COUNCIL OF EUROPE CONSEIL DE L'EUROPE

Global Project on Cybercrime (phase 2)

Update December 2009 – January 2010 / forecast February 2010

Date: 1 February 2010

PROJECT DATA

Project title	Global Project on Cybercrime, Phase 2 (DGHL/2009/2079)
Project area	A global project to support countries worldwide in the implementation of the Convention on Cybercrime (ETS 185) and its Protocol on Xenophobia and Racism (ETS 189)
Budget	Up to EURO 1.4 million (threshold EURO 500,000)
Funding	Council of Europe (Project 1429 – economic crime) Contributions from Romania, Microsoft 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 IN DECEMBER 2009 AND JANUARY 2010

Date	Place	Activity	Output
2 Dec 09	Moscow	Preparatory meeting with ROSFINMONITORING (the Financial Intelligence Unit of the Russian Federation) on the typology study on "criminal money flows on the internet".	4
8-10 Dec 09	Cairo, Egypt	1. Training workshop for judges on cybercrime and child abuse. The event was considered a success and had very positive reviews from both MOJ and MCIT. According to the Training Requirements and Evaluation Unit of the National Center for Judicial Studies Report, most of the participants considered that the training program was excellent, must be circulating among all judges and public prosecutors and the trainers succeeded in dealing with all subject matters and deliver the information in a pragmatic way. 2. During the Round table discussion on a concept for the training of judges in cybercrime/electronic evidence, including online child abuse, the CoE presented cybercrime training concept developed under the Global Project on cybercrime and the Centre provided an assessment of the training workshop delivered. It was concluded that the cooperation on training for judges in cybercrime between the CoE and the Centre should be enhanced. Follow-up: - The training concept for judges and prosecutors to be implemented in Egypt; - Consider the possibility that the centre, which provides judicial training for Arab countries, Africa and other regions, to become a pilot centre on cybercrime training in the region; - CoE will provide curricula and the Training Manual on cybercrime when they become available; - the Centre to attend the Cybercrime Octopus Conference (23-25 March 2010). The event was an example of cooperation between the Egyptian Government, local and international bodies, private and public sector (National Centre of Judicial Studies, Ministry of Communication and IT, International Peace Movement, ICMEC, INHOPE, Microsoft and the Council of Europe)	5, 7
11-13 Dec 09	Courmayeur Mont Blanc, Italy	ISPAC International Conference on Protecting Children from Sexual Offenders in the Information Technology Era. During the event, 4 workshops were held simultaneously: - technical solutions available to law enforcement and criminal justice - status of scientific research and training of law enforcement staff - collaboration between law enforcement/justice authorities and the private sector/industry (Microsoft had a presentation) - victim protection In the session *Action by international and regional institutions* the CoE representative underlined that the Convention on Cybercrime	7

		and the Convention on the Protection of Children against Sexual Exploitation and Sexual Abuse are global instruments, which provide the core elements of criminal legislation aimed at protecting children online. Both Conventions are valuable and recognised standards for online protection of children against sexual exploitation and sexual abuse. Countries and organizations should take advantage of these instruments and implement their provisions rather than launching initiatives for developing new treaties, which will only duplicate the existing work and fail in being adequately implemented.	
12 Jan 10	Ankara	Ankara Bar Association International Law Congress 2010 - Cyber Crimes Convention Workshop About 40 participants (judges, prosecution officers, representatives of the ICT-board, government representatives) took part in the meeting with the aim to explore the possibility of signing and ratifying the Cybercrime Convention (Turkey is among the 5 CoE Member States that have not yet signed the Convention) and were willing to take legislative and other actions, including launching initiatives in the private sector, as well as training for the judiciary. Statistics in 2009 showed that Turkey holds the third position on the list of countries from where malware is launched, after Serbia and Brazil. CoE presentation highlighted that there is a growth of internet users – also in Turkey – which will inevitably cause a strong growth of the number of victims and perpetrators of cybercrime. The international nature of cybercrime requires international solutions and international co-operation. CoE could offer guidance and assistance for Turkey when implementing the Cybercrime Convention and its Protocol. Microsoft made a presentation on internet security, the role of industry in its co-operation with governments and the 2Center Project.	1
18 Jan 10	Strasbourg	Typology study on criminal money flows on the Internet Following consultations with key stakeholders (including inputs from McAfee and Microsoft), the questionnaire on the typology study was agreed upon and widely circulated. A meeting of the project group will take place on 26 March 2010 in Strasbourg following the Octopus conference.	4
21-22 Jan 10	Ifrane, Morocco	Building Cyber security and Cyber confidence: Strategies, Awareness and Capacity Building This regional cybersecurity conference was organised by the Ministry of Industry, Trade and New Technologies and Al Akhawayn University with some 150 participants, primarily from Morocco but also from Tunisia, Egypt and Malaysia as well as a number of European experts.	1,2

		The Council of Europe/Project on Cybercrime presented the conditions for criminal justice action against cybercrime in the plenary session on cyberthreats: - Legislation - Training and specialisation - Public-private cooperation - International cooperation - Safeguards The subsequent workshop on legal and policy capacity building clearly showed that most of the tools needed are already available (e.g. Budapest Convention, LEA-ISP guidelines, 2Centre concept, judicial training concepts) but that a global capacity building effort was required to support countries in Africa and the near and middle east in their implementation.	
21-22 Jan 10	Washington D.C	Sixth Meeting of the REMJA Working Group on Cyber-Crime In the introductory remarks the Secretary General of the OAS, José Miguel Insulza highlighted the need for countries to bring their legislation in line with the Budapest Convention in order to enhance cooperation among states, and recognised the effort made recently by Colombia, which adopted new legislation on cybercrime. The meeting adopted a set of recommendations and provided the status of OAS Member States with regard to the implementation and accession to the Convention on Cybercrime. Recommendation 11 adopted states: *"Recognize the consideration that certain OAS Member states have given to applying the principles of the Council of Europe's Convention on Cybercrime, acceding thereto, and adopting the legal and other measures required for its implementation, and recommend to those states that have not yet done so, to give due consideration thereto, bearing in mind the recommendations adopted by this Working Group and by the REMJAs at previous meetings. Similarly, to this end, that technical cooperation activities be continued under the auspices of the OAS General Secretariat and the Council of Europe".*	1,2
26-28 Jan 10	Manila, Philippines	ASEAN/APRIS Workshop on Cybercrime Legislation in ASEAN Member States, Manila, Philippines This event was organised in cooperation with the ASEAN Secretariat, the ASEAN-EU Programme for Regional Integration Support (APRIS), the Commission for Information and Communication Technology of the Philippines and the Council of Europe with some 50 cybercrime and information security experts from Cambodia, Indonesia, Laos, Malaysia, Philippines, Singapore, Thailand and Vietnam. The workshop resulted in an analysis of legislation and progress made since the first workshop in Kuala Lumpur in November 2008: - In Cambodia a draft e-commerce law is available that incorporates key provisions of the Convention on Cybercrime. Follow up workshop in Cambodia is recommended.	1, 3, 5

		- In Indonesia, following the adoption of legislation in 2008, an additional bill is before parliament. A workshop with parliamentarians is recommended to improve the bill. Indonesia could now seek accession to the Budapest Convention on Cybercrime. - In Laos, a workshop is recommended to launch work on legislation. - In Malaysia, a review of national cybercrime and –security legislation has been completed and recommendations have been made for further improvement. Malaysia could now seek accession to the Budapest Convention. - In the Philippines it was not possible to have the legislation adopted before the May 2010 elections. There are good chances that the legislative work could nevertheless be completed in 2010, including the accession process. - In Singapore, it may be necessary to review the effectiveness of existing legislative provisions. - In Thailand, cybercrime legislation was adopted in 2007 that is largely compatible with the Budapest Convention. Thailand could now seek accession. - In Vietnam, some amendments to the Criminal Code were adopted in July 2009. Further work is underway as the Criminal Code and the Criminal Procedures Codes are undergoing major reform in 2010 and 2011. Overall, good progress was made since November 2008. Substantive law is well covered (although apart from the Philippines countries rely on general pornography provisions rather than specific articles for children), while procedural laws are less complete (most countries rely on data retention rather than preservation; specific elements on search and seizure are missing, including limitations, safeguards and conditions). A more detailed discussion would be necessary to review the functioning of provisions in practice. In addition to the Philippines, Indonesia, Malaysia and Thailand could be invited to accede, while in parallel further support should be provided to improve legislation. With regard to law enforcement/Internet service provider cooperation all countries pledged to initiate work on the matter based on the CoE guidelines adopted in 2008. Indonesia will establish a working group, while Malaysia will hold meetings to streamline cooperation which is already well functioning. With regard to the training of judges and prosecutors, none of the countries – with the exception of Cambodia – foresee specific initial training for judges but provide for in-service training. It would seem that Malaysia is the only country with a specific centre for continued training for judges and prosecutors. The workshop recommended that the Malaysian centre could become a pilot centre along the lines suggested by the CoE training concept (the CoE was asked to present the concept to this centre possibly in June/July 2010).	

		Countries were also interested in the 2Centre initiative for law enforcement training and it was recommended that at least one such centre should be established in the ASEAN region. On the suggestion of the Philippines, the workshop recommended that the issue of training (1. For judges and prosecutors using the CoE concept, 2. For law enforcement using the 2Centre approach and 3. On international cooperation for Prosecutors General Offices and Ministries of Justice on the basis the Budapest Convention) be taken up at a formal level by ASEAN. After the closure of the workshop a "concept" was prepared for submission to the ASEAN TELSOM/TELMIN joint group in Brunei in February 2010 and subsequent consideration by TELSOM Ministers. Ministerial support is considered necessary to ensure implementation. Follow up: - Workshop with CoE support in Laos to provide advice on draft legislation (June/July 2010); - Workshop with CoE support in Cambodia to guide the commission responsible for drafting legislation once established (June/July 2010); - Presentation by CoE to parliamentary commission of Indonesia responsible for the cybercrime bill; - Maintain dialogue to encourage requests for accession by Indonesia, Malaysia and Thailand; - Presentation by CoE of judicial training concept to Malaysian training centre (July 2010); - ASEAN TELSOM to discuss recommendation on cybercrime training (February to June 2010); - CoE to facilitate creation of a cybercrime centre of excellence for law enforcement training; - Mobilisation of technical assistance to countries of ASEAN.	
25–26 Jan 10	Ebene, Mauritius	The African Network Information Center (AfriNIC), the Regional Internet Registry (RIR) for Africa: First AfriNIC - Government Working Group (AfGWG) & Law Enforcement Meeting. The objectives of the meeting were to provide for the participants the opportunity to learn about the current challenges of Internet-related crimes, the steps being taken by law enforcement agencies to face such challenges and exchange ideas about the formation of a Internet Law Enforcement Working Group, which will promote security by facilitating global cooperation and coordination. Discussions included the need for the establishment of Law Enforcement Agencies and Regional Internet Registries joint working groups, to enhance Law Enforcement capabilities in fighting against crime. Some African countries mentioned that they have difficulties to join the Convention on Cybercrime because they are not yet ready to totally accept its provisions and the internal consequences of the ratification. The CoE representative highlighted that the Convention on Cybercrime is not a European instrument, but a globally binding instrument. The Convention provides for countries a global legal framework to deal with cybercrime and a model to develop domestic legislation. African countries could request the CoE for technical cooperation when drafting their legislation.	1

ACTIVITIES PLANNED FOR FEBRUARY 2010

Date	Place	Activity	Output
2-3 Feb. 10	Nigeria	1st West African Internet Fraud Summit	1
10 Feb 10	Buenos Aires	Meeting on Convention on Cybercrime	1
16-18 Feb 10	Malta	MENA Cybercrime Legislation Workshop	1
17-18 Feb 10	Brussels	EastWest Institute - the 7th Worldwide Security Conference	4
23-24 Feb 10	Pakistan	Cybercrime training for law enforcement and judges	5