

Global Project on Cybercrime (phase 2)

Update November / forecast December 2009

Date: 7 December 2009

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 NOVEMBER 2009

Date	Place	Activity	Out-put
1-3 Nov 09	Vancouver	<p>Information Security Forum 20th Anniversary Annual World Congress</p> <p>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.) participated in the event.</p> <p>The meeting showed that:</p> <ul style="list-style-type: none"> cloud computing is very high on the agenda of all stakeholders and an issue that the Council of Europe 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 could be indeed a means to enhance security through authentication while ensuring privacy. <p>A number of representatives confirmed their interest in contributing to the work of the CoE with regard to security and privacy.</p>	1, 2
5-6 Nov 09	Brussels	<p>European Commission - Annual cybercrime conference: EU-US cooperation</p> <p>Representatives of EU member States, the US Department of Justice, Secret Service and the FBI, Europol as well as InHOPE, the European Financial Coalition and the Council of Europe participated in the event.</p> <p>CoE had a presentation on the policy context of cybercrime and moderating the session on jurisdiction.</p> <p>The meeting agreed:</p> <ul style="list-style-type: none"> US and the EU strongly support the Convention on Cybercrime (reflected in the draft Stockholm Programme and the US Cyber Policy Review). A contact list/facebook-style secure cooperation platform for law enforcement, ISPs and hotlines should be established with funding from the EC. The European and US financial coalitions against child abuse are prepared to contribute to the typology study on criminal money on the internet. The question of the role of law enforcement in internet governance should be strengthened. Key issues to be addressed in this context are due diligence and accountability of registrars, and the privatisation of WHOIS (which would make law enforcement work much more difficult). Interlocutors for discussions are ICANN (Governmental Advisory Committee) and regional registrars (e.g. RIPE for Europe, Middle East and Russia). A position could be developed for the ICANN meeting in 	2

		<p>June 2010 in Amsterdam.</p> <ul style="list-style-type: none"> France is interested in undertaking with the CoE and Microsoft a study on cloud computing to define the issues involved Initiate a project report on cloud computing (in cooperation with the MoI of France and Microsoft) to define the issue (in view of a meeting planned at the National Assembly of France in early 2010 and in view of the Octopus Conference in March) 	
15-18 Nov 09	Sharm el Sheikh, Egypt	<p>The fourth annual IGF Meeting gathers over 1800 participants from 112 countries.</p> <p>Discussions examined:</p> <ul style="list-style-type: none"> ways to improve Internet access by all and promote local content and cultural diversity; ensure the safety of the Internet and fight cybercrime; manage key Internet resources such as the root server system, technical standards, interconnection and telecommunications, the domain name system and Internet protocol addresses. <p>The meeting also discussed new issues related to the continued growth of social networks, and the ensuing governance issues that are emerging, in particular, the need for new approaches regarding privacy and data protection, rules applicable to user-generated content and copyrighted material, and issues of freedom of expression and illegal content.</p> <p>Parallel to the main sessions on these issues, more than 100 workshops, best practice forums, dynamic coalition meetings and open forums were held around the broad themes of the main sessions and the overall mandate of the IGF.</p> <p>Events and results related to cybercrime include:</p> <p>Workshop 93: The Global Path for Ensuring Online Child Protection and Safety: effective strategies and specific actions (Sunday, 15 Nov 09)</p> <p>The workshop focused on effective strategies and specific actions in developing and promoting a safe and productive experience for children and youth online, and protecting children and youth from exploitation and abuse. It was aimed at promoting multi-stakeholder cooperation by identifying common elements (strategies/specific actions/good practices), contributions by and synergies between different stakeholders, and mechanisms for interaction and cooperation.</p> <ul style="list-style-type: none"> Speakers and participants underlined the need for a clear legal basis to investigate crimes related to the sexual exploitation of children and to hold offenders accountable. Approaches need to make sure that fundamental rights are protected (including privacy, the freedom of expression, self-determination) and the security of children is ensured at the same time. The workshop concluded that in order to put a comprehensive legislative framework in place that is internationally harmonized and permits efficient international cooperation, countries should make use of the Convention on the Protection of Children against Sexual Exploitation and Sexual Abuse (CETS 201) and the Convention on Cybercrime (CETS 185). 	All

		<p>Best Practice Forum 87: 2CENTRE, the Cybercrime Centres of Excellence for Training, Research & Education (Monday, 16 Nov 09)</p> <p>2CENTRE is a European project which aims at uniting law enforcement, industry and academic expertise to provide an internationally coordinated cybercrime investigation training program for law enforcement agencies and the industry in the European Union and beyond.</p> <ul style="list-style-type: none"> • Among the four memoranda of understanding signed on 18 November by the Egyptian Government in a special session in the presence of the First Lady of Egypt, Mrs. Mubarak, was also a MoU with Microsoft aiming to establish a 2Centre of excellence for training and supporting innovation in internet safety for the youth online. • Speakers included University College Dublin, Microsoft, the CoE and Ministry of Interior of Egypt. The CoE expressed the support for 2Centre initiative and 60 participants from Africa, Middle-East and Asia provided excellent feedback regarding this initiative. <p>Main session workshop on Security, Openness and Privacy (Monday, 16 Nov 09)</p> <p>The CoE participated with one panelist who focused on security and fundamental rights: how to ensure security while maintaining due process, freedom of expression and privacy in a global environment? Following the workshop, the Minister of Communication and Information Technologies of Egypt pledged to initiate work on cybercrime and data protection legislation and to consult with the CoE in these matters.</p> <p>Workshop 179: Cybercrime training for judges and law enforcement (Tuesday, 17 November 09)</p> <p>The event allowed the CoE to present the "concept on cybercrime training for judges and prosecutors" that had recently been developed by the Project on Cybercrime and the Lisbon Network, and the workshop and round table that will be organized in Egypt in December with the support of the Project on Cybercrime.</p> <ul style="list-style-type: none"> • It was agreed that the training concept should also be promoted in India through a workshop in 2010 • During the workshop as well as in a subsequent discussion with UNODC it was agreed that the CoE and UNODC should cooperate in cybercrime training. With regard to the forthcoming UN Crime Congress in Brazil, the UNODC representative pledged to have the CoE participate in an ancillary meeting on cybercrime and possibly also in a plenary session (UNICRI also seems interested to have the CoE intervene in a workshop on cybercrime and organized crime). <p>Best Practice Forum 68: Developing cybercrime legislation (Tuesday, 17 November 09)</p> <p>The event underlined that comprehensive and consistent legislation is essential to help societies meet the challenge of cybercrime and thus to enhance the security of and confidence in information and communication technologies. Legal frameworks should take into account the rights of users and the role of the private sector on the one hand, and security concerns on the other. The Convention on Cybercrime of</p>	
--	--	---	--

		<p>the Council of Europe provides a global guideline in this respect.</p> <p>The workshop:</p> <ul style="list-style-type: none"> • Promoted globally harmonised legislation based on international standards, in particular the Council of Europe Convention on Cybercrime • Highlighted the substantial assistance provided by the Council of Europe within the Project on cybercrime to different countries to harmonise their criminal law provisions on cybercrime with those of other countries in order to facilitate international cooperation • The participants' questions underlined the complexity of the legislation on cybercrime and the need for assistance and international joint efforts. <p>Workshop 257: The security and privacy implications of cloud computing (Tuesday, 17 November 09)</p> <p>The CoE was a co-organiser of this workshop together with EPIC and the French Ministry of Foreign Affairs.</p> <p>The CoE intervention focused on how to ensure security and privacy in the clouds?</p> <ul style="list-style-type: none"> • Existing instruments make sense -> e.g. full implementation of Convention on Cybercrime ("Exploiting existing opportunities by all") • Enhance the efficiency of application of international cooperation provisions of the Convention on Cybercrime and others • Develop additional international standards on law enforcement access to data stored abroad / in the clouds • Insist on procedural safeguards/due process / clear procedures for cooperation between cloud providers and law enforcement -> provide guidance to service/cloud providers • Establish globally trusted privacy / data protection standards and systems • Cloud provider that cannot guarantee data protection/privacy standards and procedural safeguards will have a competitive disadvantage <p>Workshop 288: Child Online Safety Indicators: Measuring the Un-measurable? (Wednesday, 18 November 09)</p> <p>This event was organised by the Cyber Peace Initiative of Egypt and the ITU.</p> <ul style="list-style-type: none"> • The workshop showed how the Convention on the Protection of Children against Sexual Exploitation and Sexual Abuse (CETS 201) provides benchmarks to measure progress made in the implementation of actions to protect children • The Council of Europe – through the Project on cybercrime – to continue supporting widely the strengthening of comprehensive legislation on cybercrime, data protection and protection of children against sexual exploitation and sexual abuse and to promote relevant instruments globally <p>The IGF prepared the ground for closer cooperation between Egypt and the CoE. Specific opportunities include:</p> <ul style="list-style-type: none"> - Support to the preparation of legislation on cybercrime, data protection and child exploitation in view possible future accession to Conventions 108,185 and 201 - Support to the training of judges, prosecutors and law 	
--	--	--	--

		<p>enforcement in cybercrime and electronic evidence in line with the training concept developed under the Project on Cybercrime</p> <ul style="list-style-type: none"> - Cooperate with the Cyber Peace Initiative supported by Mrs. Suzanne Mubarak, the First Lady of Egypt, President and Founder of the Suzanne Mubarak Women's International Peace Movement. <p>The question of the role of ICANN and registries to ensure due diligence and prevent the criminal abuse of domains should be discussed at the next Octopus conference.</p>	
18-19 Nov 09	Hanoi	<p>Séminaire francophone Droit des technologies de l'Information</p> <p>The visit was a cost-effective opportunity to continue the dialogue with Vietnam, to assess the current state of legislative reforms and to demonstrate the availability of the CoE to provide further assistance in view of ensuring the improvement of cybercrime legislation. With regard to data protection, the meeting primarily raised awareness to put legislation and other measures in place.</p> <p>The Project should continue to support Vietnam in the reform of its legislation in the course of 2010. Cambodia and Laos currently have no provisions in place regarding cybercrime and should be supported as soon as legislative working groups have been established.</p> <p>The training concept for judges and prosecutors should be shared with the Maison Du Droit in view of supporting its implementation in Vietnam. The ASEAN-EU-CoE workshop planned for January 2010 will provide another opportunity.</p>	6
Nov 09	Strasbourg	<p>The Consultative Council of European Prosecutors welcomed the concept for the training of judges and prosecutors on cybercrime and electronic evidence (adopted by the Lisbon Network of judicial training institutions) and invited the relevant authorities in the member states to make the best use of it.</p>	5
27 Nov 09	Brussels	<p>European Commission: Conference on Public-Private Sector dialogue on tackling online illegal activities</p> <p>COE and other speakers' interventions made reference to the CoE Guidelines for cooperation between law enforcement and internet service providers as a basis for the Council recommendations and European Union's future work.</p> <p>During the meeting public/private initiatives against cybercrime from Germany and Netherlands were presented and the EC announced that it will host a public/private contact list for industry and law enforcement.</p> <p>EuroISPA and Europol presented their work recognizing the significant contribution of Microsoft.</p>	3

ACTIVITIES PLANNED FOR DECEMBER 2009

Date	Place	Activity	Output
2 Dec 09	Moscow	Preparatory meeting with ROSFINMONITORING on the typology study on "criminal money flows on the internet"	4
7-8 Dec 09	Egypt	Training workshop for judges on cybercrime and child abuse and Round table discussion on a concept for the training of judges in cybercrime/electronic evidence, including online child abuse	5, 7
11-13 Dec 09	Courmayeur Mont Blanc, Italy	International Conference on Protecting Children from Sexual Offenders in the Information Technology Era	7