COUNCIL OF EUROPE CONSEIL DE L'EUROPE

Global Project on Cybercrime (phase 2)

Update July 2010 – December 2010

Date: 21 Jan 2011

PROJECT SUMMARY

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 Estonia, Monaco, Romania, Microsoft and McAfee
Implementation	Economic Crime Division (Directorate General of Human Rights and Legal Affairs, Council of Europe)
Duration	28 months (1 March 2009 – 30 June 2011)
Project objective	To promote broad implementation of the Convention on Cybercrime (ETS 185) and its Protocol on Xenophobia and Racism (ETS 189) and related international standards
Output 1	Legislation and policies: Cybercrime policies and legislation strengthened in accordance with the Convention on Cybercrime and its Protocol
Output 2	International cooperation: Capacities of 24/7 points of contact, prosecutors and of authorities for mutual legal assistance strengthened
Output 3	Investigation: Law enforcement – service provider cooperation in the investigation of cybercrime improved on the basis of the guidelines adopted in April 2008
Output 4	Financial investigations: enhanced knowledge among high tech crime units and FIUs to follow money flows on the internet
Output 5	Training: Judges and prosecutors trained in the adjudication and prosecution of cybercrime
Output 6	Data protection and privacy: Data protection and privacy regulations in connection with cybercrime investigations improved in line with CoE and other relevant international standards
Output 7	Exploitation of children and trafficking in human beings: Enhanced knowledge of standards against the sexual exploitation and abuse of children and trafficking in human beings on the internet

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

Tel +33-3-8841-2103
Fax +33-3-9021-5650
Email Cristina.SCHULMAN@coe.int

ACTIVITIES CARRIED OUT BETWEEN 1 JULY - 30 DECEMBER 2010

Date	Place	Activity	Output
1 July 10	Brussels	**Participation in the EU cybercrime experts group on statistics** Under the proposed EU Directive on Attacks against Information Systems EU Member States will be required to report offences and submit statistical data. The Council of Europe is a member of the expert group preparing a proposal in this respect. In this first meeting it was agreed that the reporting should be based on the offences that are common in the Budapest Convention and in the Directive.	1
2 July 10	Paris	**Contribution to the training course for judges at the Ecole National de la Magistrature in France** Council of Europe presentation in this training course on challenges for judges and public-private cooperation in relation to cybercrime investigations	5
12 -13 July 10	Phnom Penh, Cambodia	**Workshops on cybercrime legislation in Cambodia** In view of strengthening cybercrime legislation in Cambodia a workshop was held in Phnom Penh on 13 July 2010 at the premises of the Council of Ministers for some 130 representatives from governmental institutions, the private sector, international organizations and embassies. The workshop was organized by the Cybercrime Law Formulation Working Group under the Council of Ministers and the Council of Europe. The aim was to create awareness of the need for cybercrime legislation, to discuss what type of legislation was needed and to develop proposals with regard to the steps to be taken and the approach to be pursued. It was preceded by a detailed discussion on 12 July on existing and planned legislation between the Working Group and the CoE representative. On 14 July, further discussions were held with individual members of the Working Group. Following the workshop on 13 July, the Working Group will prepare a report to the Council of Ministers with a recommended course of action. The current legal framework regarding information technologies is rather weak. Recent incidents, including data breaches, website defacements – some affecting governmental websites – led to the Government making the question of cybercrime a higher priority. Presentations during the workshop – including private sector interventions – clearly underlined the need for action. The proposal coming from the workshop was that the most effective way ahead would be the preparation of a special cybercrime law covering substantive and procedural law provisions (including safeguards and conditions) based on the Budapest Convention and supplementing the existing Criminal and Criminal Procedure Codes.	1

		Subject to a decision by the Council of Ministers, the Working Group could prepare a first draft as a basis for further discussion with different stakeholders, including the Ministry of Post and Telecommunication, Ministry of Commerce, Ministry of Interior, the private sector and others. The Working Group may also seek further advice from the Council of Europe. Once a draft is available the Council of Europe could contribute to a follow up workshop to assist in the finalization of the draft law. Participants in the workshop furthermore underlined that legislation was only one step. Elements of the way ahead would include: 1. Legislation (criminalise conduct, procedural law/tools for investigation, safeguards) 2. Creation of a high-tech crime unit as well further as specialisation of law enforcement and criminal justice authorities 3. Law enforcement training 4. Judicial training (judges, prosecutors) 5. Public-private (LEA-ISP) cooperation 6. Effective international cooperation 7. Protection of children 8. Data protection	
27-29 July 10	Rabat	**Atelier de formation sur l'harmonisation du cadre légal pour la cybersécurité en Afrique du Nord** The aim of this workshop was to promote harmonization of cybercrime legislation in countries of Northern Africa. It was organized jointly by the United Nations Economic Commission for Africa (UNECA), the Council of Europe and Microsoft. Participants included some 35 representatives from Algeria, Mauretania, Morocco, Senegal, Tunisia, the African Development Bank, the United Nations Development Programme (UNDP), the Economic Community of the States of Central Africa, the Islamic Organisation for Education, Science and Culture, Union du Maghreb Arabe, the UN Economic and Social Commission for Western Asia, the UNECA Sub-regional Office for Central Africa and the Office for Northern Africa, Microsoft and the Council of Europe. The Council of Europe had provided the concept of the workshop, including the agenda and working documents, as well as two speakers (a cybercrime prosecutor from Belgium and the head of the Economic Crime Division of the Council of Europe), who took responsibility for a large share of the sessions. Results: - The workshop confirmed that Algeria and Senegal have adopted legislation which is largely in line with the Budapest Convention on	1

		Cybercrime. Algeria in particular followed closely the Budapest Convention, especially with regard to procedural law (Law 09-04 of August 2009). - In Morocco, the judicial system is undergoing a major reform. This includes the preparation of new criminal and criminal procedures codes. It will take some time until these reforms are completed and thus for Morocco to have legislation in compliance with the Budapest Convention. Laws in force reflect some substantive criminal law provisions already. - The workshop showed that while reforms are underway in many countries, there are serious risks. Several speakers pointed at initiatives underway in several regions of Africa (e.g. ECOWAS) to develop regional agreements covering information technology laws, including cybercrime, e-commerce, electronic transactions, data protection and others. The ambition seems to be that this would lead to an African Union Convention on Cybersecurity by 2012. Meeting in Abuja… This approach carries risks in that it could lead to standards not in line with other international norms, in particular the Budapest Convention, that it is too ambitious to be adopted and implemented, and that reforms will be delayed in many countries. - At the same time, the workshop underlined the usefulness of the Budapest Convention, that it already serves many countries as the basis for their reforms and that this treaty should be taken into account as the minimum standard by any initiative in Africa. - On the other hand, while the Budapest Convention is technically made use of, there remains the political argument that African countries were not involved in its preparation. - In addition to the Budapest Convention, the guidelines for law enforcement – ISP cooperation and the judicial training concept were very much welcomed by participants. In Morocco, the training concept is already being made use of and it is envisaged to train up to 600 judges and prosecutors in the near future. - Data protection is another field of great interest in Africa. Morocco and Senegal already seem to have legislation in place in line with Convention 108. Follow up: - The Council of Europe should provide targeted support to countries in their reform of legislation. - A dialogue should be sought with the African Union Commission as well as regional bodies with regard to initiatives aimed at regional agreements. - As indicated in the past, an Africa-specific support programme comprising legislation, training, institution building, public-private as well as international cooperation would be desireable. It should also contain elements related to the prevention of terrorist use of the Internet and rule of law and human rights standards.	
30 Nov-2 Dec 10	Abuja, Nigeria	**1st West Africa Cybercrime Summit** The Council of Europe participated with an expert from Senegal in this meeting.	1

		The event helped re-launch discussion of the draft cybercrime laws in Nigeria, but it appeared that the time before the elections in Spring 2011 was too short to have the bills harmonised and adopted.	
25-27 August 2010*	Mexico City, Mexico	**Regional workshop on cybercrime to promote the strengthening of cybercrime legislation and accession to the Budapest Convention in Mexico and other countries of Latin America** The workshop was largely funded with a contribution from Microsoft. Some 60 cybersecurity experts from Mexico, Argentina, Colombia, Costa Rica, Paraguay, and Peru, as well as the private sector participated in the event. A specific session for Mexican representatives was held on Wednesday, 25 August. The countries selected have either been invited to accede already (Argentina (on 16 Sep 10), Costa Rica and Mexico, or are in the process of reforming their legislation in line with the Budapest Convention and are thus open to consider accession (Colombia, Paraguay and Peru). Chile was invited to the workshop but finally did not participate (and had been invited to accede to the Convention in 2009). The workshop achieved its objectives in terms of accelerating legal reforms and accession to the Budapest Convention: - Mexico: The Intersecretarial Group on Cybersecurity decided to establish an sub-group on legislation in order to accelerate the preparation of legislative amendments (probably based on the draft prepared by the Office of the Prosecutor General) - Argentina: will complete the reform of the Criminal Procedure Code in view of early accession to the Convention. Specific measures will be taken on public-private cooperation and judicial training. The CoE is invited to contribute to an important event in October. - Colombia: Political consultations regarding accession will now be initiated. - Costa Rica: A draft law on cybercrime is now available and the political leadership including parliament is being mobilized with the support of the President of the country. - Paraguay: a strategy on cybercrime is being established and the penal legislation is being reformed. The CoE is requested to support a workshop on cybercrime legislation which would also serve to obtain high-level political support to legislative reform and accession to the Convention. - Peru: Draft laws have been prepared and as a result of the workshop these will be further improved and sent to the government for approval before going to the parliament.	1, 2
7-8 Sep 10	Baku, Azerbaijan	**OSCE: National Expert Workshop on a Comprehensive Approach to Cyber Security** Representatives from government agencies, international organizations and civil society participated in the event. The objective was to assist	1

		Azerbaijan's government in the implementation of the Council of Europe Convention on Cybercrime and in adopting of a consistent policy on cybersecurity, including cybercrime. Governmental representatives from Azerbaijan recognized the need to review the criminal legislation, ensure efficient law enforcement measures and establish a better co-operation with Internet service providers. The CoE presentation focused on the approach taken under the global project on cybercrime in assisting countries worldwide to take measures against cybercrime and further steps to be taken by Azerbaijan to implement the Budapest Convention. On this occasion meetings were held with possible donors and representatives from national institutions to discuss the feasibility of developing a specific project on cybercrime in Azerbaijan and strengthening the cooperation on this matter between the CoE and Azerbaijan.	
8-9 Sep 10	London, UK	**SANS European Digital Forensics and Incident Response Summit** Representatives from government, private sector, forensic experts, auditing organizations and other stakeholders participated in the event. The CoE representative addressed some questions stressing that: a) Cybercrime is not a specific type of crime but can be any crime, including drugs, murder and violence. Retrieval of evidence involves ICT. b) Digital material to be used as evidence is *per definitionem* forensic material and should treated accordingly. c) Cybercrime is nearly always cross-border and requires international co-operation. d) The Council of Europe is the international organization that adopted the Cybercrime Convention and its First Additional Protocol. The CoE is through its cybercrime projects active in promoting the Cybercrime Convention as the global instrument for international co-operation in cybercrime matters. e) If digital evidence is admissible before a national court depends in the first place from domestic law of criminal evidence. Gathering of digital evidence on the request of another state should take into account the conditions that the law of the requesting state poses (see R (95) 13). f) Internationally recognized standards should be developed for the gathering, preservation, analysis, elaboration, presentation and making available to process parties. Such standards could be developed by SANS and other international groups, in all cases in co-operation with LEA and the legal profession. Such activity could be taken up by the European Union (e.g. EUROJUST) for this part of the world. One of the issues raised during discussions was about the duty to report data breaches as incorporated in US-law and about to be incorporated in the draft EU privacy directive with regard to e-	2

		communications. It was questioned if the effect would be disproportional concerning the image damaging of the company in question. A number of questions were about the impact of privacy legislation, as an impediment of forensics. Some LEA representatives claimed that the legislation was too restricted where it comes to the right of LEA to preserve personal data. The regulation of the processing of personal data held by the police depends on national legislation. Besides Convention 108 and the CoE Recommendation on the matter national legislator should seek harmonized EU-regulation on the matter. It was also stressed the need for development of international standards with regard to forensics.	
12-15 Sep 10	Bucharest	**The 13th International Forum for Public Prosecutors on the Fight against Organized Cross-Border Crime** The event was organised by TAIEX, DG Enlargement in cooperation with the Prosecutor's Office attached to the High Court of Cassation and Justice of Romania and the General Public Prosecutor's Officeof the Free State of Saxony, Germany. The CoE representative contributed on the topic "The cooperation between law enforcement and private sector on combating fraud and illegal trade on the internet".	2
14-17 Sep 10	Vilnius	**Internet Governance Forum** Under the overall theme "developing the future together' the discussions reflected the contribution of the IGF in the past four years to help governments, civil society, the private sector, technical community, and international organizations to understand the challenges and potential solutions to the digital divide considering its central aim to afford all people the benefits of the Internet. Discussions in Vilnius examined: - Managing critical Internet resources; - Access and diversity; - Security, openness and privacy; - Internet governance for development; - Emerging issues: cloud computing. - Parallel to the main sessions on these issues, workshops, best practice forums, dynamic coalition meetings and open forums were held around the broad themes of the main sessions. During the whole event it was highlighted the value of the Council of Europe's legal instruments that address the challenges of evolving technology and complement the main human rights instruments. These instruments are not meant for Europe only but they contain standards that are inspiring legislations and policies around the globe. Events and results related to cybercrime included: **"Grand Coalition" meeting of key players in online child safety (Monday, 13 Sep 10)**	All

		The European NGO alliance for Child Safety Online (eNACSO) convened the meeting to bring together as many as possible of the key stakeholders around the world who are engaged in the debates and research around children's use of the internet and associated technologies. Participants: European Commission, ITU, UNICEF, Council of Europe, Council of Baltic States, UNODC, European Network and Information Security Agency, European Broadcasting Union, Interpol, Europol, ICMEC, Commonwealth IGF/Commonwealth Security Organization, Cyber Peace Initiative/Arab Safety Portal, GSMA, INHOPE, FOSI, ECPAT International, EU Kids Online, CHIS, Save the Children, INSAFE, ISafe4Kids, LSE, University of Edinburgh, Oxford Internet Institute, University of New Hampshire, eNACSO. The aim of the meeting was to exchange information on the work that different stakeholders are undertaken to address online protection of children and identify gaps in the activities currently taking place or planned. The discussion tackled: - the risks pose by Internet for children, mostly from the perspective of social and cultural implications; - what would be the focus of such research? - what methodology? - could European and US standards be extended in different countries from other continents? - It was underlined in the meeting that CoE work includes various aspects related to protection of children covering educational, preventive and legislative measures. Although the standards developed at the CoE level are mainly implemented in its Member States - through the global Project on cybercrime - the CoE promote both the Budapest Convention on Cybercrime and the Convention on Protection of Children against Sexual Exploitation and Sexual Abuse at the global level aiming to harmonise legislation and ensure a framework for international cooperation. - To ensure globally adequate criminalisation in order to protect children from sexual abuse and sexual exploitation is crucial and the CoE is prepared to work with other stakeholders on these issues. **Workshop 123: Legal Aspects of Internet Governance: International Cooperation on Cyber-security (Wednesday, 15 Sep 10)** Workshop focused on (i) legal aspects and (ii) international cooperation regarding those legal aspects. The discussions showed that: - Progress has been made in the way industry, government and law enforcement cooperate, coordinate and share information. - In order to advance there is a need to define more clearly who are the partners in this partnership, what are their roles and authority. - What can they do – and on what legal basis or mandate – to	

prevent and disrupt attacks, prosecute criminals, investigate fraud and confiscate crime proceeds?

- It was pointed out that a distinction should be made between the concepts of "cybersecurity" (aimed at protection IT systems) and criminal justice measures against "cybercrime" (aimed protecting the security and rights of people).
- Instruments and tools against cybercrime are already available. Capacity building to help countries implement them should be given priority. Cybercrime should be addressed by development cooperation agencies (including the World Bank that organised the workshop).
- The World Bank now intends to participate in the next Octopus conference.
- The creation of a mechanism to review needs and assess progress made could be considered.

Workshop 23: Cybercrime: common standards and joint action (Wednesday, 15 Sep 10)

The CoE was the organizer of this workshop and benefited from the contribution of several experts (Markko Künnapu/Estonia, Rusudan Mikhelidze/Georgia, Zahid Jamil/ Pakistan, Jayantha Fernando/Sri Lanka, Laurent Masson/Microsoft)

Some 90 participants participated and others had joined through remote hub and had raised questions (Argentina, Burundi, Cameroon and Pakistan).

The event underlined that legislation is essential to help societies meet the challenge of cybercrime. The implementation of the Budapest Convention in connection with other relevant instruments and tools developed at the Council of Europe level provide a global guideline in this respect.

The workshop demonstrated that common standards are available to undertake joint action against cybercrime. Examples from Georgia, Estonia, Pakistan, Sri Lanka as well as private sector initiatives (Microsoft) provided evidence to this effect. These examples could be replicated worldwide.

The discussions underlined the value of the Budapest Convention as a common standard and framework for joint action against cybercrime at the global level. This is particularly true for developing legislation, investigations and international cooperation.

Other tools and instruments can complement the Budapest Convention, such as the Convention on Prevention Terrorism, Convention on Protection of Children against Sexual Exploitation and Sexual Abuse, Convention on the Protection of Individuals with regard to the Automatic Processing of Personal Data). Additional tools have been developed to ensure adequate legislation, training for judges or prosecutors and public-private cooperation.

There was agreement that countries worldwide need to be supported through technical assistance in order to establish the necessary

		capacities to apply existing standards and tools. Official development aid agencies need to make cybercrime a topic of development cooperation. The workshop identified the need for stronger commitment from political leaders with regard to measures against cybercrime. The creation of a mechanism ("Cybercrime Action Task Force") to identify needs, mobilise resources for capacity building, assess progress made by countries and thus to generate stronger commitment could be given further consideration. **Main session workshop on Security, Openess and Privacy (Thursday, 16 Sep 10)** The CoE intervention on security focused on the lessons learnt from workshops 172 on public private cooperation for cyber safety (organized by the Netherlands), workshop 123 on international cooperation on cybersecurity (organized by the World Bank) and workshop 23 on cybercrime (organized by the CoE). Key points presented: - Tools, common standards, good practices are available and applied by many countries. Full implementation is the most effective and pragmatic way ahead (e.g. Budapest Convention on Cybercrime around which many tools are being built). - Need for capacity building to help countries implement what is already there. - Stronger contribution from development cooperation agencies. - There are many examples for multi-stakeholder cooperation, including public-private cooperation. - Measures against cybercrime are composed of many elements, prevention and awareness, technology, but also criminal justice measures. - Criminal law to be in place not only to prosecute criminals and deter crime, but also to prevent abuse of power, establish safeguards and conditions in procedural law, ensure that due process is followed and that human rights and the rule of law are respected. - Countries are very cautious when designing criminal law measures. - Need for stronger cooperation between the ICT and criminal justice communities when dealing with cybercrime; not only at the domestic level but also the international level. - Consider a mechanism (a sort of "cybercrime action task force") to mobilize resources for capacity building but also for monitoring progress made by countries in their measures against cybercrime. **Next IGF meeting** The mandate of the IGF is likely to be extended and the next IGF meeting will take place in Kenya.	
20 Sep 10	Yogyakarta City – Central	**International seminar in Yogaykarta on "prosecuting cybercrime: collecting and presenting digital evidence"**	1

	Java, Indonesia	Some 170 participants from different regions of Indonesia, including telecom sector, judges, prosecutors, police, academia and private sector participated in this event organised by the Department of Communication and Information Technology of Indonesia to which the Council of Europe contributed. In addition, a bilateral meeting was held at the Parliament. Following a first CoE mission in November 2007, a written analysis and translation of the Budapest Convention into Bahasa, the then draft law on Electronic Information and Transaction was considerably improved to reflect the substantive law provisions of the Budapest Convention and subsequently adopted by the Parliament in 2008 (Act 11/2008 on Electronic Information and Transaction). In 2008 and 2009, the DepKomInfo worked on a draft law on cybercrime to fill the gaps regarding in particular procedural law. This draft law was discussed with the CoE on several occasions (workshop in Strasbourg in March 2009, ASEAN workshop on cybercrime legislation in January 2010, discussions with the Indonesian delegation in Strasbourg in March 2010 where they also met the DSG). Four drafts are now on the priority list of the Parliament for 2010: - Draft law on cybercrime covering in particular procedural law measures - Amendments to Act 11/2008 on Electronic Information and Transaction (remove the legal interception provision and regulate it in the draft law on cybercrime; reduce the penalties for defamation). - Convergence law - Law on Ratification of Budapest Convention They are still with the DepKomInfo and have not yet been submitted to the Parliament. In the coming weeks, they will be reviewed by the Law Ministry and are expected to be submitted to the Parliament before the end of 2010. Results: - The meeting at the Parliament helped alert the Vice-Chair of Committee 1 that is responsible for cybercrime matters of the importance of speedy adoption of the draft laws one submitted to parliament. The availability of the CoE was confirmed to provide further advice in the process if necessary. - The Vice-Chair and the DG of DepKomInfo confirmed the intention of Indonesia to seek accession to the Budapest Convention (even if the Ministry of Foreign Affairs is favouring a UN treaty on cybercrime at the same timer). Once the laws are in Parliament, that would be the most appropriate moment to send a request to the SG of the CoE to initiate informal consultations. - The seminar in Yogyakarta strongly promoted the Budapest Convention and confirmed that current and draft laws are largely in compliance with the Budapest Convention, but also pointed at certain issues to be further improved (e.g. provisions on preservation vs retention are to be clarified). - Both, meetings showed that Indonesia is concerned about human rights and rule of law standards, including safeguards and	

		conditions (as reflected in a public discussion on legal interception [question of independent judicial supervision] and the broad agreement to reduce penalties for defamation). - Confirmed the need for further training of judges and prosecutors (along the concept developed by the CoE Project on Cybercrime). - The meeting showed the wisdom of an approach combining global (Octopus), regional (ASEAN) and country-specific activities. The relations between Indonesia and Malaysia are currently tense, and thus more can be achieved working bi-laterally with these countries at this point.	
4-5 Oct 10 2010	Moscow, Russian Federation	**Meeting of the working group on criminal money flows** (in cooperation with MONEYVAL and the MOLI-Russia project) The meeting agreed on the contents of the typology study that is to be submitted for adoption by Moneyval in spring 2011.	4
11-16 Oct 10	Seattle/Vancouver (Microsoft)	**20th Annual World Congress of the Information Security Forum** Some 400 information security professionals from major corporations, primarily from Europe and northern America (eg ABN AMRO, Air France, Barclay's Bank, Boeing, BBC, British Airways, Credit Suisse, EADS, Fujitsu, Goldman Sachs, Hewlett Packard, IBM, Michelin, Microsoft, Orange, PricewaterhouseCoopers, Samlink, Société Générale, Volvo etc.) Keynote speakers included Henry Shaw (Assistant Director FBI) and Scott Charney (Microsoft). The meeting showed that: - cloud computing is very high on the agenda of all stakeholders is indeed an issue that the Council of Europe through the Project on Cybercrime, T-CY and T-PD should be dealing with from a cybersecurity and data protection/privacy perspective - data protection/privacy is very much of concern to US and European companies. Harmonisation of regulations within Europe is a particular concern of European companies - in Europe a more cooperative approach is pursued between industry and law enforcement with respect to information security than in the USA - the "end-to-end-trust" approach proposed by Scott Charney (he had presented to the DSG of the CoE already in Redmond in Feb 2009) could be indeed a means to enhance security through authentication while ensuring privacy. A number of representatives confirmed their interest in contributing to the work of the CoE with regard to security and privacy. The Information Security Forum could be used as a means to reach out to hundreds of major corporations. The meeting was furthermore useful in terms of reinforcing contacts with the FBI and Interpol.	All
13-15 Oct 10	Sibiu, Romania	**International Conference on Cybercrime** The Conference was organized by the Romanian National Police in	1,4

		cooperation with the US Department of State, Visa and Microsoft. Opening speeches were delivered by high officials from the National Romanian Police, the General Prosecutor of Romania and the Ambassador of the United States of America. Overall the event provided an overview of the status of cyber crime in Romania and the countermeasures taken. Specific topics related to cybercrime were discussed in the working groups. The Council of Europe presentation in the plenary session focused on the trends of cybercrime, the importance of the Budapest Convention and the CoE work in providing at global level assistance to countries for taking measures against cybercrime. The CoE intervention included also challenges in the collection of electronic evidence in view of further technological developments like P2P communications, cloud computing and possible answers as well as the importance of international co-operation against cybercrime.	

14 – 15 Oct 10	Buenos Aires, Argentina	**Training workshop on cybercrime and electronic evidence (Buenos Aires, Argentina, 14 October 2010)**
		
		Approximately 20 judges and prosecutors participated in the training workshop on cybercrime and electronic evidence. Speakers from US Department of Justice, Portugal and the Council of Europe.
		
		The discussions examined:
		
		- The challenges in the investigation of computer crimes:
		  - the representative of US DoJ presented examples of practical application and value of the Budapest Convention in international investigations;
		
		- The challenges for judges and prosecutors in investigating and adjudicating such cases:
		
		  - the CoE intervention promoted the implementation of the Concept paper on cybercrime training and electronic evidence for judges and prosecutors in order to equip them with the necessary skills to deal with such cases;
		  - the intervention of Portugal (involved in the developing of the concept) provided an example of how the training on cybercrime is organised in Portugal.
		
		The conclusion of the meeting was that although in Argentina there are some isolated initiatives to ensure cybercrime training for judges and prosecutors there is a need for a coherent strategy. There is also an interest to work more with the Council of Europe on this matter, including establishing a regional pilot centre in Argentina for training on cybercrime and electronic evidence in line with the CoE concept training.
		
		International conference "Combating Cybercrime: Argentina and Budapest Convention (Buenos Aires, Argentina, 15 October 2010)
			1, 2, 3

		Approximately 100 judges, prosecutors, police officers, representatives of private sector and other stakeholders participated in the conference "Combating Cybercrime: Argentina and Budapest Convention". Speakers from Argentina, Chile, US DoJ, Portugal and CoE.
		
		The discussions examined:
		
		- The CoE intervention highlighted the CoE global work on cybercrime, the need for a capacity building mechanism and recognised the efforts of Argentina at national and international level in fighting against cybercrime.
		
		- During the conference the panels tackled various topics:
		  - Industry view (Microsoft, Google, Eset)
		  - Criminalization of cybercrimes and electronic evidence (draft law to amend criminal procedural law of Argentina in line with the Budapest Convention)
		  - Accession and value of the Budapest Convention.
		
		In general the discussion reflected the strong interest of Argentina to align its national legislation with the principles of the Budapest Convention in view of becoming Party.
		
		Other areas that could be the object of further CoE work and assistance on cybercrime in Argentina and Latin America are training for judges and prosecutors, data protection and public/private cooperation.	

18-19 Oct 10	Santiago de Chile	**Bilateral meetings to promote accession by Chile to the Convention on Cybercrime** Meetings with the Chief of Prosecutors Office and other officials from the Public Ministry and a round table discussion with representatives of Ministry of Interior, Ministry of Foreign Affairs, Ministry of Justice, other public institutions and private sector (Microsoft). The CoE representative provided a summary of the CoE work to globally harmonise cybercrime legislation, the substantial assistance provided to different countries, cooperation with Chile and benefits for Chile to become Party to the Convention. Overall the meetings confirmed the interest of Chile to accede to the Convention but the process needs to be followed and complemented with the support in other areas.	1, 2
25-29 Oct 10	Kuala Lumpur, Malaysia	**Co-organisation of a cybercrime training workshop for judges and prosecutors at Judicial and Legal Training Institute (ILKAP) with approximately 30 judges and prosecutors from Malaysia and CoE trainers.** The course: - Provided 30 participants (judges and prosecutors) with basic understanding on how to prosecute and adjudicate cybercrime, handle electronic evidence as well as basic information regarding computer systems and how internet is functioning. The topics	5

		covered included: - - Cybercrime Phenomena - Current and specific Threats - Case study - Simple explanation of computer equipment and how the internet functions - Video clip - warriors of the net - Global Prosecutors E-crime Network (GPEN) presentation - Case preparation, presentation, digital evidence and case management - Internet Service Providers - Negotiating jurisdiction - Role of the expert witness and glossary of terms. - Underlined the importance of Malaysia becoming a party to the Budapest Convention in view of harmonising the substantive law and procedural law provisions on cybercrime as well as establishing a framework for international cooperation. - Showed that the CoE training materials need to be further improved to reflect practical cases and challenges in the application of the Convention. - Showed that ILKAP could indeed play the role of a regional (ASEAN) cybercrime training centre (pilot centre) for judges and prosecutors - Prepared the ground for an ASEAN-wide judicial training workshop in 2011.	
25-27 Oct 10	Kuala Lumpur, Malaysia	**Regional seminar on money laundering, trafficking and cybercrime organised by France and the Southeast Asia Regional Center for Counter Terrorism** Approximately 50 representatives from the Association of Southeast Asian Nations (ASEAN) countries as well as China. Speakers from France (including Jean-Louis Brugière), Belgium Financial Intelligence Unit (FIU), Europol/ Camden Asset Recovery Inter-Agency Network (CARIN) and Council of Europe It provided an opportunity to: - Promote the standards, monitoring and cooperation activities of the CoE related to money laundering, trafficking in human beings/sexual exploitation of children and cybercrime (including criminal money flows on the Internet) - Encourage accession to the Budapest Convention - Establish contacts for further work in the region, including China, on cybercrime.	4
28 Oct 10	Kuala Lumpur, Malaysia	**Meeting with The International Multilateral Partnership Against Cyber Threats (IMPACT) on cybercrime (Cyberjaya)** The meeting with the leadership of the IMPACT was held to discuss the implications of the results of the Tenth International Telecommunication Union Plenipotentiary meeting (ITU-PP 10) in Mexico that ended on 22 October and possible cooperation with IMPACT.	

2-4 Nov 10	Moscow, Russian Federation	Meeting of the working group on criminal money flows (in cooperation with MONEYVAL and the MOLI-Russia project)	4
7-8 Dec 10	Kiev, Ukraine	**Regional workshop: Protecting children against sexual exploitation and sexual abuse** The event was organised within the framework of the joint CoE/EU Project on Strengthening and Protecting Women's and Children's Rights in Ukraine (TRES) in cooperation with the CoE global Project on Cybercrime with the support of Microsoft. Officials responsible for law reform and investigators from Armenia, Azerbaijan, Belarus, Georgia, Moldova, Russian Federation and Ukraine participated in the event and shared their national experiences in fighting against online sexual abuse of children. Public and private sector organisations and initiatives engaged in this field, such as the European Union, OECD, Interpol, ICMEC, ECPAT, eNACSO, La Strada and Microsoft promoted good practices and contributed to the discussion on strategies and policies to promote a safer Internet for children A session on legislation discussed the criminalisation of sexual exploitation and sexual abuse in the participating countries and identified some legislative gaps that might prevent the law enforcement to prosecute this conduct. Each country presented short reports on further steps to be taken at the national level, most of them recommending that the ratification and implementation of this Convention to be a priority.	1
13-16 Dec 10	UAE (Abu Dhabi and Dubai), Bahrain and Qatar	**Workshops on cybercrime in the Gulf Region** Training meetings in Bahrain (Manama), Qatar (Doha) and the United Arab Emirates (Abu Dhabi were organised by Microsoft Europe, Middle East and Africa in cooperation with local authorities and the Council of Europe. The overall objective was to promote the implementation of Budapest Convention. The interventions focused on the Convention as a global framework, the need for developing national legislation on cybercrime and adequate training for judges and prosecutors on cybercrime matters. The Council of Europe's representative underlined the advantages for countries to accede to the Budapest Convention as a global legal framework on cybercrime, which allow international cooperation among Parties.	1
20 Dec 10	Lebanon	**Cyber Security Conference in Lebanon** The Conference was held within the frame of a Regional Pan-Arab Observatory for Safety and Security in Cyberspace. Representatives from Lebanon, Syria, Egypt, and different North African countries, including Tunis and Morocco participated in the event. The discussions focused on the establishment and operation of	1

		national CERTs, internet trust issues (e.g. e-commerce rules and electronic signatures) and cybercrime legislation. The Council of Europe presentation covered the Convention on Cybercrime underlying the need for harmonization. During discussions it was mentioned that the number of the Parties to the Cybercrime Convention represents more than 50% of the internet infrastructure, volume of communication and internet users and the number of supporting states in short term will considerably increase. In the substantive part of the Convention the main conduct is criminalized, but that in view of further harmonization it would recommendable to study legislative initiatives by the Parties concerning enactment of pre stage offences to the main conduct defined by the Cybercrime Convention, in particular concerning articles 7 and 8. With regard to the procedural part the enactment of new investigative powers should be undertaken at international level.	