COUNCIL OF EUROPE CONSEIL DE L'EUROPE

Global Project on Cybercrime (Phase 2)

Summary

Version 26 September 2011

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 (CETS 185) and its Protocol on Xenophobia and Racism (CETS 189)
Budget	Up to EURO 1.4 million (threshold EURO 500,000)
Funding	Council of Europe (Project 1429 - economic crime) Contributions from Estonia, Japan, Monaco, Romania, Microsoft and McAfee
Implementation	Economic Crime Division (Directorate General of Human Rights and Legal Affairs, Council of Europe)
Duration	34 months (1 March 2009 – 31 December 2011)

BACKGROUND AND JUSTIFICATION

Computer networks have turned the world into a global information society in which any kind of information is available to internet users almost anywhere and which provides unique opportunities for people to develop their economic potential and exercise their fundamental rights and freedoms. However, this process is accompanied by an increasing dependency on information and communication technologies (ICT) and a growing vulnerability to criminal misuse and attacks. ICT facilitate illegal access to information, attacks on private or public computer systems, distribution of illegal content as well as cyber-laundering, terrorism and other forms of serious crime. Online fraud is expanding rapidly as cybercrime is increasingly aimed at generating illegal proceeds and as offenders are organising to commit crime on the Internet. This is true for all societies, including developing countries which are relying on ICT without the necessary legal and institutional framework.

Cybercrime thus poses new challenges to criminal justice and international cooperation. In order to counter cybercrime and protect computer systems, Governments must provide for:

- effective criminalisation of cyber-offences. The legislation of different countries should be as harmonized as possible to facilitate cooperation
- investigative and prosecutorial procedures and institutional capacities which allow criminal justice agencies to cope with high-tech crime
- conditions facilitating direct cooperation between State institutions, as well as between State institutions and the private sector
- efficient mutual legal assistance regimes, allowing for direct cooperation among multiple countries.

The "Budapest" Convention on Cybercrime (ETS 185) of the CoE helps countries respond to these needs. It was opened for signature in November 2001 and by December 2008 had been ratified by 23 and signed by another 23 countries. These include non-European countries such as Canada (signed), Japan (signed), South Africa (signed) and the USA (signed and ratified). Costa Rica, the Dominican

Republic, Mexico and the Philippines have been invited to accede. The Additional Protocol on the Criminalisation of Acts of a Racist and Xenophobic Nature Committed through Computer Systems (ETS 189) of January 2003 had been ratified by 13 and signed by another 21 States. Equally important is that a large number of countries worldwide is using the convention as a guideline or model law for the strengthening of their cybercrime legislation.

From September 2006 to February 2009, the CoE implemented the first phase of the Project on Cybercrime in order to support countries worldwide in the implementation of the Convention. The project was funded by the CoE and contributions from Microsoft and Estonia.

During this period the project helped establish the Convention as the primary reference standard for cybercrime legislation globally. This is reflected among other things in the recognition that the Convention received by a wide range of international and regional organisations and the ever stronger cooperation with the private sector and other initiatives.

The project helped create a momentum of cooperation against cybercrime at all levels. Several Octopus Interface conferences and a large number of other meetings were organised or supported. It provided specific legislative advice and helped shape cybercrime legislation in a wide range of European and non-European countries in Africa, Asia, the Caribbean and Latin America. More than 100 countries now use the Convention as a guideline for their legislation. The project familiarised hundreds of law enforcement and criminal justice officers around the world with the investigative tools provided by the Convention. In this connection, modules for the training of judges were prepared. The project promoted effective international cooperation and in particular the creation of 24/7 points of contact and stronger cooperation with the G8 High-tech Crime Subgroup and Interpol.

Issues identified during phase 1 of the project included:

- The need for public-private cooperation, in particular the cooperation between law enforcement and internet service providers. In response, guidelines were developed to help law enforcement and ISPs structure their cooperation in the investigation of cybercrime
- The need to protect personal data and privacy while enhancing the security of cyberspace
- The need for a further strengthening of measures to protect children from exploitation and abuse on the internet.

The present project (phase 2) is designed to follow up on this and to build on the momentum created. It is to serve as a resource allowing the CoE to support European and non-European countries in a pragmatic and flexible manner.

OBJECTIVE, EXPECTED OUTPUTS AND ACTIVITIES

Project objective	To promote broad implementation of the Convention on Cybercrime (CETS 185) and its Protocol on Xenophobia and Racism (CETS 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 Indicators • Legislation analysed of at least 30 countries • At least 10 legal opinions provided and at least 15 draft laws available • Country profiles available for at least 75 countries • Workshops and conferences on cybercrime legislation organised covering up to

	100 countries
Output 2	International cooperation: Capacities of 24/7 points of contact, high-tech crime units and of authorities for mutual legal assistance strengthened Indicators • Directory of contact points updated on a regular basis in cooperation with the G8 High-tech Crime Subgroup • Increase in the number of urgent requests sent and received by contact points • Advice provided to 24/7 points of contact and high-tech crime units • Cooperation manual on mutual legal assistance in cybercrime matters available
Output 3	Investigation: Law enforcement – service provider cooperation in the investigation of cybercrime improved on the basis of the guidelines adopted in April 2008 Indicator • Cooperation agreements concluded between law enforcement and ISPs in at least 5 countries in line with the guidelines developed during the first phase • At least 10 events organised to promote LEA-ISP cooperation • Further proposals for public-private cooperation developed
Output 4	Financial investigations: enhanced knowledge among high tech crime units and FIUs to follow money flows on the internet and stronger cooperation between financial intelligence and investigation units, high-tech crime units and the private sector Indicators • Typology study on money flows and financial investigations adopted and disseminated among MONEYVAL, FATF and Euro-Asia Group members • Up to 2 international workshops carried out • Recommendations on financial investigations on the internet available • Recommendations available on multi-stakeholder action against criminal money on the internet
Output 5	Judges and prosecutors: Training for judges and prosecutors in cybercrime and electronic evidence institutionalised Indicators • Training concept for judges and prosecutors adopted and widely disseminated • Model training manual and workshop for judges and prosecutors available and tested in up to seven training events. • Up to 150 judges and prosecutors trained • Training manual disseminated
Output 6	Data protection and privacy: Data protection and privacy regulations in connection with cybercrime investigations improved in line with Council of Europe and other relevant international standards Indicator • Up to 5 legal opinions on data protection standards in line with CETS 108 and 181 prepared and at least 5 draft laws available in non-European countries

	meeting these standards • Accession requests by at least 3 non-European countries to CETS 108
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 Indicators • Comparative study on the implementation of art 9 (child pornography) of the Convention on Cybercrime • Up to 10 events promoting the Convention on the Sexual Exploitation and Sexual Abuse of Children (CETS 201) and on Trafficking in Human Beings (CETS 197) in relation to the internet.

IMPLEMENTATION ARRANGEMENTS

The project serves as a resource to support:

- activities carried out by the CoE
- activities carried out by other partners with CoE inputs
- the participation of officials from different countries in specific activities carried out by other organisations or partners.

The project is implemented by the Economic Crime Division of the Directorate General of Human Rights and Legal Affairs of the CoE by making use of the expertise available in countries which are party or signatory to the Convention. Close cooperation with public and private sector partners will be sought.

CONTACT

For any additional information please contact:

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

Tel +33 3 9021 4506
Fax +33 3 8841 3955
Email alexander.seger@coe.int