybercrime experts from some 55 countries, international organisations and the private sector met at the Council of Europe 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 specific impact of the Conference includes the merger of the directories of 24/7 contact points of the G8 and the Council of Europe, intensification of cooperation with the Philippines and many other countries in view of their accession, observer status to the London Action Plan, specific studies on cybercrime legislation, law enforcement-service provider cooperation, more intensive cooperation with the European Commission, and others.

In sum, the event added considerable momentum and credibility to the anti-cybercrime efforts of the Council of Europe.

2.3.2 Asia and Pacific Economic Cooperation

The Council of Europe 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 may also open the door for further cooperation with ASEAN.

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.

As follow-up, the CoE has already been invited to participate in next year’s conference which will foster its European dimension. Depending on the funding available, conferences of this type could be developed between the organisers and the CoE elsewhere in Europe such as in South-eastern Europe and Russia where there is a need for this type of awareness raising, networking and exchange of best practices among officials, practitioners from law enforcement and judiciary, academics, international organisations and private sector.

2.3.4 European Union (Portuguese Presidency) and European Commission

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

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

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

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

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

2.3.5 Europol

Europol participated in the Octopus Conference in June 2007. 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 held 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).

In a workshop session dedicated to training coordination held on 6 November, the CoE presented the training activities organised within the framework of the cybercrime project.

At the opening of the plenary session on 7 November, the organisers of the meeting invited the CoE to make a presentation on the state of play of the Convention on Cybercrime and activities related to cybercrime. The presentation was followed by several questions related to the provisions of the Convention and state of signatures and ratifications.

As a follow-up, Europol and CoE will continue to increase their common efforts, in particular, to develop a common understanding and cooperation between law enforcement and the private sector during the investigations.

2.3.6 G8 High-tech Crime Working Group: 24/7 Network of contact points

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 Council of Europe on this question.

The Octopus Interface Conference of June 2007 also included a workshop for contact points which was 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 Council of Europe with that of the G8. This proposal was agreed upon in November 2007. Specific details and procedures now need to be elaborated regarding the maintenance of the directory.

2.3.7 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 the cybersecurity strategy and called, among other things called for the development of model laws to ensure interoperability in the absence of international legal frameworks. The Convention on Cybercrime has been ignored.

Furthermore, the ITU decided to carry out an event in Vietnam on its own in August 2007; although this had been planned as a joint CoE/UNODC/ITU event since October 2006.

On the other hand, the CoE was invited to the ITU Workshop on Frameworks for National Action organised on 17 September 2007 in Geneva. Participants included officials from many European and non-European countries (including from Middle-East and Africa).

In October 2007, the ITU established a High-level Expert Group to advice the Secretary General of the ITU with regard to the cybersecurity strategy. The CoE was invited to the first meeting of this group, but the role and expected result of this group remain vague.

The "model law" part of the ITU cybersecurity strategy may be controversial. However, the discussion of that question in different fora (including the Internet Governance Forum) also had a positive effect in that it re-confirmed the Convention on Cybercrime as the global guideline for cybercrime legislation.

2.3.8 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.

Officials from Costa Rica, Brazil, Argentina expressed strong willingness to accede to the Convention soon while other participants from countries such as El Salvador, Kuwait, Israel, Lesotho, Tunisia and many others showed serious interest towards the Convention and for direct bilateral follow-up with the Council of Europe.

Contact was established by the Deputy Secretary General of the CoE with the Indian authorities responsible for the next IGF in Delhi in December 2008. That event could help promote the accession of India to the Convention on Cybercrime.

2.3.9 Interpol

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

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

> *The delegates at the 7th International Conference on Cyber Crime recommend:*
>
> - *That the Convention on Cyber Crime of the Council of Europe shall be recommended as providing the international legal and procedural standard for fighting cyber crime. Countries shall be encouraged to join it.*

2.3.10 London Action Plan

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

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

2.3.11 Organisation of American States

The OAS had supported the implementation of the Convention on Cybercrime among its 34 member states for some years. The Council of Europe 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).

The Dominican Republic adopted a new law on cybercrime in 2007 which is very much inspired by the Convention and accession can be sought once Congress approves ratification. A workshop is envisaged to be held in February 2008 in order to create a political momentum in this respect.

A number of other countries expressed interest in receiving support from the Council of Europe such as Bahamas, Mexico, Nicaragua and Peru.

Moreover, basic agreement was reached to hold a joint OAS/Council of Europe event on cybercrime legislation for the 34 OAS countries, possibly in June 2008 in Cartagena, Colombia.

2.3.12 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 Council of Europe. 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.

2.3.13 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).

The idea of a joint event of the CoE, UNODC and the ITU which had been planned for August 2007 in Vietnam was cancelled due to the ITU deciding to organise this event on its own.

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

2.4 Studies

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

1. Cybercrime situation report ("Current threats and trends and the adequacy of the international response")	The study should provide policy makers with an up-to-date analysis of current cybercrime threats and trends and of how these can be addressed by implementing existing international instruments. It should furthermore provide an assessment as to whether existing instruments are commensurate to these threats and trends. The study will also feed into the work of the Cybercrime Convention Committee (T-CY) of the Council of Europe. The study is currently being carried out by researchers from France and the Netherlands.
2. Study on cybercrime legislation ("Legislation implementing the Convention on Cybercrime: comparative analysis of good practices and effectiveness")	The study should serve as a resource for countries that are in the process of strengthening their national legislation against cybercrime in line with the Convention. The study is underway and carried out by research institute in Verona, Italy.
3. Study on the role of service providers ("Cooperation between service providers and law enforcement against cybercrime: towards common guidelines?")	The study is aimed at facilitating the cooperation between service providers and law enforcement in the prevention and investigation of cybercrimes. It should include a proposal for common guidelines for such cooperation for further discussion at the cybercrime conference on 1-2 April 2008 and the Cybercrime Convention Committee (T-CY) of the Council of Europe on 3-4 April 2008. A working group was established and held its first meeting in Paris on 22 October 2007.
4. Study on international cooperation ("The effectiveness of international cooperation against cybercrime: examples of good practice")	The study is to help countries make better use of the international cooperation provisions of the Convention on Cybercrime, including Article 35 on 24/7 points of contact. This study is being carried out by an expert from Portugal.
5. Study on data protection ("Investigating cybercrime and the protection of personal data and privacy")	The purpose of the paper would be 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 is being carried out by a researcher from the Netherlands.

3 Results

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

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

Even the controversial discussions on the proposal of the International Telecommunication Union to develop a "model law" helped re-confirm the Convention as the global guideline for cybercrime legislation.

3.1 Output 1: Legislation

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

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

Specific advice on draft laws was provided to:

- Argentina (workshop in November 2007 with subsequent analysis of draft legislation)
- Brazil (review and comments on draft legislation in February 2007)
- Colombia (workshop reviewing the draft law in October 2007)
- Egypt (meetings with public authorities in February 2007, written analysis of the draft law in May 2007 and follow up conference and discussions in November 2007)
- India (meetings with public authorities in February 2007, written analysis of the draft law in May 2007 and follow up discussions in September 2007)
- Indonesia (meetings with public authorities and written analysis of the draft law in November 2007)
- Pakistan (analysis of the draft law in February 2007)
- Philippines (written analysis of the draft law in June 2007 and a follow up workshop resulting in additional comments in October 2007)
- Serbia (series of workshops in 2006/7 and a written analysis of legislation in October 2007).

Cooperation with Morocco was initiated in June 2007 and draft criminal law provisions are now being analysed.

Meetings with representatives from countries of central, eastern and south-eastern Europe also indicated that further legislative work is required in countries that already ratified the Convention, such as in Albania, Bosnia and Herzegovina, "the Former Yugoslav Republic of Macedonia" and Ukraine. In Bulgaria amendments to existing legislation are underway and a workshop to analyse these amendments will take place in December 2007.

In order to facilitate the analysis of cybercrime legislation against the provision of the Convention, "profiles" have been prepared for more than 40 countries of which 22 have been published in June 2007. The profiles for countries that have ratified the Convention were reviewed and improved in November 2007 and will serve as bases for in-country workshops which are to be conducted in the coming months and which will be aimed at further improving cybercrime legislation.

The Dominican Republic and Sri Lanka adopted new legislation in 2007 with the Dominican Republic following very closely and Sri Lanka to some extent the Convention. Legislative work guided by the Convention is furthermore underway in countries such as Lebanon, Senegal and Thailand. Interest for assistance to the review of legislation has also been expressed by many other countries from around the world and may lead to specific cooperation in 2008.

In sum, the legislative processes that the project was able to support and initiate in 2006/7 exceeded the expectations, in particular considering that with many of the non-European countries, the CoE had little contact before. The Convention is used as a guideline or "model law" in a large number of countries.

In terms of additional ratifications by European countries, the progress made has been less satisfying although legislative work is underway in many of them. While in 2006 seven countries deposited the instrument of ratification, in 2007 (by November) only three additional countries became parties to the Convention. In two additional countries (Germany and Slovakia) parliaments ratified this treaty in the second half of 2007 and they are expected to deposit the instrument shortly. Nevertheless, half of the European Union member States still need to ratify this Convention. The call for ratification of the EU Justice and Home Affairs Council of November 2007 may help accelerate this process. Eight member States of the Council of Europe have not yet signed the Convention.

Ratification of the Convention on Cybercrime since November 2001

Year	Year 1	Year 2	Year 3	Year 4	Year 5	Year 6
	2002	2003	2004	2005	2006	2007
Add. ratif.	+ 2	+2	+4	+3	+7	+3
Total	2	4	8	11	18	21

Regarding the Protocol on Xenophobia and Racism the number, four additional countries ratified this instrument in 2007 and the total number now stands at eleven, while 20 others have signed it.

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[1], that the

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

implementation of procedural law measures (of which the Conventions contains more than other international treaties) takes time, and that countries are expected to have the legislation in place and adopted by parliaments by the time of ratification. On the other hand, it also appears that in some countries the question of cybercrime – in spite of its significance – is not given the necessary priority.

Status of signatures and ratifications of the Convention on Cybercrime (November 2007)

Ratified (21):

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

Signed (22):

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

Not signed (8 CoE member States):

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

Invited to accede (2):

- Costa Rica
- Mexico

Request for accession (1):

- Philippines

3.2 Output 2: Criminal justice capacities

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

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.

A particular problem identified in different countries is related to the need for law enforcement to cooperate with service providers in the investigation of cybercrimes. A study has been launched and a working group has been created in order to develop guidelines in this respect which could be applied in any country.

While law enforcement officers of many countries have made much progress in developing their subject-matter skills and while this is also partly true for prosecutors, the judiciary is clearly lacking behind. Steps have therefore been taken by the project to develop training modules for judges. A first training event will be held in Bulgaria in mid-December 2007.

3.3 Output 3: International cooperation

Capacities of criminal justice bodies to cooperate internationally re-enforced

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

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

In October 2007, a study was launched which is to document good practices in the implementation of the international cooperation provisions of the Convention. The results should be available by April 2008.

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

The risk of competing networks or a multiplication of contact points and networks was reduced by reaching an understanding in November 2007 with the G8 subgroup to merge the directories of contact points of the CoE and the G8.

4 The way ahead

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

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

The momentum created by the project now provides unique opportunities to make an impact around the world between December 2007 and the scheduled end of the project in February 2009.

By the end of 2008, the project should be evaluated and proposals should be prepared with regard to future technical cooperation activities of the Council of Europe in the field of cybercrime.

4.1 Priorities in 2008[2]

In general terms, the successful approach chosen by the project will remain the same:

- Cooperation will continue to be sought with a broad range of organisations (such as the United Nations, the OAS, Interpol, Europol and many others) as a cost-effective means to reach maximum outreach and impact. This will also facilitate the involvement in discussions on the development of additional international and European standards, for example on the question of identity theft, attacks against critical infrastructure or the question of privacy which will gain in importance in the near future.
- Strong cooperation with the private sector will be sought. The preparation of the guidelines on law enforcement/service provider cooperation should be instrumental in this respect.

A global Octopus Conference will be held in Strasbourg on 1-2 April 2007 which will add impetus to the objectives and expected results of the project. It will be followed by the 3rd Consultations of the Parties to the Convention (the T-CY) on 3-4 April.

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

As in 2006/7, the Convention will be promoted as a guideline or "model law" for the development of cybercrime legislation around the world.

A study analysing the implementation the provisions of the Convention on Cybercrime will be finalised by April 2008.

[2] While funding is available to cover activities up to April 2008, the implementation of the project beyond April is subject to the availability of further contributions (see the relevant section below).

While the promotion of ratification and accession to the Convention will remain essential, more focus will be put on the actual implementation of the provisions of the Convention. In addition to the studies that are underway, other practical tools will need to be developed.

The preparation of country profiles on cybercrime legislation will be expanded to cover new countries, and the existing ones will be improved. These help share good practices and examples of cybercrime legislation and serve as a starting point for the analysis of legislation against the provisions of the Convention.

More emphasis will be put on the implementation of the Protocol on Xenophobia and Racism.

Specific activities will be carried out related to Article 9 (child pornography) in conjunction with the new Convention on the Sexual Abuse and Exploitation of Children (CETS 201).

In Europe, activities will focus on promoting ratification of countries that are not yet party (EU member States, Moldova, Montenegro, Russia, Turkey and others). In European countries that are already parties, workshops will be carried out to enhance the effectiveness of cybercrime legislation, such as in Albania, Bosnia and Herzegovina, Bulgaria and "the former Yugoslav Republic of Macedonia").

In Africa, cooperation with Egypt, Morocco and South Africa will continue. Additional countries such as Nigeria and Senegal will be supported.

Opportunities with other countries of the Arab region will explored.

In the Americas, cooperation will continue with Argentina, Brazil Colombia, Costa Rica, Dominican Republic and Mexico in view of accession. A workshop with the 34 member States of the Organisation of American States will help promote the strengthening of legislation throughout this region.

In Asia and Pacific, work will continue with India, Indonesia and the Philippines. The accession by countries where relevant legislation already exists will be promoted (such as Australia, New Zealand, Singapore, Sri Lanka). Cooperation with ASEAN will be sought in view of legislative reforms throughout this region.

The project will contribute to the Internet Governance Forum in India in December 2008.

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

Guidelines for the cooperation between law enforcement and service providers are to be finalised and subsequently to be disseminated around the world. This will support the implementation of the procedural provisions of the Convention.

A study on the question of data protection/privacy in the investigation of cybercrime will be completed in April and may lead to further activities in this regard.

The Council of Europe will contribute to the training of investigators and prosecutors through this project and activities organised by other organisations.

The project will carry out a series of activities aimed at the training of the judiciary. The first event will be held in Bulgaria on 17-18 December 2007 and will help develop a training module that can subsequently be delivered in other countries. Other activities will follow in the second half of 2008 should funding be available.

4.1.3 International cooperation

A study on good practices in the implementation of the international cooperation provisions of the Convention will be completed by April 2008.

In cooperation with the G8 High-tech Crime Subgroup, the project will help maintain the Directory of Contact Points.

Specific training activities will be carried out in order to strengthen the effectiveness of existing contact points.

In countries that have ratified the Convention but have not yet established such contact points their creation will be promoted.

4.2 Activities proposed (December 2007 – June 2008)

Date	Place	Description
Oct 2007 – April 2008	Strasbourg and others	Studies on cybercrime legislation, situation report, law enforcement – service provider cooperation, international cooperation, privacy
13-14 Dec 2007	The Hague, Netherlands	ILC public-private cooperation meeting
17-18 Dec 2007	Bulgaria	Training workshop for judges (Bulgaria, Romania, Serbia and "the former Yugoslav Republic of Macedonia", and review of the cybercrime legislation
Dec 2007	Strasbourg	Analysis of the cybercrime legislation of Nigeria
Jan 2008	Kosovo	Legislative assistance workshop
Jan 2008	Georgia	Legislative assistance workshop
	Albania	Workshop on cybercrime legislation and investigation
Feb 2008 (tbc)	Senegal	Legislative assistance workshop
Feb 2008	Morocco	Workshop on cybercrime legislation and investigation
7 Feb 2008	Düsseldorf, Germany	Study on law enforcement – service provider cooperation: 2nd meeting of the working group
March 2008	Dominican Republic	Workshop to review legislation and promote accession to the Convention
Feb 2008	Montenegro	Legislative assistance workshop
20-21 Feb 2008	London	McAfee cybersecurity meeting
March 2008	"the former Yugoslav Republic of	Workshop on cybercrime legislation and investigation

	Macedonia”	
March 2008	Bosnia and Herzegovina	Legislative assistance workshop
1-2 April 2008	Strasbourg	Octopus Interface Conference on cybercrime (to be followed by Cybercrime Convention Committee on 3-4 April 2007)
May 2008	Europe (place tbc)	Workshop for 24/7 contact points of European countries
Apr – June 2008	Africa	Up to 2 legislative assistance workshops
Apr – June 2008	Asia and Pacific	Up to 3 legislative assistance workshops
Apr – June 2008	Arab region	Up to 2 legislative assistance workshops
Apr – June 2008	Americas	Up to 2 legislative assistance workshops
18 – 23 May 2008	Australia	AusCERT annual Asia-Pacific Information Security Conference
June 2008	Colombia (TBC)	OAS/CoE regional conference on cybercrime legislation for 34 OAS member States
Dec 2007 – June 2007	Global	Participation in events organized by other organisations

4.3 Cooperation with Microsoft

Project activities in 2006 and 2007 were funded by voluntary contributions from Microsoft and the budget of the Council of Europe (Project 143 on Economic Crime). 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 Council of Europe
- They promoted the implementation of the Convention through events organised by Microsoft; and the CoE was invited to participate in a number of these
- They made use of the Convention in order to analyse the legal framework of countries of Asia and the Pacific
- They carried out a number of activities related to child protection and promoted the implementation of Article 9 on child pornography of the Convention on Cybercrime and now also take into account the new Convention on the sexual exploitation and abuse of children (ETS 201)
- Microsoft is supporting the study on law enforcement-service provider cooperation and facilitated the participation of other service providers in the working group established by the CoE that is aimed at developing draft guidelines for such cooperation.[3]

The cooperation between Microsoft and the CoE has been very pragmatic and result-oriented. A continuation of this partnership in 2008/9 should be in the interest of both parties. At the same time, funding from other public and private sector institutions should be sought.

[3] In addition to Microsoft, eBay, British Telecom, Telefonica and different service provider associations also participate in this working group.