European Commission
Commission européenne

Council of Europe
Conseil de l'Europe

www.coe.int/cybercrime

Project on Cybercrime in Georgia

Summary

Version 19 May 2009

Project title	Project on Cybercrime in Georgia – policy advice (DGHL/2009/2215)
Project area	Georgia
Budget	220,000 EURO
Funding	European Commission and Council of Europe
Counterpart institutions	Ministry of Justice of Georgia Ministry of Interior of Georgia
Implementation	Economic Crime Division (Directorate General of Human Rights and Legal Affairs, Council of Europe)
Duration	12 months (1 June 2009 – 31 May 2010)

BACKGROUND AND JUSTIFICATION

Georgian society, like many others around the world, is increasingly relying on information and communication technology (ICT) and thus increasingly vulnerable to threats such as cybercrime.

Challenges include attacks against the confidentiality, integrity and availability of computer data and systems, including different types of malware (viruses, trojans, worms), botnets and denial of service attacks, phishing and other types of identity theft, computer-related forgery and fraud, child pornography, hate speech and infringements of copyright and related rights. Cybercrime is probably the most transnational of all forms of crime thus requiring extensive and efficient international cooperation. While in the recent past such risks were not considered imminent for Georgia, the perception changed since August 2008 when Georgian websites were under botnet attacks, the country's internet infrastructure was affected due to massive traffic sent and when Georgian websites were defaced.

These attacks showed the clear need to strengthen capacities in Georgia against cybercrime, including legislation, training, the creation of specialized institutions for the investigation of cybercrime, international cooperation and public-private cooperation, in particular cooperation between law enforcement and internet service providers (ISPs).

Georgia signed the Convention on Cybercrime of the Council of Europe in April 2008, but has not yet ratified it. Current criminal legislation seems to meet requirements only partially with regard to substantive law. With regard to procedural tools important provisions are also missing. This not only prevents efficient measures by law enforcement but leaves the obligations of ISPs largely unregulated. Moreover the lack of specific regulations carries the risk of privacy and data protection violations.

In terms of institutional capacities there are no specialized units dealing with high-tech crime in the criminal police and very limited knowledge in the prosecution service and the judiciary regarding cybercrime and the use of electronic evidence.

OBJECTIVE, EXPECTED OUTPUTS AND ACTIVITIES

Project objective	The overall objective of the project is to contribute to the security of and confidence in information and communication technologies in Georgia. The purpose of the project is to help Georgia develop a consistent policy on cybercrime in view of implementing the Convention on Cybercrime (ETS 185).
Output 1	Legislation: Legislative proposals will be available to bring Georgian legislation fully in line with the Convention on Cybercrime and related European standards on data protection
Activities	• Review Georgian legislation against the provisions of the Convention on Cybercrime (ETS 185)
	• Review Georgian legislation against the provisions of the Convention on the Protection of Personal Data (ETS 108)
	• Advise the Georgian working group in the drafting of legislative amendments
	• Up to 2 in-country workshops on cybercrime legislation
Output 2	Training: Training policies and modules are available for standard training courses for law enforcement authorities, prosecutors and judges regarding the investigation, prosecution and adjudication of cybercrime
Activities	• Analysis of training needs for law enforcement, prosecutors and judges
	• Review internationally available training materials and adapt them to Georgian needs
	• Support up to 2 pilot training workshops
	• Support the drafting of a training policy
Output 3	Institution building: Proposals available for the creation of a 24/7 point of contact for international police cooperation, the establishment of a high-tech crime unit within the police and competent authorities for international judicial cooperation in cybercrime cases
Activities	• Review the capacities of the criminal police regarding cybercrime investigations and cyberforensics
	• Propose a design for a high-tech crime unit or a similar specialized unit within the criminal police, including equipment required
	• Prepare a proposal for the creation of a 24/7 point of contact for international police cooperation in line with article 35 of the Convention on Cybercrime
	• Develop a proposal for competent authorities and efficient procedures for international judicial cooperation against cybercrime
Output 4	Law enforcement/internet service provider cooperation: Policy available regarding law enforcement authorities and Internet service provider cooperation in the investigation of cybercrime in line with Georgian legislation and the guidelines adopted at the Council of Europe in April 2008
Activities	• Workshop on law enforcement – ISP cooperation to review current practices and challenges
	• Develop proposals for regulations and other measures to help law enforcement and ISPs to organize their cooperation based on the guidelines developed by the Council of Europe in April 2008.

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 +33-3-8841-2103
Fax +33-3-9021-5650
Email email: cristina.schulman@coe.int