Project on Cybercrime
www.coe.int/cybercrime

COUNCIL OF EUROPE CONSEIL DE L'EUROPE

Global Project on Cybercrime (phase 2)

Update February 2010 – April 2010 / forecast May 2010

Date: 5 May 2010

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 FEBRUARY - 30 APRIL 2010

Date	Place	Activity	Output
2-3 Feb 10	Abuja, Nigeria	**Pre-Summit Workshop, West African CyberCrime** It was discussed the organisation of the 1st West African Cybercrime Summit, which will take place on 7-10 September 2010 in Abuja, Nigeria. The event is hosted by EFCC in partnership with UNODC and Industry. Participants: Council of Europe, ECOWAS, EFCC, European Union Delegation Nigeria, Europol, French Gendarmerie, Google, INTERPOL, Microsoft, UK SOCA, UNODC, US Department of Justice. It was agreed: ▪ The 1st West African Cybercrime Summit will focus on: raising political awareness and commitment to combat cybercrime, legislative framework, training, capacity building/sustainability and international cooperation. ▪ The event will bring together an international group of political leaders and decisions makers, criminal justice authorities, industry representatives and other relevant stakeholders. ▪ Summit Planning Committee: EFCC (West African LE), Microsoft (Industry), UNODC (Intl Development), ECOWAS (Region), IMMWG (US/UK LE) On this occasion the song “Maga No Need Pay” was lunched in Nigeria within an awareness campaign launched by EFCC, Microsoft and UNODC. The Council of Europe has invited the EFCC and Microsoft to present the song at the opening session of the Council of Europe global Octopus Conference on cooperation against cybercrime, which will showcase the song as a global best practice for education and awareness against cybercrime.	1
10 Feb 10	Buenos Aires, Argentina	**Meeting on Argentina’s accession to the Budapest Convention on Cybercrime** Further to the last CoE visit in Buenos Aires in November 2009 and the letter sent to the government to consider accession, the authorities organised a meeting with the key people involved in the process of assessing the compliance of the cybercrime legislation of Argentina with the Convention on Cybercrime. Three experts on substantive law, procedural law and international cooperation on cybercrime presented the report analyzing to what extend the domestic legislation of Argentina covers the provisions of the Convention. The presentations concluded: - substantive law provisions are generally covered by the legislation adopted recently in Argentina and by making use of some reservations allowed by the treaty; - existent procedural law provisions should be amended - international cooperation provisions under Convention would also require the implementation of the procedural law measures both at the national and international level. - although more legislative and institutional measures are required to better deal with cybercrime and fully comply with the Convention	1

		there is no major impediment to request accession and in parallel to continue the legislative reform. Most of the speakers expressed a clear support for Argentina to become Party to the Convention and cooperate with the Council of Europe. The results of the meeting were encouraging. Moreover, a strong interest was expressed by the participants to attend the Octopus Conference on Cybercrime (Strasbourg on 23—25 March 2010) as most of the issues raised (e.g. legislation on cybercrime, training, jurisdiction and cloud computing etc) will be discussed during the Conference.	
16-18 Feb 10	Malta	**Cybercrime Workshop for North Africa and the Middle East** The regional workshop was organized by US with the participation – thorough the Project - of the Council of Europe. Law enforcement representatives, prosecutors, judges and representatives responsible for national criminal policy participated in the event. The purpose of the meeting was to raise awareness on the importance of the cybercrime legislation and prepare legislative profiles using the text of the Cybercrime Convention as a basis and guidance. The CoE representative highlighted the urgency of adopting cybercrime legislation, arguments for Arab countries to join the Budapest Convention on Cybercrime and also the need for financial support for developing countries in order to be able to deal with cybercrime. Tunisia and Morocco stated their support to the Cybercrime Convention, which is considered a very useful instrument. Malta's Parliament is discussing an Amendment Bill that would allow Malta to ratify the Convention. Ratification can be expected within a couple of month. The meeting was highly appreciated and served as a platform for exchanging experiences and views among participants and increased the interest in the Cybercrime Convention and relating Council of Europe work.	1
17-18 Feb 10	Brussels	**EastWest Institute - the 7th Worldwide Security Conference** This conference covered a wide range of security issues, including a special consultation on "international pathways to cybersecurity". In this context, the CoE through the Project on Cybercrime, participated in a workshop on legal cooperation. The EastWest Institute intends to focus stronger on the question of cybersecurity through its "Worldwide Cybersecurity Initiative". However, it would be useful that this initiative be more closely linked to existing mechanisms and initiatives underway, build on progress made already, and put a stronger focus on criminal justice issues.	4
23-24 Feb 10	Islamabad, Pakistan	**Cybercrime training for law enforcement and judges** The Federal Investigation Agency (FIA), Microsoft and the Council of Europe jointly organised two cybercrime training sessions for law enforcement officers in Islamabad on 23 and 24 February 2010. Furthermore, round table discussions were held on institutionalising cybercrime training with FIA as well as judicial training with the Federal	5

		Judicial Academy. In addition, an exchange of views took place with the Pakistan Information Security Association (PISA). These events will feed into ongoing legislative reforms and help bring the legislation of Pakistan further in line with the Budapest Convention on Cybercrime. Recommended follow up includes: - Delivery of a two-weeks basic law enforcement training course in view of preparing for the creation of a cybercrime centre of excellence - Assisting the Federal Judicial Academy in the preparation of a basic training course for judges - Support to cybercrime legislation (transforming the Prevention of Electronic Crimes Ordinance into a proper law taking into account the Budapest Convention)	
16-17 Mar 10	Barcelona, Spain	**SecureCloud 2010 – ENISA/Cloud Security Alliance joint Conference on Cloud Computing** The CoE, through the Project on Cybercrime, contributed to this event which involved several hundred participants. The CoE presentation focused on law enforcement and data protection issues. The meeting helped prepare for the Octopus conference and helped secure the participation of ENISA and the Cloud Security Alliance in Octopus.	1, 6
23-25 March 10	Strasbourg	**Octopus Interface conference: Cooperation against cybercrime** More than 300 cybercrime experts representing countries from all continents, international organisations and the private sector met in Strasbourg to enhance their cooperation against cybercrime. At the close of the conference participants adopted key messages aimed a guiding further action underlining that: - For security and the protection of rights to reinforce each other, measures against cybercrime must follow principles of human rights and the rule of law. - Security and the protection of rights is the responsibility of both public authorities and private sector organisations. - Broadest possible implementation of existing tools and instruments will have the most effective impact on cybercrime in the most efficient manner. Following detailed discussions, participants recommend: - Making decision makers aware of the risks of cybercrime and encouraging them to exercise their responsibility. Indicators of political commitment include steps towards the adoption of legislation and institution building, effective international cooperation and allocation of the necessary resources. - Implementation of the Budapest Convention on Cybercrime worldwide to sustain legislative reforms already underway in a large number of countries. Countries should consider becoming	All

		parties to make use of the international cooperation provisions of this treaty. Consensus on this treaty as a common framework of reference helps mobilise resources and create partnerships among public and private sector organisations. In this connection, the ratification of the Budapest Convention by Azerbaijan, Montenegro and Portugal prior and during the conference, and the expression of interest to accede by Argentina and other countries serve as examples to other countries. - Establishing the Budapest Convention as the global standard goes hand in hand with strengthening the Cybercrime Convention Committee (T-CY) as a forum for information-sharing network, policy-making and standard-setting. It is encouraged to address issues not (exhaustively) regulated by the provisions of the Cybercrime Convention such as electronic evidence, jurisdiction and liability of ISP's. - Coherent and systematic training of law enforcement, prosecutors and judges based on good practices, concepts and materials already available. - The establishment and strengthening of high-tech crime and cybercrime units, and incidents response and reporting teams and systems. - The development of cooperation procedures between law enforcement agencies, CERTs/CSIRTs as well as internet service providers and the IT industry. - Due diligence measures by ICANN, registrars and registries and accurate WHOIS information. Endorsement of the "Law Enforcement Recommended Amendments to ICANN's Registrar Accreditation Agreement (RAA) and Due Diligence Recommendations" in line with data protection standards. ICANN is encouraged to implement these recommendations without delay. - The many networks and initiatives against cybercrime that exist already create a dynamic and innovative environment involving a wide range of actors. Stronger networking among networks is encouraged to allow for synergies and reduce duplication. The mapping of networks exercise initiated by the Council of Europe should be continued. - A contact list for enhanced cooperation between industry and law enforcement should be established. A proposal for a secure portal for interested parties is in preparation. - Initiatives aimed at preventing, protecting and prosecuting the sexual exploitation and abuse of children are most valuable but require stronger support and consistency. The "Lanzarote" Convention of the Council of Europe (CETS 201) offers guidance in this respect and provides benchmarks to determine progress. - Making use of the guidelines for law enforcement – ISP cooperation adopted at the Octopus Conference in 2008. - Completion and broad dissemination of the results by the Council of Europe of the typology study on criminal money flows on the Internet that is currently underway. - In order to meet the law enforcement and privacy challenges related to cloud computing existing instruments on international	

		cooperation – such as the Data Protection Convention (CETS 108) and the Budapest Convention – need to be applied more widely and efficiently. Additional international standards on effective mechanism for cooperation in the law enforcement especially with regard to the access to data stored in the “clouds” may need to be considered. Globally trusted privacy and data protection standards and a common activities on enforcement and policies addressing those issues need to be put in place and the Council of Europe is encouraged to continue addressing these issues in its standard-setting activities as well as by the Global Project on Cybercrime. Public authorities, international organisations, civil society (including non-governmental organisations) and the private sector should apply existing tools and instruments without delay and cooperate with each other to identify additional measures and responses to emerging threats and challenges. In order to add impetus and resources to efforts against cybercrime and allow societies worldwide to make best possible use of tools, instruments, good practices and initiatives already available, a global Action Plan aimed at obtaining a clear picture of criminal justice capacities and pressing needs, mobilising resources and providing support, and assessing progress made should be launched, preferably by the United Nations and the Council of Europe in partnership with the European Union, Parties to the Budapest Convention, and other interested parties. The results of the Octopus conference to be submitted to the United Nations Crime Congress in Salvador, Brazil (12-19 April 2010) for consideration.	
26 Mar 10	Strasbourg	**Working meeting on the typology study on criminal money on the Internet** The meeting discussed and reached agreement on the outline of the report. It is expected that a full draft will be finalised by early September when the group will hold its next meeting in Moscow.	4
31 March – 1 April10	Lille	**French National Gendarmerie: 4th International Forum on Cybercrime** http://www.fic2010.fr/fr/php/accueil.php4 This event organised for the 4th time by the Gendarmerie of France provided a platform for many hundred participants from different countries but primarily from France to exchange ideas. It took place shortly after the Octopus conference and allowed to follow upon some of the key messages, as reflected in the presentation of the Minister of Interior of France. The CoE, through the Project on Cybercrime presented the results of the Octopus conference and the need for a global capacity building effort based on existing instruments in the plenary session on “La	1

		mobilisation européenne et internationale pour la lutte contre la cybercriminalité” and in a workshop organised by the OSCE on "Une approche globale de la cyber-sécurité”.	
12-19 Apr 10	Salvador, Brazil	**The 12th United Nations Congress on Crime Prevention and Criminal Justice** The UN Crime Congress held intensive discussions on cybercrime in Committee II (agenda item 8. recent developments in the use of science and technology by offenders and by competent authorities in fighting crime, including the case of cybercrime) and in the negotiation of the political “Salvador Declaration”. In Committee II some speakers argued for the preparation of a new treaty on the grounds that this would enhance ownership also of developing countries, while others underlined the need for operational action on the basis of existing instruments and in particular the Budapest Convention on Cybercrime. There was, however, general agreement on the need for technical assistance to build criminal justice capacities to cope with cybercrime. Specific reference was made by some speakers to the outcome of the Octopus conference. The discussions in Committee II are reflected in the draft report A/CONF.213/L.4/Add.1. This document, in Paragraph 17, proposes the preparation of an Action Plan for capacity building. The compromise reached regarding cybercrime in the political Salvador Declaration is reflected in paragraphs 41 and 42: 41. We recommend that the United Nations Office on Drugs and Crime, upon request, provide, in cooperation with Member States, relevant international organizations and the private sector, technical assistance and training to States to improve national legislation and build the capacity of national authorities, in order to deal with cybercrime, including the prevention, detection, investigation and prosecution of such crime in all its forms, and to enhance the security of computer networks. 42. We invite the Commission on Crime Prevention and Criminal Justice to consider convening an open-ended intergovernmental expert group to conduct a comprehensive study of the problem of cybercrime and responses to it by Member States, the international community and the private sector, including the exchange of information on national legislation, best practices, technical assistance and international cooperation, with a view to examining options to strengthen existing and to propose new national and international legal or other responses to cybercrime. In short: broad agreement on technical assistance and capacity building as well as public-private cooperation, but no agreement on the preparation of a new treaty. The Octopus Conference (23-25 March 2010), and the Secretariat of the Council of Europe (submission of the Secretary General to the UN Crime Congress, statement of Director General Philippe Boillat at	All

		the Congress) had argued that a global capacity building effort based on existing instruments was the most effective way ahead. The UN Crime Congress confirmed this as the most feasible option. Discussions will continue at the UN Crime Commission in Vienna from 17 to 21 May and certainly in the years ahead. In the meantime, countries and organisations need to prepare to respond as soon as possible to the call for capacity building. Resources will need to be mobilised in particular by European Union and other developed countries that took position in favour of implementing existing instruments. The Council of Europe will continue to offer assistance through the Project on Cybercrime and other projects in partnership with public and private sector partners.	
29-30 Apr 10	Madrid	**EuroDIG 2010 – workshop on cross-border cybercrime jurisdiction and cloud computing** This workshop allowed to continue the discussion of the Octopus conference and to identify the questions that need to be addressed with regard to cross-border law enforcement access to data on cloud servers, the role of Internet service providers and the question of data protection. It re-affirmed the need for international guidance through best practice guidelines, or a soft-law instrument (recommendation) or a binding hard-law instrument (for example a protocol to the Budapest Convention on Cybercrime). The need for globally trusted data protection systems (based for example on the data protection convention 108 of the Council of Europe) was underlined once again.	1, 6

ACTIVITIES PLANNED FOR MAY 2010

Date	**Place**	**Activity**	**Output**
6 May 10	Brussels	Brainstorming session on the EU Internal Security Strategy	1
12-13 May 10	Burbank, California, USA	POLCYB International Conference 2010	1, 4
17-21 May 10	Vienna, Austria	United Nations Commission for Crime Prevention and Criminal Justice	all

Note: A number of requests for support to training and legislative advice in Africa, Asia and Latin America (June to August 2010) are on hold pending the availability of funding.