CyberCrime@EAP

Eastern Partnership – Council of Europe Facility:
Cooperation against Cybercrime

www.coe.int/cybercrime

Version 25 April 2012

Agreement number: CN 2010/256-600

Progress Report

covering the period

1 June 2011 – 31 March 2012

Prepared by the
Data Protection and Cybercrime Division
Directorate General of Human Rights and Rule of Law
Council of Europe

Funded
by the European Union
and the Council of Europe

EUROPEAN UNION

COUNCIL OF EUROPE
CONSEIL DE L'EUROPE

Implemented
by the Council of Europe

Contact

For further information please contact:

Cristina Schulman
Head of Cybercrime Unit
Data Protection and Cybercrime Division
Directorate General of Human Rights and Rule of Law
Council of Europe
Strasbourg, France

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

Disclaimer

This technical report does not necessarily reflect official positions of the Council of Europe, the European Union or of the parties to the instruments referred to.

LIST OF ABREVIATIONS

ATM	Automated Teller Machine
CEPOL	European Police College
CNI	Critical National Infrastructure
CoE	Council of Europe
DdoS	Distributed Denial Of Service
DN	Domain Name
DoS	Denial of Service
e.g.	For example
ECTEG	European Cybercrime Training and Education Group
ENPI	European Neighbourhood and Partnership Instrument
ENFSI	European Network of Forensic Science Institutes
EU	European Union
EU-EAR	European Union -European Agency for Reconstruction
FBI	Federal Bureau of Investigation
FIU	Financial Intelligence Unit *or* Financial Investigation Unit
FTK	Forensic Tool Kit
G8	The Group of Eight
GRECO	Group of States against Corruption
HTCU	High Tech Crime Unit
i.e.	*Id est* meaning “that is”
ICT	Information and communications technology
IOCE	International Organisation on Computer Evidence
IP	Internet Protocol
IPA	Instrument for Pre-accession Assistance
ISEC	Prevention of and Fight against Crime as part of the general programme Security and Safeguarding Liberties
ISP	Internet Service Provider
IT	Information Technology
LE	Law Enforcement
LEA	Law Enforcement Agency
LEO	Law Enforcement Officers
MLA	Mutual Legal Assistance
MONEYVAL	Committee of Experts on the Evaluation of Anti-Money Laundering Measures and the Financing of Terrorism
OLAF	European Anti-fraud Office (Office Européen de Lutte Anti-fraude)
OSCE	Organisation for Security and Co-operation in Europe
SECI	Southeast European Cooperative Initiative (Regional Center for Combating Trans-border Crime)
SOCA	Serious and Organised Crime Agency
TAIEX	Technical Assistance and Information Exchange instrument managed by the Directorate-General Enlargement of the European Commission
UN	United Nations
USA/US	United States of America

Contents

1 Executive summary

The aim of the CyberCrime@EAP regional project is to strengthen the capacities of criminal justice authorities of Eastern Partnership countries to cooperate effectively against cybercrime in line with European and international instruments and practices.

Through CyberCrime@EAP the European Union and the Council of Europe support countries of the Eastern Partnership region in their efforts to take measures against cybercrime based on existing tools and instruments, in particular the Budapest Convention on Cybercrime. The countries covered by the project are Armenia, Azerbaijan, Belarus, Georgia, Republic of Moldova and Ukraine.

The project started in March 2011 with an inception phase, which was completed in May 2011 following the launching conference held in Tallinn, Estonia, on 30-31 May 2011. The present report provides an analysis of activities carried out during the period 1 June 2011 to 31 March 2012 under the CyberCrime@EAP project. During this period this the project made considerable progress towards achieving its objectives.

A Cybercrime Situation Report was finalised during the reported period that provides information on the state of capabilities with regard to cybercrime in the six countries. This document is used as a basis for designing project activities carried out under the project. The regional workshops on international cooperation, legislation, financial investigations as well as on specialised high-tech crime units contributed to completing this information, to identifying further national and regional needs and to planning the way ahead for the project.

The main achievements during the reporting period can be summarised as follows:

Result 1: Eastern Partnership countries have defined strategic priorities regarding cybercrime and assessed measures taken

- The launching conference included a session that discussed priorities regarding cybercrime in the region.
- Policy- and decision-makers participated in the activities organised under the project. This resulted in a stronger involvement and support of decision-makers for the project, as well as a greater awareness about cybercrime as a threat against society.
- The activities carried out so far have helped identify needs at national and regional levels, which will be reflected in the declaration on the strategic priorities regarding cybercrime for Eastern Partnership countries to be concluded by the end of the project.

Result 2: Eastern Partnership countries are provided with the tools for action against cybercrime

The project:

- Advised project countries on the strengthening of legislation. In this context, relevant provisions in project countries were assessed from the perspective of their compliance with international standards, in particular with the Budapest Convention on Cybercrime. The main gaps were identified and project countries were encouraged to undertake reforms for reviewing the legal framework. These reforms will bring EAP countries closer to Council of Europe and European Union standards and practices.

- Discussed challenges in the implementation of the Cybercrime Convention (e.g. procedural safeguards and conditions, preservation orders, computer-related fraud etc.).
- Drafted a Cybercrime Situation Report on the current capabilities and situation regarding cybercrime in project countries. Project countries were advised to consider recommendations for improvement made in the Report.
- Submitted a legal opinion on draft amendments to the Criminal Code of Azerbaijan.
- Supported institutional reform, such as advising on the establishment of a specialised high-tech crime unit in Georgia and the National Investigation Centre against Cybercrime in the Republic of Moldova.
- Submitted an expert opinion on the National Investigation Centre against Cybercrime of the Republic of Moldova.
- Identified and discussed the main obstacles that prevent effective investigation of cybercrime, including criminal money flows on the Internet, international cooperation and specialised high-tech crime units.
- Contributed to increasing the efficiency of international cooperation and the 24/7 points of contact[1] in all EAP countries, which are Parties to the Budapest Convention.

Result 3: Eastern Partnership countries participate more actively in international cybercrime efforts

The project facilitated the participation of representatives from project countries in the following events:

- OSCE National Expert Conference: Tackling Cybercrime – A Key Challenge to Comprehensive Cybersecurity (6-7 October 2011, Baku, Azerbaijan);
- G8 High-Tech Crime Sub-Group training event for 24/7 points of contact (8-11 November 2011, Rome, Italy);
- Octopus Conference (21-23 November 2011, Strasbourg, France) and Cybercrime Convention Committee Meeting (T-CY) (23-24 November 2011, Strasbourg, France).

At the level of practical achievements, the project contributed to enhancing the capabilities of law enforcement and judicial authorities to detect, investigate, prosecute and adjudicate cybercrime. Four regional events were organised to exchange experience and share good practices, which increased knowledge of methods used by offenders, as well as of tools and good practices to investigate.

The project pursues a regional approach and generates dynamics of cooperation while bringing in European and other international expertise. In all events organised under the project, good practices were presented by EU Member States (e.g. Belgium, Estonia, Germany, Ireland, Romania, France, the Netherlands and United Kingdom), as well as from the private sector (Microsoft, VISA Inc., PayPal) to be implemented in EAP countries. Synergies were created with a broad range of initiatives and organisations, in particular developed at the European Union level (e.g. Cybercrime Centres of Excellence for Training, Research and Education (2CENTRE), the Organization for Security and Co-operation in Europe (OSCE), Organization for Democracy and Economic Development (GUAM) and others.

The project created synergies with another joint project of the Council of Europe and European Union on cooperation against cybercrime in South-eastern Europe (CyberCrime@IPA), which is funded under

[1] According to Article 35 of the Convention of Cybercrime each Party shall designate point of contact available on a twenty-four hour, seven-day-a-week basis, in order to ensure the provision of immediate assistance for the purpose of investigations or proceedings concerning criminal offences related to computer systems and data, or for the collection of evidence in electronic form of a criminal offence

the Instrument of Pre-Accession (IPA)[2]. This created a great opportunity to link the two projects and exchange experiences in the fight against cybercrime between two regions. Furthermore, this project provides the opportunity to build upon the achievements of the joint EU/COE Project on cybercrime in Georgia, which helped authorities to develop a consistent policy on cybercrime[3].

CyberCrime@EAP project relies on close cooperation with multi-agency working groups that were established in each project country during the inception phase. Representatives of working groups and other institutions confirmed on many occasions the relevance of the project and the need for assistance on these issues at the national and regional level. In most activities organised under the project all project countries participated and contributed to the discussions and to the implementation of the project.

In the regional seminars delegations prepared a set of recommendations for measures to be taken in their respective country. The recommendations provide a valuable input from EAP countries and will be considered in the implementation of the project under each component.

In conclusion, the project – during the reporting period – made important progress towards its objective and advanced under each of the expected results.

[2] For more information about CyberCrime@IPA see www.coe.int/cybercirme

[3] Information available at: http://www.coe.int/t/dghl/cooperation/economiccrime/cybercrime/cy_project_in_georgia/projectcyber_en.asp

2 Description of the Action

Title of the Action	Eastern Partnership – Cooperation against cybercrime (DGHL/2010/2467)
Name of beneficiary of grant contract	Council of Europe
Name and title of the Contact person	Alexander Seger, Head of Data Protection and Cybercrime Division
Contract number	2010/256-600
Project area	Eastern Partnership Countries: Armenia, Azerbaijan, Belarus, Georgia, Republic of Moldova, Ukraine
Duration	30 months (1 March 2011 – 31 August 2013)
Budget	EUR 724 040
Funding	European Commission, ENPI
Implementation	Data Protection and Cybercrime Division (Directorate General of Human Rights and Rule of Law, Council of Europe)
Target countries	Armenia, Azerbaijan, Belarus, Georgia, Republic of Moldova, Ukraine
Final beneficiaries	Media, civil society and general public in the Beneficiaries and international justice and human rights professionals and organizations worldwide
Project partners	-

The objective and expected results of the project are:

Objective	To strengthen the capacities of criminal justice authorities of Eastern Partnership countries to cooperate effectively against cybercrime in line with European and international instruments and practices
Result 1	Eastern Partnership countries have defined strategic priorities regarding cybercrime and assessed measures taken
Result 2	Eastern Partnership countries are provided with the tools for action against cybercrime
Result 3	Eastern Partnership countries participate more actively in international cybercrime efforts

3 Assessment of implementation

The CyberCrime@EAP project started on 1 March 2011 with an inception phase, which was completed with the launching conference held in Tallinn, Estonia on 30-31 May 2011. This phase was very productive and created a solid basis for a successful project:

- The project management team established.
- Activities were carried out from 1 March 2011.
- In all project countries multi-agency working groups are in place and are interacting with the project.
- An updated workplan was prepared and project countries have taken responsibility for the hosting and organisation of activities.
- The logical framework of the project (objectives, results, indicators) has been confirmed during the inception phase. Modifications at the activity level are reflected in the updated workplan, which is a living document that will be further reviewed at future Steering Committee meetings.

The Inception Report was submitted in June and subsequently approved by the European Union.

This present report summarises the activities implemented under the CyberCrime@EAP project between 1 June 2011 and 31 March 2011.

The following activities were carried out during the reporting period:

Date	Place	Activity
May- 6 June 2011	Strasbourg, France	Drafting and sending to the working groups a questionnaire to obtain baseline information with respect to the cybercrime situation in project countries
15 June – 20 September 2011	Strasbourg, France	Assessment of the legislation in project countries regarding its compliance with the Convention on Cybercrime and related international standards
15 July – 31 October 2011	Strasbourg, France	Drafting a situation report based on information collected through the questionnaires
5-6 September 2011	Chisinau, the Republic of Moldova	Regional seminar on international cooperation against cybercrime
December 2011	Strasbourg France	Expert opinion provided on the National Investigation Centre of Cybercrime of the Republic of Moldova
13-14 December 2011	Baku, Azerbaijan	Regional Seminar on cybercrime legislation
27-29 February 2012	Kyiv, Ukraine	Intra-regional workshop on Criminal money flows on the Internet
20-21 March 2012	Tbilisi, Georgia	Regional seminar on specialised cybercrime units

3.1 Activity: Situation Report on the current state of measures against cybercrime in project countries

In order to assess the current state of project countries regarding measures against cybercrime during the Launching Conference and 1st Steering Committee Meeting it was agreed that a Situation Report will be drafted based on information collected with the assistance of the working groups.

Two questionnaires were sent out to the working groups inquiring about a number of legal issues and other measures taken by countries. Based on the replies a report (two parts: legislation and existing measures against cybercrime) was drafted and sent to the project working groups. Overall, the report provides an analysis of the information received and makes recommendations for improvement to be considered by policy makers at national level. Moreover, the report enhances the ability of countries to work effectively with others using similar standards and resources and by concerted actions and effective cooperation.

The Situation Report represents a valuable source of information regarding current status and existing measures against cybercrime taken in project countries. It serves as the basis for planning and designing project activities. Furthermore, it will also serve as a baseline for assessments under expected Result 2 to determine progress made with regard to legislation, strengthening institutional capacities for investigation, prosecution and adjudication of cybercrime and efficient international cooperation.

Situation Report on legislation and international cooperation (Part I)

With regard to legislation the report states that different legislative approaches were taken in project countries, which resulted in different level of implementation of the requirements of the Budapest Convention on Cybercrime. Comparison of legal solutions could be helpful to improve and eventually achieve full implementation of the Cybercrime Convention and relating instruments in the region.

Concerning international cooperation a number of responses consider that the issue of fast international cooperation is a serious impediment to successful investigations in cross border cases. However, not much experience has yet been obtained. That includes experience with 24/7 contact points. Many factors, including legislation, could be of influence on the relatively low appeal on international cooperation. Experience from other countries learns that this may change rapidly in the course of time. Online crime is global and will only continue to manifest itself globally.

Situation Report on existing measures against cybercrime (Part II)

Part II of the Situation Report on measures taken by countries against cybercrime focuses on the following themes:

- Threat of cybercrime;
- Specialised institutions;
- LEA and judicial training;
- Financial investigations and criminal money flows on the Internet;
- LEA-ISP cooperation;
- Other information (including other projects, initiatives).

The responses identify a modest number of cases. The majority of those cases concern credit card fraud, Internet fraud, some hacking and computer sabotage and child porn; with some instances of DDoS-attacks prominent. Where statistics were available a strong increase of cases is reported in comparison of the years from 2006 to 2011. Differences between those periods may be caused by a number of factors including investigation priorities and internal organisation of law enforcement. An important recommendation made in the report is to improve project countries' capacity to keep such statistics.

The reports states that it is a reasonable expectation that the number of cybercrimes affecting countries from the region will strongly increase, keeping path with the growth of economies as well with a strength growth of computer users and computer use.

3.2 Activity: Regional seminar on international cooperation (Chisinau, Republic of Moldova, 5-6 September 2011)

3.2.1 The seminar

Expected result 2 is related to *international cooperation*:

> Eastern Partnership countries are provided with the tools for action against cybercrime – the project supports measures to strengthen the national legislations on cybercrime through defining country-specific needs as well as to assist the understanding and discussion of the challenges of the application of the Convention on Cybercrime (CETS 185).

The main achievements of the regional seminar are:

- Provided the opportunity for sharing experience and good practices on the use of existing standards that allow efficient international cooperation in cybercrime cases;
- Assessed the current situation regarding international cooperation in the region;
- Promoted networking of persons responsible for international judicial and police cooperation;
- Identified the countries where clarifications or further advice is required in order to establish a 24/7 point of contact. Subsequently, the information about the contact points was updated in all project countries that are Party to the Cybercrime Convention.
- Participants prepared a set of recommendations for action to be taken in their respective countries.

From each project area – with the exception of Moldova – three participants were funded from the project budget, representing:

- Ministry of Justice (department on judicial cooperation in criminal matters, including cybercrime);
- Prosecutions services (24/7 point of contact if established within the prosecution);
- High tech crime unit (24/7 point of contact if established within the police).

A fourth participant was funded in the countries where the 24/7 point of contact is established within a different body (i.e. outside the police or the prosecution department).

The Republic of Moldova as host country nominated additional representatives responsible with international judicial cooperation and/or cybercrime investigations.

The regional seminar was opened by Mr Valeriu Zubco, Prosecutor General of the Republic of Moldova, Mr Dirk Schuebel, Head of the European Union Delegation to the Republic of Moldova and the Council of Europe. The Prosecutor General expressed his committed to the project and underlined the measures taken by Moldova to tackle cybercrime, including the creation of the National Investigation Centre of Cybercrime. The representative of the European Union Delegation underlined the support given by the European Union to the countries in the region to tackle cybercrime, as well the excellent cooperation on these issues with the Council of Europe. In the opening remarks the Council of Europe underlined the importance of implementing Chapter III of the Convention on Cybercrime, which provides a legal framework for international cooperation and oblige Parties to cooperate to the widest extent possible. Countries, when becoming parties to the Convention on Cybercrime, need to indicate central authorities for extradition (article 24) and for mutual assistance requests (article 27), as well as 24/7 points of contact (article 35). These authorities and points of contact for international cooperation are very important to increase the efficiency of international cooperation.

The seminar discussed good practices and addressed the difficulties encountered in cybercrime investigations taking into account the existing standards provided by the relevant international instruments.

An overview of the relevant instruments and good practices on international cooperation, including the Second Additional Protocol to the European Convention on Mutual Assistance in Criminal Matters, drawn up within the Council of Europe was provided by an expert from Belgium. Therefore, in addition to Cybercrime Convention, countries are encouraged to join and apply the Second Additional Protocol to the European Convention on Mutual Assistance in Criminal Matters to the fullest possible extent. The concept of direct co-operation between judicial authorities is the central idea prescribed by Second Additional Protocol.

The seminar addressed the need to accelerate the endeavours to increase the efficiency of the 24/7 points of contact established under Article 35 of the Convention on Cybercrime. Further to the T/CY Secretariat request to update the information on the 24/7 contacts points it was agreed that project countries will provide complete information on points of contact where necessary (e.g. Azerbaijan, Ukraine).

The general feedback from the participants was that international cooperation is not achieving the desired results. Participants mentioned issues of delays and non-responsiveness by their counterparts while executing MLA requests. Some delegations experienced difficulties in cooperation with private companies based in the USA, i.e. Facebook, Google, Gmail, Yahoo etc.

The discussion underlined the need for fast exchange of information on cybercrimes due to the specific character of such crimes: their trans-border nature and speed of such crimes require a more efficient mechanism of cooperation. Examples and experiences from Belgium, Estonia, the Netherlands, Romania, United Kingdom and project countries were discussed in the seminar.

The Organization for Democracy and Economic Development (GUAM), which is relevant for cooperation in the region and include as Member States Azerbaijan, Georgia, the Republic of Moldova and Ukraine, made a presentation.

3.2.2 Situation in project countries and recommendations

Armenia

Armenia ratified the Cybercrime Convention (CETS 185) and its Additional Protocol concerning the criminalisation of acts of a racist and xenophobic nature committed through computer systems (CETS 189) on 12 October 2006. It also ratified the Second Additional Protocol to the European Convention on Mutual Assistance in Criminal Matters (CETS No. 182) on 8 December 2010 and signed the Convention on the Protection of Children against Sexual Exploitation and Sexual Abuse (CETS 201), but has not ratified it yet.

In preparation of the ratification of the Cybercrime Convention, the Armenian legislation was amended by Law HO-119-N of 1 June 2006. Armenia has not adopted provisions beyond the obligations set by the Cybercrime Convention; however, the legislation largely complies with its provisions.

In 2010, the hi-tech crime unit of the Organised Crime Department within the Police of Armenia, investigated 15 cases that resulted in the opening of criminal proceedings; 4 - distribution of malware; 1 – storage of child pornography; 4 – distribution of pornography; 1 – collection and distribution of data that contain family or personal secret; 1 – SIM card fraud; 1- false warning of a terrorist attack (this crime was solved due to fast reaction of UK SOCA 24/7 contact point) etc.

The international cooperation with off-shore countries are identified as a main obstacle for delivering effective investigations.

The 24/7 contact point is established within the Division for Fighting against High Tech Crimes, Main Department Fighting against Organised Crime in the Police. According to the information received in 2010-2011, 52 requests for assistance were handled by the 24/7 contact point and 32 requests received.

Recommendations made by the delegation

- To research existing regulations on obtaining evidence from service providers, compare them with the relevant provisions of the EU regulations and make appropriate decision at national level.
- For countries that have joined the Cybercrime Convention, to provide for harmonisation of existing norms regarding typology of cybercrime and corresponding punishment.
- To formalise requests sent through the national contact points 24/7.
- To organise a closed professional conference for the law enforcement agencies to exchange experience in fighting cybercrime and share information on new types of cybercrime and trends in the field.
- To organise continuous training of law enforcement staff, forensic experts, judges and prosecutors.

Azerbaijan

Azerbaijan ratified the Convention on Cybercrime on 15 March 2010. It has not signed the Additional Protocol concerning the criminalisation of acts of a racist and xenophobic nature committed through computer systems (CETS 189) or the Second Additional Protocol to the European Convention on Mutual Assistance in Criminal Matters (CETS No. 182). It signed the Convention on the Protection of Children against Sexual Exploitation and Sexual Abuse (CETS 201) but not (yet) ratified.

The Department of Combating Crimes in Communications and IT Sphere, 24/7 National Contact Point Division, General Directorate of Combating Organised Transnational Crimes within the Ministry of National Security is the 24/7 contact point. The Cybercrime unit is part of the same department. No statistical information is available about cases in which the contact point was involved.

A major impediment for effective international cooperation is considered the lack of political will and the heterogeneity of national legal systems, including the gaps in domestic legislations.

Recommendations made by the delegation

- To take specific measures to improve legal culture in cyberspace.
- To create an efficient platform for inter-agency cooperation in fighting cybercrime.

- To focus on interaction with the private sector.
- To resolve conflicts of jurisdiction when dealing with multi-stage trans-border cases on the assumption that investigation should be carried out in the country where there are evidence of the case that could help solve the case quickly and fairly.
- To adopt a law on cybercrime to provide for a legal, administrative, organisational and technical basis to create conditions for investigation of cybercrime, in particular to establish an obligation of service providers to store technical traces for at least one year.
- To amend the Criminal Procedure Code with regard to the procedure of seizing data stored on digital media, rules for its safe-keeping, depositary institutions, competent institutions to provide expert assessment of the data seized.
- To amend the Criminal Procedure Code with regard to establish conditions of judiciary investigation into cases of child pornography that would not victimise children.
- To establish a national laboratory of digital forensics.
- To define terms to be used by all authorities that in any way deal with hi-tech crime.
- To assign staff in charge with legal assistance within the law enforcement agencies, General Prosecutor's Office, and Ministry of Justice so that to ensure expedited communication on matters of investigation and legal assistance.
- To set up a procedure to register mutual assistance requests and responses in order to keep accurate statistical record; the procedure is to be used individually by each authority that is competent to cooperate with foreign states in this field.
- To develop administrative procedures to monitor the quality of requests processing.
- To develop a common database on offences, offenders, forms and methods of criminal activity; all relevant authorities having direct access thereto.
- To establish strict professional criteria for selection of heads or coordinators of the contact points. For instance, they should speak the Council of Europe official languages, have a degree in law and a certain minimum knowledge of IT.
- To raise the status of the coordinators/heads of the contact points so as to empower them to assess incoming requests from the point of view of the domestic law and national interests, make decisions (at least regarding those parts of a request, which would not require a higher level of decision-making) and order service providers to preserve relevant data.
- To develop training courses to raise professional qualification of the contact points coordinators.

Belarus

International cooperation is regulated by section XV BeCP. Police cooperation is allowed under Belarus law. If these specific powers can be applied in case of an incoming MLA-request depends on domestic procedural law (see *para* 5.5). Not all the investigative powers defined by the Cybercrime Convention are part of Belarus' BeCP.

Belarus is member of the G8 Network since 2008 and the contact point is established in the Ministry of Interior. Statistics for National Contact Point requests in 2011:

- Sent requests – 226 (Russia-172, Lithuania-14, Ukraine-13, Germany-7, US-4, Nethrlands-3, Italy, UK, Czech Republic-2, Kazakhstan, Norway, Luxemburg, Belgium, Israel, Romania, Bulgaria -1)
- Received ansvers-188
- Sent answers and information – 20 (Russia, Ukraine, Italy, Germany)

Recommendations made by the delegation

- To establish conditions required for Belarus to join the Convention on Cybercrime.
- To develop a strategy for training judges and prosecutors on cybercrime investigation and digital forensics. To provide training for judges and prosecutors on matters related to cybercrime and digital forensics.
- To better equip national cybercrime units with edge-cutting special-purpose soft- and hardware.
- To take steps to found a national computer emergency response team (CERT) and integrate it into the international CSIRT/CERT network.

Georgia

Georgia signed the Convention on Cybercrime (CETS 185) on 1 April 2008 and the Convention on the Protection of Children against Sexual Exploitation and Sexual Abuse (CETS 201) on 12 march 2009. It has not signed the Additional Protocol concerning the criminalisation of acts of a racist and xenophobic nature committed through computer systems (CETS 189) or the Second Additional Protocol to the European Convention on Mutual Assistance in Criminal Matters (CETS No. 182).

A specific joint EU/COE Project on cybercrime was implemented in 2009/2010 in Georgia, which included legal advice on cybercrime legislation[4]. Amendments implementing Cybercrime Convention were adopted by the Parliament soon after the ending of that project. It is expected that Georgia will ratify soon the Cybercrime Convention.

Georgia has cybercrime laws in place. The specific powers of the Cybercrime Convention are part of domestic law and can be applied in case of incoming requests for international co-operation.

According to the information received no incoming requests for cooperation were received or sent. Direct cooperation with other national police bodies is possible. On-going work is carried out in Georgia to set up a 24/7 contact point.

Recommendations made by the delegation

- Ratification of the Convention on Cybercrime.
- Creation of a 24/7 contact point under the Ministry of Internal Affairs of Georgia. The point will be in direct contact with prosecution and investigation services all over the country.
- Professional trainings for personnel at all levels in the field of investigating cybercrime for IT personnel, investigators, prosecutors and judges.
- Creation of the specialised unit for investigating cybercrime under the Ministry of Internal Affairs of Georgia. The unit will consist of IT experts and investigators.
- Organisation of regional seminars in Georgia in order to share experience of foreign countries in the field of combating cybercrime: methods of investigation, specific programs, recommendations/ instructions.

[4] For more information see: http://www.coe.int/t/dghl/cooperation/economiccrime/cybercrime/cy_project_in_georgia/projectcyber_en.asp

The Republic of Moldova

Moldova signed the Cybercrime Convention on 23 November 2001 and ratified it on 5 May 2009. The Additional Protocol was signed on 25 April 2003, but not yet ratified. The Convention on the Protection of Children against Sexual Exploitation and Sexual Abuse (CETS 201) was signed on 25 October 2009 and recently (12 March 2012) was ratified. The second Additional Protocol to the MLA Convention (CETS 182) has been signed by Moldova on 13 March 2012.

In principle, Moldova is capable of cooperating internationally provided that the laws are supplemented and reviewed as recommended in the Situation Report. From the other information provided it can be concluded the following that little experience with MLA-requests has been obtained. In the first quarter of 2011 three MLA-requests were executed, nine requests were submitted through Interpol and SECI/GUM.

Recommendations made by the delegation

- Establishment of the Cybercrime Investigation Centre at the national level (Centre).
- Develop and amend the national normative framework to specify attributions, duties and structure, personnel, objectives of the Centre forming a legal base of its functioning.
- Review of the national normative framework in combating cybercrimes and its coordination with the Convention on Cybercrime.
- Establishment of a joint mechanism of transmission-reception and execution of rogatory commissions and setting time limits for their execution, as well the development of a standard form (common content) of the rogatory commissions submitted for execution between the competent authorities.
- Professional joint training of experts in combating cybercrimes and preserving/storing digital evidence, especially of the departments’ personnel involved in the process.
- Unification of the jurisprudence in the field and development of methodological guidelines on the specificity and positive practices of cybercrime investigation.
- Determine the way of interaction between interstate law enforcement authorities in a joint group in case of committing transnational serious crimes using information technologies.

Ukraine

Ukraine was one of the first countries in the region that signed the Cybercrime Convention and ratified the Convention on 10 March 2006. Ukraine ratified the Additional Protocol to the Cybercrime Convention on 21 December 2006 and the Second Additional Protocol to the European Convention on Mutual Assistance in Criminal Matters (CETS No. 182) on 14 September 2011. The Convention on the Protection of Children etc. (CETS 201) was signed on 11 November 2007 but not (yet) ratified.

The 24/7 contact point is part of the Ministry of Internal Affairs. No statistics about the number of requests are available.

Recommendations made by the delegation

- To provide the Council of Europe with the contact details of the 24/7 national contact point (within the Ministry of Interior of Ukraine).
- To take measures to initiate amendments in Ukraine regarding expedited preservation of computer data including traffic data stored in computer systems, in particular, where there are grounds to believe that such computer data are especially vulnerable to loss or modification (Cybercrime Convention Articles 16, 29, 30).
- To take measures to initiate amendments in Ukraine regarding real-time collection of traffic data (Cybercrime Convention Articles 20, 33), interception of content data (Articles 21, 34).
- To propose a standardised form of request for technical advice (Cybercrime Convention Article 35) and respective response covering typical situations of information exchange, taking into consideration the domestic legislation in different countries and the need to speed up data exchange by formalisation and automation of data verification and processing.
- To propose to develop a common platform (a forum) for the 24/7 network with enhanced information protection and user- friendliness.
- To provide for Ukraine's participation in OCTOPUS conferences and other activities within the Project (four people; one from each of the following headquarters: Ministry of Justice, General Prosecution, and Ministry of Interior plus a representative of the private sector).
- It seems feasible to hold regional seminars in Ukraine on fighting cybercrime introducing an international aspect thereto so as to develop qualification of judiciary and law enforcement (expert, methodological (overview of existing practice and reports on activities of 24/7 contact points) and financial support are welcomed,

From the Situation Report and discussions in the seminar it resulted that except Ukraine and Belarus not much experience in investigation cybercrimes has yet been obtained. This includes also experience of 24/7 contact points in exchanging. The answer to the question about trans-border investigative activity is not clear. Further work will be carried out on this issue in the Cybercrime Convection Committee (T-CY) where most of EAP countries (except Belarus) are represented as Parties or observer (Georgia).

3.2.3 Follow up

- Work under the project to fill the gaps in national legislation aimed at ensuring an effective international cooperation in line with the Cybercrime Convention and other relevant standards;
- Encourage EAP countries to ratify the relevant Council of Europe instruments e.g. Convention on Cybercrime (Georgia, Belarus), Additional Protocol concerning the criminalisation of acts of a racist and xenophobic nature committed through computer systems (Azerbaijan, Belarus, Georgia, the Republic of Moldova), the Second Additional Protocol to the European Convention on Mutual Assistance in Criminal Matters (Azerbaijan, Belarus, Georgia, the Republic of Moldova), the Convention on the Protection of Children against Sexual Exploitation and Sexual Abuse (Armenia, Belarus, Georgia, Ukraine);
- Training for staff responsible with MLA;
- Increase the efficiency of the 24/7 contact point;
- Ensure participation of EAP countries in the Octopus and Cybercrime Convection Committee (T-CY), including in the discussion on transborder access of data.
- Support a follow-up to the recommendations drafted in the workshop.

3.3 Activity: Regional seminar on legislation (Baku, Azerbaijan, 13-14 December 2011)

3.3.1 The seminar

Expected result 2 is related to cybercrime *legislation*:

> Eastern Partnership countries are provided with the tools for action against cybercrime – the project supports measures to strengthen the national legislations on cybercrime through defining country-specific needs as well as to assist the understanding and discussion of the challenges of the application of the Convention on Cybercrime (CETS 185).

Adequate legislation in place is a prerequisite for all related measures against cybercrime e.g. training for judges and prosecutors, cooperation between law enforcement and internet service providers, international cooperation etc.

Based on the information received from EAP countries, a Cybercrime Situation Report was prepared, which assessed the legislation in project EAP countries from the perspective of their compliance with the Cybercrime Convention. The aim of the report is to provide an overview on the existing measures undertaken by the countries covered by the project and make recommendations for improvement that can be implemented individually by each country as well as at the regional level. This Report includes a section on the existing legal framework of each country and provides country specific advice for improvement.

The regional seminar on legislation held in Baku, Azerbaijan, was aimed at discussing the findings of the Cybercrime Situation Report and the actions to be taken to implement its recommendations made regarding legislation. The seminar also intended to help countries face some problematic issues in the implementation of the Budapest Convention.

Three representatives from each country - with the exception of Azerbaijan - were funded by the project, representing:

- A governmental institution involved in the development of cybercrime legislation, a parliamentary body or working group responsible for such legislation.
- Prosecution unit (department specialised in high-tech crime).
- A judge dealing with cybercrime cases.

Armenia was not represented in the seminar.

The main achievements of the seminar are:

- Provided advice to project countries on strengthening of legislation and discussed the gaps identified in the Situation Report.
- Discussed challenges regarding the implementation of some articles of the Budapest Convention e.g. safeguards and conditions, preservations or data retention, electronic evidence etc.
- Discussed the effectiveness of the legislation in project countries with regard to prosecution and adjudication of cybercrime cases.
- Participants prepared a set of recommendations for action to be taken in their respective countries.

Experts from Estonia, the Netherlands and Microsoft contributed to the event. The seminar discussed in details the implementation of the Budapest Convention provisions in EAP countries.

Gathering and presenting electronic evidence in the court is a general difficulty in practice for prosecutors and judges. Thus the seminar ensured that good practices and experiences from other countries (the Netherlands, Estonia) and the private sector (Microsoft) were presented and discussed.

Review of articles of the Budapest Convention

The seminar discussed the observations and recommendations provided by the Situation Report. An overview was provided on the following common/major problems identified:

- The definitions of different notions are not clear (without right, computer system etc.), which might create problems in practice.
- Article 2 and 3 of the Cybercrime Convention are not fully understood and thus are not adequately implemented in national legislations.
- The combination of several offences in one article may limit or broaden the provisions of the Budapest Convention.

Substantial law: Article 1 Definitions

Different notions are used in legislations analysed e.g. computer network, computer devices etc. instead of the comprehensive term ''computer system'' provided by Article 1 of the Convention. Although the Parties to the Cybercrime Convention are not obliged to copy *verbatim* the definitions of the Convention, they should implement the concept behind these terms in a consistent manner and in line with the principles of the Convention.

Concerns were raised, in particular in relation to the legal meaning of the term "*without authorisation*". Several domestic provisions include a mental element not only different from the Convention, but which might limit the application of respective provisions e.g. illegal, without permission, unlawful, without right etc. The recommendation made was that the more general the definition applied in domestic legislation the broader the scope is.

Azerbaijan pointed out that the intent under Criminal Code has to be illegal, meaning without permission or authorisation. The Belarusian delegation stated that the Criminal Code does not contain definitions but once Belarus becomes a Party to the Convention, the definitions will apply into the national legislation. In Georgia the notion "*without right*" is understood as illegal and covers possible cases for direct and indirect intent. It was agreed that the legal meaning of the term "without right" is broader than illegal. The delegation of the Republic of Moldova raised the issue of translation in the interpretation given in the Situation Report and underlined that although the definitions are provided by a specific law, they apply for criminal law in general. Ukraine stated that the definitions are not included in the criminal code but in the Telecommunication and apply in general.

Substantial law: Article 2 – Illegal access

The Convention criminalises the mere (illegal) access, which is aimed at protecting the interests of organisations and individuals to manage, operate and control their systems in an undisturbed and uninhibited manner. Thus criminal liability is attached to this conduct (access without right) and it is not required other additional conditions in order to be an offence.

Explanation was given for the difference between '′illegal interception′′ and '′illegal access′′. It was also pointed out that a correct definition of a computer system is essential for Article 2 since the computer system is a container of (computer) data being stored, processed or transferred by it.

In general, delegations agreed with the observations made in the report. Azerbaijan and the Republic of Moldova informed about on-going or planned legal reforms that will consider the recommendations. In some cases, court decisions provide an interpretation for these notions.

Substantial law: Article 3 – Illegal interception

There is an important distinction between Article 2 and Article 3 of the Convention that needs to be considered when implementing these articles. Article 2 deals with illegal access to a computer system "through the front door", while Article 3 focuses on other ways to capture information flows, in particular by application of technical means. Article 2 has a broader meaning whilst Article 3 is privacy oriented and not directed at a particular system but generally to the storage in a system. The main observation regarding illegal interception is that the concept of the Cybercrime Convention was not fully understood.

All delegations agreed on the observations and expressed that the implementation of these provisions needs to be improved in line with the Budapest Convention.

Substantial law: Article 4 – Data interference

It was advised not to include several articles of the Convention into a single paragraph because this may result in misinterpretations. It is better to include the offences provided by the Convention in separate articles and add aggravating circumstances if this is desired.

Attention to be made not to make reservations that will limit the scope of these provisions. Azerbaijan (made a reservation to include serious harm) accepted the explanation and the requirement for improvement. Belarus pointed out the complexity of elaborating definitions and accepted the observations to make use of the Explanatory Memorandum of the Budapest Convention as a guide in drafting legislation, as well as examples from other countries. The Republic of Moldova agreed on the improvement of the national legislation with regard to Article 4, in particular since no reservation was made when ratifying the Convention. Ukraine informed the participants that it is planned to revise the section of the Criminal Code with regard to cybercrime offences. By February 2012 a draft may be available.

Substantial law: Article 5 – System interference

The definition for "serious hindering" may be a difficult task. Hindering shall be criminalised when it prevents the functioning of a computer system and slows down the process. The article does not cover the real interference (when creating a risk for the functioning of a computer system). Aggravating circumstances may be added in order to differentiate the seriousness of hindering.

The delegations agreed that the main problem is defining "serious hindering". Belarus informed the participants that the Criminal Code of Belarus is old and not updated to effectively fight cybercrime (there are many general provisions but amendments are needed). The Ukrainian delegation agreed that there is a further need for improvement of the provisions in their national legislation to comply with the Convention.

Substantial law: Article 6 – Misuse of devices

The implementation of this article is difficult and, thus, the Convention offers the possibility to make reservations, which allows for a restricted or non-implementation of *para* 1a. The minimum is, however, criminalisation sale, distribution or otherwise make available of the items provided under paragraph 1a, ii (passwords, access codes etc.). The offence has to be committed intentionally and without right.

The wording "primarily designed or adapted" refers to the situation when a device has an original function but this function was abused for other purposes. This element prevents a too narrow scope of Article 6.

The delegations provided clarifications regarding the implementation of this article and agreed on the need to further review the national provisions on the occasion of ratification/accession (Georgia, Belarus) or when future amendments are prepared in the case of the other countries.

Substantial law: Article 7-8 – Computer related forgery and computer related fraud

The aim of Article 7 is to ensure that Parties review its laws on forgery in order to make these provisions applicable to the electronic environment. Traditional provisions on forgery may refer to all types of documents to be used in different situations or for different purposes. When such documents are replaced by digital or electronic equivalents, forgery provisions should apply also in such situation. For this reason, Article 7 is drafted in the form of a traditional forgery provision, however referring to electronic or digital equivalents (data strings, records, files).

Similarly, the aim of Article 8 is to review relevant fraud provisions and to establish that the way an illegal transfer of property is achieved is also criminalised if caused by means of electronic manipulation.

The concept behind these offences was neither fully understood nor implemented in the national legislations of EAP countries.

Substantial law: Article 9 – Offences related to child pornography

The aim of Article 9 of the Convention is to accomplish a review of existing legislation by the Parties with regard to computer-related offences to ensure protection of children against sexual exploitation when computer systems are used in the commission of sexual offences against children.

It was emphasised that this offence belongs to offences committed against minors rather than offences against moral.

In this context, it was underlined that full ratification and implementation of both the Cybercrime Convention and the Convention on the Protection of Children against Sexual Exploitation and Sexual Abuse is very important.

Procedural law: Article 16 -17 – Expedited preservation

This article gives law enforcement the power to order preservation of volatile data for a period of 90 days. It was explained that it does not refer only to service providers considering that not only service providers can have control over data.

A general problem regarding procedural law provisions, in particular Articles 16-19, is that they were not fully implemented in national legislation of EAP countries. The implementation of Article 19 needs to be improved and clarified in project countries.

For example, the Azerbaijani procedural law cannot be considered sufficient. The Situation Report clearly identified that Article 16-19 are (partly) not implemented.

Procedural law: Article 18 – Production order

Insufficient information was provided by most of the Working Groups from project countries regarding the disclosure of data. The scope of this provision is that data is taken "under control" of the competent authorities both from service providers and natural persons. The concept behind Article 18 is to enable authorities to obtain data with a less intrusive measure than search and seizure. The article does not seek to seize but to disclose specific data, regardless if it is followed by a formal seizure of the data carrier.

In general, the delegations agreed with the observations and recommendations made in the report. Belarus informed the participants that there are several laws that can be used as legal basis by the Belarusian authorities to request information from anybody. This procedure applies to criminal procedure in general regardless of the nature of the crime.

Procedural law: Article 19 – Search and seizure of stored computer data

Due to insufficient information received, the preliminary assumption was that these provisions are not adequately implemented. A computer or computer system can be anywhere and, thus the legislation needs to ensure powers for competent authorities to access the locations where data is available. A computer system can have several users and, therefore it is not possible to seize the whole system. It should be possible to copy data and deleted it afterwards.

Azerbaijan provided a general explanation of the procedure on search and seizure and ensured that observations made will be considered. Belarus explained that there are no specific provisions and general rules on obtaining electronic evidence are applied. Georgia pointed out that there is a general problem of the criminal justice system in the region that in order to fully implement the requirements of the Convention national legislations need to be changed. The Republic of Moldova explained that general provisions are applied in case of search and seizure of computer data. The future National Investigation Centre for Cybercrime will include specific measures and its staff will be trained accordingly. Ukraine informed the participants that the criminal code is subject to reform in the course of the beginning of next year.

Procedural law: Article 20-21 – Real-time collection of traffic data/Interception of content data

It is not only the technical equipment that is required, but cooperation with service providers needs to be developed. These provisions are intrusive and, therefore it is necessary that a warrant to be issued. The application of traditional provisions on interception of communications might raise problems in practice due to the nature of electronic data.

Belarus informed that there is a law on operational investigative rights and regulations regarding cooperation with service providers. After a warrant is issued by the prosecutor, the police can collect traffic data and intercept content data although this is not specified in the national legislation. The Georgian legislation is similar to the provisions of the Convention and needs only little changes. The delegation of the Republic of Moldova noted that a draft law is being elaborated and will cover the gaps identified. However, technical equipment is required to be able to collect and intercept data. Ukraine explained that the provisions apply to any form of communication and there is no difference if it is in electronic format or not. As the criminal code is currently subject to reform this will allow for amendments and corrections.

Without availability of all relevant legal texts, it was not possible a full analysis. A number of questions remains open before it can be said that Articles 19 and 20 of the Convention are fully implemented in the legislations analysed e.g. definition of service provider; how factual interception of communications is achieved, in particular internet communications? on the basis of which specific powers subscriber data are obtained by the investigating authorities, and if other agencies are competent, how is the exchange of this information regulated? Grounds for application?

As mentioned in the executive summary the conditions and safeguards (duration of measure, judicial supervision etc.) will be considered later on under the project.

Challenges in the implementation of the Budapest Convention

The Chair of the Cybercrime Convention Committee (T-CY Committee) explained the structure and role of the Committee as well as the main challenges in the implementation of the Convention:

- Lack of interest
- Non- (real) commitment
- Representatives of the Parties do not always participate actively in the work of the T-CY
- Lack of coordination at national level

The T-CY works on the problems addressed by Parties and, thus it facilitates the implementation of the Convention.

Due to the importance of **Article 15 (Conditions and safeguards)** of the Budapest Convention, a special session was dedicated to explain this provision. It was stated that principles of a fair trial have to be maintained throughout the criminal procedure, especially with regard to the application of special investigative powers. The implementation of these measures should be done by ensuring the relevant conditions and safeguards (e.g. proportion of intrusiveness, principle of equality during the procedure, constitutional and fundamental rights etc). The existence of an independent body in a country has to be ensured to apply the safeguards. The example of Netherlands was presented, which explained the application of different investigative powers and safeguards. It is the investigative judge who is authorised to approve such powers. The prosecutor is only entitled to perform part of these powers and police is empowered by the prosecutor. The application of special powers requires special circumstances although an official report is required (even if it is given later) on some circumstances: suspicion of serious crime; in case of urgency oral empowerment is can be applied only if it is confirmed in writing; special investigative measures are urgently required.

Microsoft highlighted the importance of electronic evidence and practical problems regarding gathering and presenting electronic evidence in the court. The role of electronic evidence in legal procedures is increasing (not only in cybercrime cases but other crimes as well). Parties to the Budapest Convention have the responsibility to ensure the exchange of such evidence. The presentations focused on the following issues:

- Cybercrime is a cross jurisdictional crime (victims, perpetrators, evidence is scattered in different places).

- Technical subject matter (requiring training).
- The problem of virtualised communication.
- Balancing freedom and security through the protection of personal information.
- Person identifying information.
- Cooperation between the public and private sector.

3.3.2 Situation in project countries and recommendations

Azerbaijan

With regard to substantive law provisions, once the draft law will be adopted the legislation in Azerbaijan will largely comply with the requirements of the Cybercrime Convention. Most of the recommendations made in the legal opinion submitted under the project to the Working Group were included in the revised version. Few additional suggestions were made in the Situation Report for further improvement.

However, there is an urgent need to establish a Working Group in Azerbaijan to prepare amendments to the procedural law. In particular, there is a concern about (partly) missing implementation of Articles 16-19. The equivalent procedures around Articles 20 and 21 may need further review.

In this respect a letter was sent to the Head of Department on Work with Law-Enforcement Bodies Administration of the President of Azerbaijan welcoming the progress made regarding the amendments to the Criminal Code and supporting a similar effort with respect to procedural law.

With regard to international cooperation there is a 24/7 contact point operational. However, the number of cases in a year is modest.

Recommendations made by the delegation

- Electronic and other carriers are listed among the documents in Article 135 of the Criminal Procedural Code (CPC). It is necessary to make clarifications in this article in accordance with the requirements of the Convention.
- Article 7 of CPC stipulates main definitions used in the Criminal Procedural Code.
- Since the CPC was adopted in 2000, improvement of its definitions section as well as the introduction of the definitions used in the Convention on Cybercrime is suggested (for instance, provider, computer database, computer systems, etc.)
- Article 259 of CPC regulates the capture of information transmitted by means of communications and other technical means. The modification of this article in accordance with relevant articles including Article 20 of the Convention is suggested.
- Article 445.1.3 of CPC determines "extraction of information from technical communication channels and other technical means". Adjustment of this paragraph in accordance with appropriate articles, Articles 17, 18, 19 of the Convention on Cybercrime is suggested.
- Preparation of amendments in line with the requirements of Articles 16, 17, 19 of the Convention in the relevant legislation of Azerbaijan is expedient.
- In order to increase the effectiveness of cooperation between law enforcement bodies and service providers to make use of the Council of Europe Guidelines on cooperation between the law enforcement and service providers.
- Taking into account the experience of Microsoft in collection and submission of electronic evidences, to modernize computer forensic laboratory under Forensic Examination Centre of the Republic of Azerbaijan and to use it for investigation of such crimes.

Belarus

Specific attention should be given to the definitions in relation with substantive and procedural law provisions. Correct implementation of Articles 2, 6 and 9 of the Convention is recommended and implementation of Article 12 (corporate liability).

With regard to procedural law, additional information is needed for an analysis of the implementation of Article 15 (Conditions and safeguards) of the Cybercrime Convention. The preliminary measures (expedited preservation) have not been implemented.

The system of data retention does remove the need for powers to order expedited preservation foreseen in Article 16. Article 18 has not been fully implemented and Article 19 has been only partly implemented. No information was provided to what extent these powers can be executed in an expedited manner. It is unclear whether Article 20 has been implemented, or whether the authorities rely on the system of data retention. It is not clear to which kind of service providers that system applies. Apart from the applied definitions, there is still a need for a power as provided by Article 20.

With regard to international cooperation, a review of the current substantive and procedural law may be necessary in order to create conditions for international cooperation.

Recommendations made by the delegation

- Continue to work towards the accession of the Republic of Belarus to the Council of Europe Convention on Cybercrime. The Ministry of Internal Affairs of the Republic of Belarus requested the Ministry of Foreign Affairs to address the Secretary General of Council of Europe a request to consider the possibility of accession by Belarus to the Budapest Convention.
- To review and consider the possibilities to prepare amendments in the following year to the national legislation of the Republic of Belarus in order that the national legislation becomes more in line with the requirements of the Budapest Convention.
- To analyse the standards of Cybercrime Convention together with representatives of the scientific community, judiciary, prosecution services and investigative units as well as to examine the standards of substantive and procedural law of Belarus with a view to implement the requirements of the Convention.
- To examine the strategy on training for judges and prosecutors with regard to cybercrime investigations and cyber forensics as well as to hold appropriate trainings for judges and prosecutors (including joint trainings with members of other stakeholders of the criminal justice system) with foreign experts.

Georgia

A specific joint EU/COE Project on cybercrime implemented in 2009/2010 in Georgia[5], which included legal advice on cybercrime legislation. Amendments to the legislation in order to implement Cybercrime Convention were adopted by the Parliament soon after ending the project. Therefore the legislation in Georgia is largely in line with the requirements of the Cybercrime Convention. It is expected that Georgia will ratify soon the Cybercrime Convention.

[5] For more information, please follow the link to the webpage of the project: http://www.coe.int/t/dghl/cooperation/economiccrime/cybercrime/cy_project_in_georgia/projectcyber_en.asp

Recommendations made by the delegation

As a general note, Georgia would initiate and implement the legislative amendments listed herein on the condition that there would be no possible delays in ratification/accession process:

- Georgia should revise and update the definitions of substantive criminal law provisions related to child pornography in order to sufficiently address acts of grooming and obligations deriving from the CoE Convention on Protection of Children against Sexual Exploitation and Sexual Abuse.
- In case reservations are made on this matter, envisage the possibility to implement Article 16-17 of the Convention at a later stage, provided that resources for expedited preservation are available; gradual or sectorial introduction may also be a solution.
- Add provisions to criminal procedure legislation that fully implement paragraphs 2, 3 and 4 of Article 19 of the Convention.
- Resolve potential constitutional challenge to internet surveillance provisions in the Law on Operative-Search Activity.
- Adjust terminology in Article 136-138 of the Criminal Procedure Code to remove limitations related to acts being committed "through the computer system".
- Adopt the currently discussed Personal Data Protection Law to provide universally applicable definition of "data controller".
- Adopt the currently discussed Law on Information Security as one of the means for cybercrime prevention and a platform for extended CERT/law enforcement cooperation.
- Launch regular review of national case law on cybercrime to ensure that admissibility and use of digital evidence develops along the general lines of currently applicable rules of evidence, and to propose/implement changes in case the current regulations prove insufficient.

The Republic of Moldova

With regard to substantive law it is recommended to review the provisions referred to on the basis of observations and suggestions made in the Situation Report. Due to contradiction or inadequate implementation of the Cybercrime Convention special attention should be paid to Articles 259, 260^2, 260^4 and 208^1.

With regard to procedural law review is recommended of the provisions referred to on the basis of the observations and suggestions made in the Situation Report. On the basis of the information provided some interference appeared between the system of Criminal Procedural Law and the provisions of the Law on Preventing and Combating Cybercrime of 2010. The way the power of Article 16 has been implemented needs additional clarifications e.g. the time involved before action can be taken. Article 18 needs to be more clearly defined and Article 19 is not implemented with regard to specific powers. The concept of seizure may not be applicable.

Recommendations made by the delegation

- Amendments to the Criminal Code (hereinafter "the CC") in order to make criminal liability independent from the occurrence of detrimental effects (the draft law on the amendment of the CC passed the national interdepartmental group).
- Adjustment of the CC in line with the Additional Protocol to the Cybercrime Convention by introducing new articles regarding racism and xenophobia (the draft law on the amendment of the CC was submitted to the Government).

- Adjusting the existing definitions to the Cybercrime Convention requirements (a detailed report will be submitted in due time).
- To regulate search and seizure of a computer system in a separate provision along the lines of Article 19.
- To amend existing provisions of the Criminal Procedure Code (hereinafter "the CPC") with special rules regarding collection in real-time of traffic data and real-time interception of content data.
- To supplement the CPC with new provisions regarding the procedural rules of data preservation, meaning the preservation of data from the national ISPs on the motivated request of the Prosecutor.

***

- Final work on the establishment and functioning of the National Centre for Cybercrime Investigation.
- Renewal of the National Action Plan on Preventing and Fighting Cybercrime.
- Adoption of a new law on monitoring the internet.

Ukraine

With regard to criminal substantive law there is no effective implementation of Articles 2, 3, 5, 6 of the Convention. It is recommended to review the provisions referred to based on the questions, observations and suggestions made in the Situation Report, in particular concerning the implementation of Articles 7, 8 and 9. Attention to be given also to the definitions and their applicability to the offences provided by the Criminal Code.

With regards to procedural law no implementation has been found of Articles 16, 18, 19.

With regards to international cooperation Ukraine is in principle capable of rendering MLA.

Recommendations made by the delegation

- To finalise the draft amendments to the Criminal Code with regard to measures against cybercrime within the Inter-Ministerial working group.
- To analyse the compliance of the national legislation with the Cybercrime Convention. There are some conducts that are not criminalised.
- Currently there are no such rules as provided by Article 2 of the Cybercrime Convention, however the prosecution of perpetrators illegally accessing systems (without permission) in order to access and influence data can be concluded upon Article 361 of the Criminal Code of Ukraine. Such an approach could suit Ukraine without the gander of over-criminalisation.
- To take into account the requirements of the Budapest Convention with regard to search, seizure and use of evidence in the form of computer data.
- To amend the Law on Telecommunications on the time span of storing computer data and identifying information and also to amend the legislation on definitions, terminology to be in line with the Budapest Convention.
- To continue the utilisation of the Unified State System against cybercrime.

3.3.3 Overall assessment

The Easter Partnership countries have divers national cybercrime legislations. Some countries applied the minimum level of requirements and some (e.g. the Georgian legislations) went further. Moreover, there is a different level of experience regarding cybercrime issues.

The provisions of the Budapest Convention are not or not fully implemented. The concept behind some of the articles is not entirely reflected in most of the national cybercrime legislations. Future legislative reforms should consider amendments to ensure full compliance with the Cybercrime Convention and related standards.

Gathering and using in the court digital evidence still remains a challenge due to lack of experience and lack of implementation of both the substantial and procedural provisions of the Budapest Convention.

The seminar served as a platform for better understanding of the concepts and principles of the Budapest Convention. The recommendations made by the delegations showed the need for further need to review and improve national legislation.

3.3.4 Follow up

- Provide further advice in project countries on adequate implementation of the provisions of the Budapest Convention.
- Involve EAP countries in the drafting of Electronic Evidence Guide to be developed under CyberCrime@IPA.
- Assess the application of law in practice during different project activities, including peer-to-peer assessment visits.
- Support a follow-up to the recommendations drafted in the workshop.

3.4 Activity: Legal opinion on draft law amending the Criminal Code of Azerbaijan

As previously indicated, a legal opinion was submitted on 27 May 2011to the Azerbaijan authorities, which provided an assessment of the draft law in view of its compliance with the requirements of the Cybercrime Convention.

Further advice on the revised version that included most of the recommendations made in the legal opinion was included in the Situation Report (legislative Part).

See also section 3.4

3.5 Activity: Intra-regional seminar on criminal money flows on the Internet (Kyiv, Ukraine, 27-29 February 2012)

3.5.1 The seminar

Expected result 2 is related to *financial investigations*:

> Financial investigations: awareness raised to confiscate proceeds from crime on the Internet among representatives of FIUs, asset recovery and financial investigation bodies, police and prosecution dealing with high-tech and economic crime and corruption, financial and supervisory authorities, banks and ISPs. Interagency and public-private cooperation in this area is strengthened as well as countermeasures and good practices are identified.

Under this result, the project supports raising awareness of the need for confiscating proceeds from crime on the internet, strengthens interagency and public-private cooperation against criminal money flows on the internet as well as identifies countermeasures (good practices) that could be implemented in EAP countries.

The activity was organised as a joint activity with the CyberCrime@IPA joint project on cooperation against cybercrime in South-eastern Europe implemented under the Instrument of Pre-Accession (IPA)[6]. Both projects include a component that supports raising awareness of the need for confiscating proceeds from crime on the internet, strengthens interagency and public-private cooperation against criminal money flows on the internet as well as identifies countermeasures (good practices) that could be implemented in projects countries. Thus, synergies have been created between the two projects on cybercrime, as well as with two other joint European Union and Council of Europe projects in Serbia, namely, the Criminal Asset Recovery (CAR) project and the MOLI-Serbia project against money laundering.

A wide spectrum of institutions involved in detecting, tracing, seizing and confiscating criminal money on the Internet from EAP countries were represented in the meeting from the following institutions:

- Financial intelligence units
- Asset recovery and/or financial investigation bodies
- High-tech crime units of the police, units dealing with economic crime and corruption
- Prosecution services

Experts from Ireland, Belgium, representatives of the private sector (VISA Inc. and PayPal) and the FATF shared their initiatives, programmes and experiences.

In order to update information on inter-agency and public-private cooperation a questionnaire was sent to the project working groups.

The main achievements of the intra-regional seminar are:

- Raised awareness of the need to confiscate proceeds from crime on the Internet.
- Strengthened interagency and public-private cooperation against criminal money on the Internet.
- The new FATF Recommendations were presented to take measures for their implementation.

[6] For more information about CyberCrime@IPA see: www.coe.int/cybercrime

- The (draft) Typology study on Criminal money flows on the Internet: Methods, trends and multi-stakeholder counteraction was presented and discussed and additional information was included in the draft study before its subsequent adoption by MONEYVAL[7]
- Participants identified solutions for overcoming the problems encountered in the prevention and control of criminal money flows on the Internet.
- Good practices were presented.
- Each delegation prepared a set of recommendations for measures to be taken in their respective country/area.

Under anti-money laundering regulations based on an all-crimes approach, all proceeds-generating types of cybercrime would be considered as predicate offences for money laundering, and all profits from these crimes taken out of or put into the "system" at any point would be considered as "dirty" money. Cybercrime is thus highly relevant for anti-money laundering and counter-terrorist financing efforts. A wide range of stakeholders should be involved in measures against such forms of crime – not only from the public sector but in particular from the private sector. Although there are examples of multi-stakeholder action, efforts remain rather fragmented. Initiatives against fraud on the Internet are not necessarily linked to activities carried out by financial intelligence units (FIUs) or law enforcement authorities responsible for financial investigations. This hinders effective measures against criminal money flows on the Internet.

The FATF Recommendations[8] set out a comprehensive and consistent framework of measures that countries should implement in order to combat money laundering and terrorist financing, as well as the financing of proliferation of weapons of mass destruction. In February 2012, the FATF recommendations and special recommendations were revised and consolidated into new 40 recommendations. A representative of the FATF Secretariat presented the new recommendations and explained their practical effect on the existing procedures and standards. An important development is that the new recommendations encourage the countries to implement, among other relevant international standards and conventions, the Budapest Convention on Cybercrime.

A better knowledge of methods used for fraud, money laundering and terrorist financing on the Internet through exchange of information between relevant public and private sector stakeholders will facilitate more effective financial investigations, seizure and confiscation of crime proceeds as well as prevention of fraud, money laundering and terrorist financing on the Internet.

Furthermore, the Council of Europe (Moneyval and Global Project on Cybercrime) has carried out a typology exercise on criminal money flows on the Internet. The Typology study was presented in the workshop as a response to the general need of law enforcement authorities to learn about trends, methodology and multi-stakeholder counter-action.

The Situation Report identifies in most instances the types of crime they are encountering on the Internet. These include: computer fraud, electronic banking and electronic transfer fraud, credit card fraud (including counterfeiting of cards), identity theft, as well as phishing type frauds.

The main problems identified as obstacles to prevention and control of criminal money flows on the Internet are:

[7]http://www.coe.int/t/DGHL/cooperation/economiccrime/cybercrime/Documents/Reports-Presentations/MONEYVAL_2012_6_Reptyp_flows_en.pdf

[8] http://www.fatf-gafi.org/dataoecd/49/29/49684543.pdf, International Standards on Combating Money Laundering and the Financing of Terrorism & Proliferation, FATF, February 2012.

- Technical inability to determine cash flows, especially when anonymous services are used and where data is held in countries where international legal assistance is needed.
- The speed of the transactions is not matched by the speed of the legal procedures needed to trace the transactions.
- Lack of equipment and trained staff.

The discussions in the workshop pointed out that:

- Effective mechanisms for confiscating proceeds of crime on the Internet are vital for an effective fight against cybercrime and other forms of serious and economic crime.
- Cooperation at all levels – interagency cooperation, public-private cooperation and information exchange, as well as regional and international cooperation is a prerequisite for an efficient confiscation. Predicate offences to money laundering (such as different types of fraud, offences related to child abuse material, counterfeit medicines, offences against intellectual property rights etc.) are committed through the Internet and different mechanisms are used for channelling criminal proceeds by using the Internet with the aim of disguising their origin and transforming them into cash.
- Involvement of different stakeholders is required to trace and seize criminal money on the Internet (AML system, anti-cybercrime institutions, financial sector, ISPs, institutions monitoring the Internet), and a number of possible countermeasures needs to be taken, including reporting on e-crime, raising public awareness, managing risks in the private sector, legal framework, specialised high-tech crime units etc.

The issues of public-private cooperation and intelligence exchange with financial sector institutions was also discussed (e.g. the High-Tech Crime Forum of the Irish Banking Federation, PayPal and VISA Inc.). Representatives of PayPal (introduction to Signal Spam) and VISA Inc. introduced their initiatives, guidelines in order to facilitate and enhance cooperation between law enforcement authorities and the public sector.

An in-depth explanation was presented by the Deputy Head of the Ukrainian FIU on the relevance of the Convention on Laundering, Search, Seizure and Confiscation of the proceeds from crime and on the Financing of Terrorism (CETS 198).

A complex case investigated by Belgian public prosecutor related to investigating international money laundering scheme through the Internet and a similar complex case of Ukrainian FIU were discussed.

Another presentation focused on the typology of most common varieties of cybercrime and related offences, such as compromising confidential data, unauthorised access to computer systems, ATM skimming, forged means of electronic payment and other. It was highlighted different factors that favoured proliferation of these types of crime. Examples from specific cases and investigation techniques (including interception of Internet and telephone communications) and steps undertaken in terms of financial investigations have been provided.

3.5.2 Situation in project countries and recommendations

Armenia

The following offences are identified as the main types of fraud and other offences on the Internet that involve crime proceeds:

- Embezzlement of bank cards details;
- Embezzlement of funds from accounts linked to these cards;
- Use of e-purses to cash money;
- Internet fraud, in particular, sexual services, sale of various goods and services, etc.

Low supervision, low levels of awareness and identification of users are considered the main problems that are encountered by those with responsibility for the prevention and control of criminal money flows on the Internet. In order to enhance the level of public awareness the General Prosecutors' Office with support of the Presidential Administration started to prepare and broadcast commercials. Information was published on the website of the General Prosecutors' Office.

The cooperation with commercial banks and e-payment systems are good since this sector has interest to cooperate with law enforcement authorities.

Financial investigations are the responsibility of the Police of Armenia, State Security Service of Armenia, State Proceeds Committee of Armenia, and General Prosecutor's Office of Armenia. These authorities are responsible for asset seizure and confiscation of proceeds of crimes committed on the Internet.

Recommendations made by the delegation

- In order to increase effectiveness of the fight against financial crimes committed on Internet and the cooperation between agencies and private sector to examine advanced practice of foreign countries and organize seminars for law enforcement agencies in the country.
- Organise public awareness campaigns to increase knowledge of society and private sector about new types of financial crimes and strengthen cooperation between them and LEA.
- Take appropriate measures to increase international cooperation with countries, which are not cooperating, in particular offshore countries.
- Prepare amendments on current legislation in order to enhance cooperation between LEAs and ISPs.

Azerbaijan

Different types of fraud ("419" fraud, credit card fraud, advance fee payment fraud) are frequent although money laundering through online gambling, e-payment services, e-gold are also identified as main methods for committing money laundering.

The following shortcomings are identified in their ability to effectively control and prevent these activities:

- insufficient staff;
- lack of trainings/training materials for law enforcement as well as contact points for public-private cooperation in ministries and financial service providers and ISPs.

- lack of inter-agency cooperation and written procedures to regulate information exchange.
- public – private cooperation:
  - opening commercial sites on the Internet is not clearly regulated;
  - no written procedures are available on information sharing and exchange;
  - unified databases maintained by stakeholders are not available;
  - awareness raising needs further improvement;

- proof of burden is on the LEAs.
- complexity of criminal money flows schemes.
- reporting networks are not or not well established and need further development.
- unified procedure for international cooperation is not available.

Recommendations made by the delegation

- To organise trainings for law enforcement authorities, public prosecutors and judges in order to ensure specialisation, overt and covert search and investigatory structures.
- To develop programs of joint training of employees of law enforcement bodies and representatives of a private sector.
- To organise direct physical access for law enforcement authorities to databases of financial service providers ensuring that privacy rights are not infringed.
- To develop national system of monitoring of suspicious transactions.
- To develop special software for the above mentioned purpose taking into consideration the safeguards and conditions. The development of the software should be prepared with the consent of all stakeholders.
- To unify national legislations in the field of AML/CFT with regard to the requirements of the international standards and procedures. It will create conditions for effective international cooperation in issues of rendering of mutual legal assistance.
- To use the already operating network of 24/7 contact points of the Budapest Convention of the Council of Europe or G8 High Tech Crime Subgroup.
- To create a permanent multi-agency working group including both public and private sector to enhance the efficiency in drafting amendments to improve national legislation.
- To establish a national coordination board or working group to improve inter-agency cooperation.
- To create the general database on crimes, criminals, methods and money-laundering schemes, black lists of accounts of physical persons and legal entities and other information for optimisation of work of participants of financial monitoring, the account, conducting statistics, research of tendencies.
- Establishment of a trusted forum for LEAs and also a public forum for users, clients in order to raise awareness.
- Develop government programmes for awareness raising, including opening hotlines (both in public and private institutions).
- Establish National Cybercrime Centre, which will assist not only on investigations of hi-tech crimes but criminal money flows on the Internet and would also serve as an analytical, research and methodological institution.

Belarus

The following are the main types of fraud and other offences on the Internet that involve crime proceeds:

- Embezzlement through the use of computer devices (including use of bank card details and forged cards).
- Advertising and distribution of child pornography.

Major issues identified are: the on-line nature of the crimes, no borders for criminals; borders and serious limitations related to bank secrecy for LEA; multi-turn schemes to transfer money through shell companies in off-shores, where the information virtually cannot be received; bank accounts in the name of front persons or non-existent persons; bank employees being either negligent or directly involved in criminal arrangements.

If a financial investigation is connected to a crime under investigation at "K" Department, then it investigates such financial crimes. If it is considered that the financial investigation is a separate law enforcement activity, the investigation authority in charge thereof in Belarus is the Financial Investigation Department of the State Controlling Committee of Belarus.

Where necessary, resources of the economic crime unit, organized crime and corruption unit of the Ministry of Interior can be used as well as resources of the Financial Investigation Department and Financial Monitoring Department of the State Controlling Committee of Belarus.

Competencies of the state authorities of Belarus as to investigation of crimes are described in Article 182 of the Criminal Procedural Code of Belarus[9].

Recommendations made by the delegation

- Consider creation of an online platform for complaints from users on small-scale fraudulent transactions and analysing such information.
- Enhance interagency cooperation between specialized anti-cybercrime bodies and the Department for Financial Monitoring of the Republic of Belarus.
- Continue the implementation of the FATF Recommendations in the national legislation.
- Further promote and expand private-public partnership initiatives, using, inter alia, the positive experience of interaction between the law enforcement and the VISA Regional Office. Such PPP initiatives should cover both national (cooperation between the National Bank and commercial banks) and international (electronic payments systems) levels.
- Learn best practices from Georgian experience of electronic processing of criminal cases on cybercrimes.
- Continue work on accession of the Republic of Belarus to international legal instruments on countering cybercrimes, in particular the Budapest Convention.

[9] http://www.pravo.by/WEBNPA/text.asp?RN=hk9900295#&Article=182

Georgia

The main types of fraud involving crime proceeds are credit card fraud, phishing; in addition, there are cases of legalisation of illegal income involving Internet.
The main obstacles for prevention are the lack of awareness, as well as insufficient training of professionals. In terms of control of criminal money flows on the Internet difficulty of identification of depositors (offender) and finding the true origin of money involved. For instance, a crime may involve opening an account as a fictitious person and then transferring particular sums of money to or from this account. In some cases it is complicated to provide adequate evidence of depositor's identity for the court.

The Investigation Service of the Ministry of Finance of Georgia was established in 2009 by Law on Investigative Service of the Ministry of Finance. It constitutes a special investigative body, which according to the legislation of Georgia is responsible for prevention, suppression and investigation of crimes committed within financial and economic spheres. According to the Article 8 of the Law, the investigative service is entitled to conduct investigative-operative activities, carry out investigations, obtain necessary information and carry out other activities provided by the legislation of Georgia.

The Financial Monitoring Service of Georgia is an administrative type of FIU. Its activity is regulated under the Law of Georgia on Facilitation the Prevention of Illicit Income Legalization (adopted on June 6, 2003) and the Regulation of Financial Monitoring Service of Georgia – Legal Entity of Public Law (approved under the Ordinance 859 of the President of Georgia on November 26, 2009).

Recommendations made by the delegation

- Improve international cooperation.
- Establish an inter-agency task force to improve cooperation among relevant government agencies.

The Republic of Moldova

The main problems encountered in the prevention and control of criminal money flows on the Internet, are the use of servers located outside the Republic of Republic of Moldova and the lack of cooperation with the financial institutions in the field. The institute responsible for financial investigations is the Centre for Combating Economic Crime and Corruption.

Further improvement is required in the field of inter-agency cooperation in order to effectively follow criminal money and to search, seize and confiscate proceeds from crime on the internet / on computer systems.

There are legislative problems with regard to obtain data from telecommunication companies, namely there has to be an open investigation to ensure information exchange. In the course of the preparation of the cybercrime legislation the private sector (including ISPs, TSPS, financial institutions) were invited to discuss the draft legislation. Cooperation is not only initiated by LEAs but also by the private sector.

Recommendations made by the delegation

- Amend CPC and AML legislation in order to:
  - launch investigations without the burden to prove the predicate offence
  - the offenders is under the burden of proof regarding proceedings
  - simplify the procedure to seize, confiscate property originating from criminal proceeds
- Expand the reporting list of the AML legislation to include obligatory reporting of (suspicious transactions, offences) ISPs, TSPs.
- Finalise and adopt the law on electronic payment services and electronic money.
- Awareness raising among the private sector on IT tools, methods, trends of criminal money flows on the Internet.
- Establishment the National Cybercrime Investigation Centre.

Ukraine

The following crime types have been identified: GSM network fraud, Internet-auction fraud, payment card fraud and the use of compromised bank account details or accounts in electronic payment systems. Social networks and social engineering are used often as well.

One of the most frequent fraud activities in the Ukrainian segment of the Internet is international financial fraud, (financial pyramids). Many commercial entities pretend to provide financial services (trust management of financial assets) or to carry out investment activities through web resources and e-payment systems; they offer people the opportunity to give their money to these companies, purportedly, in order to invest it in business projects with unrealistic (economically unfeasible) interest rates; usually accounts of such companies are held off-shore. The major problem is to overcome the anonymity of such companies on the web, i.e. to establish the link between these web resources and individual companies and thus to prove the fact of rendering a service that should be licensed under the law of Ukraine.

The problem in prevention and control over criminal money flows in the Internet is that e-payment system operation (in Ukraine) is not regulated, thus making it harder to trace monies of Ukrainian citizens deposited and withdrawn from fraudsters' accounts, as well as to control their further movements between accounts of companies participating in a criminal arrangement. Control and registration of money flows to off-shore jurisdictions and back into Ukraine (legalization) is yet at a low level due to the lack of an efficient mechanism of cooperation with international AML bodies and insufficient laws of Ukraine (which do not reflect the today's pace of IT development).

Recommendations made by the delegation

- Implement the revised FATF Recommendations.
- Send questionnaire to the participants of the seminar on problems hindering search, seizure and confiscation of digital assets.
- Strengthen international cooper.ation in search, seizure and confiscation of proceeds of cybercrime
- Create a website which would raise public awareness in cybercrime issues and would work as an Internet Crime Complaint Centre.

3.5.3 Follow up

- Filling the gaps of legal framework aimed at preventing criminal money flows on the Internet
- The project is to support and follow up on the recommendations made in the event with special regard to:
  - awareness raising programmes;
  - establishment of trusted fora;
  - development of e-crime reporting networks, hotlines;
  - support training needs of the project countries;
  - discuss LEA-ISP cooperation on regional seminars.

- Provide EAP countries with an Electronic Evidence Guide (to be developed under CyberCrime@IPA).
- Support a follow-up to the recommendations drafted in the workshop.

3.6 Activity: Regional seminar on specialised cybercrime units (Tbilisi, Georgia, 20-21 March 2012)

3.6.1 The seminar

Expected result 2 is related to specialised cybercrime units:

> EAP countries are provided with the tools for action against cybercrime – the project will support measures to strengthen specialised cybercrime units within the police, prosecution services as well as cyber forensic units.

Under the EU/COE Joint Project on Regional Co-operation in Criminal Justice: Strengthening capacities in the fight against cybercrime (CyberCrime@IPA) a good practice study[10] has been developed to help public authorities create or further strengthen specialised cybercrime units as a key element of the response to cybercrime. It is intended to complete this study with the experience of EAP countries based on the replies to a questionnaire sent to the working groups.

The Regional seminar on specialised cybercrime units (high-tech crime, cyberforensics and prosecution services) discussed the findings of the Cybercrime Situation Report, challenges faced in cybercrime investigations, as well as better coordination and cooperation between national authorities with responsibilities in fighting against cybercrime. Moreover, the seminar was a follow up on the recommendations made during the Regional seminar on international cooperation held in Chisinau, Moldova on 5-6 September 2011.

The main achievements of the regional seminar are:

- Provided advice and shared experience on the institutional set-up, responsibilities, authority of specialised cybercrime units within the police, prosecution services and cyber forensic laboratories.
- Reinforced inter-agency cooperation among national authorities (cybercrime units of police, prosecution services, state security services etc.).
- Updated the information on specialised cybercrime units.
- Provided advice and general overview on the Cybercrime Centres of Excellence initiative of the European Union since some of project countries intend to establish national centres of excellence.
- Followed up on the recommendations made during the Regional seminar on international cooperation (Chisinau, Moldova, 5-6 September 2011)[11].

From each project country, three participants were funded (ten participants from Georgia), representing:

- High-tech crime units (24/7 point of contact);
- Security services[12];
- Prosecution services;

[10] Available at: http://www.coe.int/t/DGHL/cooperation/economiccrime/cybercrime/Documents/Reports-Presentations/Octopus2011/2467_HTCU_study_V30_9Nov11.pdf

[11] Included in section 3.5.2

[12] According to the Situation Report security services of most of the project countries have responsibility to investigate cybercrimes

At the opening session the Deputy Head of the International Relations Department, Ministry of Justice of Georgia welcomed the participants and expressed the commitment of Georgia regarding the cooperation against cybercrime. Georgia has made serious progress in the cooperation against cybercrime through participating in international efforts. In this context, the importance and impact of the European Union – Council of Europe project on cybercrime in Georgia[13] was underlined. Georgia received considerable impetus from the results of that project and will continue to work on the steps forward especially to join the Budapest Convention.

The Head of the Council of Europe Office in Georgia welcomed the participants of the seminar and introduced the achievements of the CyberCrime@EAP project. She underpinned the relevance of the cooperation between the European Union and the Council of Europe in the field of actions against cybercrime and thanked the European Union for its commitment to support these efforts.

A number of experts from Belgium, "the Former Yugoslavian Republic of Macedonia", the Netherlands, Romania and United Kingdom shared their experience. The presentations made provided information on:

- Requirements for establishing specialised cybercrime units within the police, prosecution services and cyber forensic laboratories;
- Experience of establishment, functioning and challenges faced, including training strategy of the Romanian National Police;
- The current structure of the specialised cybercrime units of prosecution services in the Netherlands;
- Inter-agency cooperation in Belgium and challenges between different LEAs in the cooperation against cybercrime;
- Functioning (including training and basic technical requirements) of specialised cyber forensic laboratories;
- Experience of the Romanian cyber forensic laboratories;
- Introduction of the Cybercrime Centre of Excellence initiative (e.g. experience, functioning of 2Centre in Ireland (Research, Training and Education); experience of the establishment of the Belgian Cybercrime Centre of Excellence; challenges to establish the Romanian Cybercrime Centre of Excellence).

3.6.2 Situation in project countries and recommendations

Armenia

Specialised units within the State Security Service and the Police of Armenia perform investigations. For instance, there is a hi-tech unit within the Organized Crime Department of Armenia's police. Investigation units of relevant law enforcement agencies and the General Prosecutor's Office of Armenia undertake initial investigations.

The high tech crime unit is competent to investigate offences committed against computer systems such as hacking, attacks on the CNI, illegal interception and data interference. The unit is also competent to deal with offences involving technology such as computer related fraud, Internet crimes, offences involving the abuse of children, intellectual property offences as well as racism and xenophobia.

Specialised units deal with collection and processing of digital evidence; however they do not have laboratories of their own. Where an expert evaluation is necessary, it is performed at specialised

[13] http://www.coe.int/t/dghl/cooperation/economiccrime/cybercrime/cy_project_in_georgia/projectcyber_en.asp

centres, in particular the National Bureau of Expert Evaluation that is a State non-commercial centre of Armenia's Academy of Sciences.

The main challenges encountered by the high tech crime unit fall into two categories:

- External factors: the main challenges are to be able to receive information from certain servers outside Armenia and to interact with 24/7 contact points of some countries.

- Internal factors: the main challenges are caused by contradictions in Armenian law. For instance, the Law on Investigation Activities establishes that users' data, details and log files of electronic communication can be requested only through a court order regarding grave or especially grave crimes; however, some computer crimes belong to the category of medium and low gravity according to the Criminal Code of Armenia.

Recommendations made by the delegation

- Organise trainings for law enforcement officials, prosecutors and judges.
- Increase the staff and capabilities of cyber forensics of the National Bureau of Forensic Laboratories with trainings on technical materials, electronic evidence.
- Establishment of specialised prosecution service for prosecutorial supervision of cybercrime cases.
- Establish a centre for automated monitoring of illegal content on the Internet.
- Development and adoption of a law on cooperation between LEA-ISP/TSP.
- Further improve awareness raising with involvement of the private sector and society in organisation of TV spots as well as other fora.

Azerbaijan

In Azerbaijan the Ministry of National Security has a dedicated cybercrime unit. A dedicated unit to fight cybercrime will be established in the Ministry of Interior and probably within the Special State Protection Service. Investigative competencies are to be distributed between several authorities basing on the importance of the criminal objects and the level of social danger they present.

The Cybercrime unit of the Ministry of National Security has the powers to investigate any crimes related to modern technology, such as computer-related fraud, crimes on the Internet, child abuse, and racism. Mainly, the activities aim at fighting child pornography, signs of terrorism in the Internet, embezzlement and fraud related to use of IT and Internet. There are no accurate statistics on the matter.

Cooperation with foreign specialised units in investigation of computer-related crimes is carried out largely in the form of direct requests and reciprocal exchange of information. Three cases were successfully investigated this way in the last year.

Obtaining operative field data is hard due to specific features of such crimes. To date, the most efficient method to timely obtain operative data is interception and semantic analysis of Internet traffic. However, encoding the traffic done by applications such as GTalk and Skype hinders this work. On the other hand, there is no targeted and continuous awareness raising effort that would help to obtain information on offences from the population.

There are no dedicated units in the law enforcement system that deals with child pornography carried out through Internet and IT technologies. There is insufficient experience in the investigation of cases related to IT and telecommunications, or enough professionals in the field of digital forensics, interpretation of technical traces, analysis of log-files, analysis of intercepted web and mail traffic. There are unresolved issues related to technical equipment for digital forensics and correct seizure of data stored at electronic media. More attention should be paid to legal training in the field and investigative officers, with targeted specialisation of professionals.

Recommendations made by the delegation

- Adopt the amendments to the Criminal Code.
- Draft amendments to the Criminal Procedure Code in order to stipulate regulations on search, seizure of electronic evidence, stored computer data. Adjudicating cybercrime would gather impetus since this amendment would facilitate admissibility and use of electronic evidence in court as direct and indirect evidence.
- Draft a law on cybercrime including provisions on ISPs to maintain the availability of data for at least 2 years.
- Develop regulation for licensing providers to adopt technical specifications of the Ministry of National Security.
- Organise specialised trainings, as well as joint trainings for law enforcement officials, prosecutors and judges in a manner that facilitates that every stakeholder learns the challenges of investigating cybercrimes.
- Develop direct access to a unified LEA database.
- Establish national monitoring system in the field of criminal money flows on the Internet and money laundering, as well as develop a specialised software on automated monitoring systems.
- Establish a multi-agency national working group (including both public (ministries) and private sector) in order to improve legal standards for cooperation.
- Develop a national database including information on cybercrime methods, schemes, blacklist of IP addresses, phishing sites etc. to optimise the efficiency of law enforcement authorities.
- Create a trusted as well as an open fora for the inter-agency cooperation and for public-private cooperation.
- Raise awareness by establishing and developing national programmes in cooperation with the private sector; open hotlines for both awareness raising and e-crime reporting.
- Design specialised government programmes for strengthening capacities against cybercrime.
- Establish a National Cybercrime Centre of Excellence for cyber forensic work, analysis, research, training and education (for both LEA officials and representatives of the private sector). Establish a specialised cyber forensic laboratory within the centre.

Belarus

Since 2002, there is a separate unit to counter hi-tech crime within the Ministry of Interior of Belarus ("K" Department) whose competency is to detect and deal with crimes against information security, embezzlement by means of computers, including that conducted by means of stolen and forged bank cards or their details, and to counter distribution and advertising of child pornography in the Internet.

There is also a specialised unit within the investigation body of the Ministry of Interior that is a hi-tech and intellectual property unit; its function is to initiate criminal proceedings and conduct initial investigation of detected criminal activity.

Since 2000, there is a designated independent IT security unit (ITSU) within the State Security Committee of Belarus whose competency includes investigation of cybercrime, where state information resources and systems are the object of criminal infringement, and where national security is affected. ITSU holds all necessary investigation powers to detect and register illegal acts; when there are sufficient data, the case is transferred to the investigative unit of the Security Committee to open a criminal case (there are officers in the Committee specialising in this type of crime).

The division of functions between the specialised units of the Ministry of Interior and the State Security Committee, with regard of the general investigative competence towards the relevant articles of the Criminal Code of Belarus (articles 349-355), is established by inter-agency regulations.

The Prosecution office has no specialised units or prosecutors designated for dealing with cybercrime cases. A specialised unit of the State Security Committee of Belarus investigates attacks on critical state infrastructure.

Where it is necessary to obtain evidence for criminal cases under investigation, the hi-tech and intellectual property crime unit of the Ministry of Interior sends an investigation request through the Belarus General Prosecutor’s Office to law enforcement agencies of foreign countries on the basis of mutual assistance.

Major difficulties faced by the hi-tech crime units of the Ministry of Interior of Belarus are caused by the absence of a comprehensive legal framework that is compatible with the majority of European countries, the United States and other countries on international cooperation related to computer crimes. Belarus is not yet a Party to the Budapest Convention on Cybercrime, which makes it impossible to obtain information important for the investigation and make use of the provisions of this Convention.

Recommendations made by the delegation

- Consider the establishment of a National Cybercrime Centre of Excellence in order to deliver trainings for law enforcement official, prosecutors and judges as well as cyber forensic experts.
- Establish a specialised prosecution unit within the General Prosecutors’ Office.
- Develop a national cybercrime strategy including the protection of critical infrastructure.
- Criminalisation of not guaranteeing access to encrypted files and systems.
- Establish a multi-agency task force to discuss and resolve practical challenges against cybercrime.
- Continue the work to accede to the Budapest Convention.

Georgia

In June 2011, an amendment was introduced to the regulations of the Criminal Police Department of the Ministry of Internal Affairs of Georgia (MIA). According to this amendment, the 3rd Division of the Criminal Police Department (Division) will be responsible for investigation of high tech crime. Within the same Division, there will be established 24/7 contact point for international cooperation against cybercrime.

The division is competent to investigate cybercrime offences in narrow sense, in particular crimes provided for in Chapter XXXV (Cybercrime) of the Criminal Code of Georgia.

Separation of investigative jurisdiction in Georgia is regulated under the Decree 178 of the Minister of Justice of Georgia. The document underlines that the competence in general is vested in the investigative agencies of the Ministry of Internal Affairs of Georgia, except for the cases/crimes specifically listed in the Decree to be under competence of other agencies, among them Investigative Division of the Ministry of Finance of Georgia. The separation in this case is based on the type of crime.

Currently, there are three detective-investigators within the Division who are responsible for investigation of cybercrime. However, the number of staff members working on cybercrime issues will increase upon creation of High Tech Crime Unit.

The main difficulties encountered by the Division are lack of experience in investigation of cyber cases and weak international cooperation in this field as well as lack of relevant equipment.

Recommendations made by the delegation

- Adopt the currently discussed Law on Information Security as a major tool for cybercrime prevention through "target hardening" and as a platform for extended national critical infrastructure/CERT/law enforcement cooperation.
- Review national case law on cybercrime to ensure that admissibility and use of digital evidence develops along the general lines of currently applicable rules of evidence, and to propose/implement changes in case the current regulations prove insufficient.
- Ensure that offences that involve technology (computer related fraud, Internet crimes, offences involving abuse of children, intellectual property offences and others) are also analysed and accounted in the overall cybercrime context.
- Continue dialogue with the National Security Council with a view to coordinate and implement cybercrime-related parts of the National Cyber Security Strategy and its Action Plan.
- Continue efforts and seek assistance in creating a Centre for Cyber Security Research and Training, with a view to develop it further into a regional institution.
- Continue efforts to develop capacities in setting and strengthening existing expert forensic capabilities at the Ministries of Internal Affairs (IT) and Justice (CERT).

The Republic of Moldova

The Parliament's Decision No.77 dated 04.05.2010 on approval of the structure of the General Prosecutor's Office, as well as by the Order of the General Prosecutor No.364-p dated 24.05.2010 on internal organization of the General Prosecutor's Office, stipulate the creation of an Information Technology and Cyber Crime Investigation Section as an independent structural subdivision of the General Prosecutor's Office in direct subordination of the General Prosecutor.

There is also a Cyber Crime Combating Section within the Fraud Investigation Directorate of the Police Department of the Ministry of Internal Affairs.

A cyber lab has been created within the Technical Criminalist Directorate of the Ministry of Internal Affairs, where technical specialists work on information data analyse, collect, process etc. information data in compliance with the provisions of the Criminal Code, Criminal Procedure Code, developed methodological materials, etc.

The following has been identified as the main difficulties encountered by the high tech crime unit:

- Insufficient training of law enforcement officers involved in combating cybercrime;
- Lack of training in specific information technology areas;
- Insufficient hardware and software in cybercrime investigation;
- Hard cooperation with the competent bodies of other states;
- Innovative nature of cybercrimes in criminal prosecution and court practice;
- Gaps in the criminal procedure legislation on regulations referring to investigation of cybercrimes;
- Formalism in case of international rogatory commissions;
- Deficit of specialists and experts in information technologies;
- Lack of expert in specific information technologies.

Recommendations made by the delegation

- Involve the Academy to develop training programmes for law enforcement authorities.
- Develop strategy against cybercrime.
- Increase the staff by appointing special investigators.
- Develop an MoU with ISPs.
- Develop a methodology for investigating cybercrimes.
- Train cyber forensic experts to conclude examination for cybercrime cases.

Ukraine

There are dedicated units to fight hi-tech crime within the Ministry of Interior of Ukraine (Cybercrime and Human Trafficking Department) and the state Security Service of Ukraine (Information Security Department). These units' functions are to detect and clear such crimes; a pre-trial investigation unit performs their investigation. There are no specialised investigative units for cybercrime within the prosecution.

Functions are distributed between the units of the Ministry of Interior and the Security Service of Ukraine on the basis of investigative competence re a relevant crime as established by Article 112 of the Criminal Procedural Code of Ukraine. In many cases, investigative competence on such crimes can vary. Besides, distribution of functions is linked to the area of responsibility of the police and state security agency. For the Ministry of Interior, the key focus is to protect rights of people, companies, institutions, organizations, interests of the state and the society from unlawful infringement. For the Security service the focus is to protect the state, its constitutional order, state security, as well as to conduct counter intelligence activities. Ministry of Interior's competencies cover investigation of cybercrime established by Criminal Code of Ukraine.

Staff of the Cybercrime and Human Trafficking unit of the Ministry of Interior has powers to detect, clear, register, and stop offences against computer systems. Investigators of the law enforcement agencies hold criminal proceedings on such cases. The Security Service investigate crimes (e.g. Illegal use of technical means for covert capture of information). Competencies of the Security Service of Ukraine also include investigation of crimes committed by means of computers and telecom channels.

The main difficulties identified as being encountered by the High Tech Crime Unit in performing its assigned tasks are:

- Lack of technological means;
- The need to develop multimedia distant learning courses to upgrade qualification of the staff.

Recommendations made by the delegation

- Provide practical and technical advice regarding 24/7 points of contact in the field of international cooperation.
- Sustain and further develop Cybercrime Centres of Excellence;
- Develop specialised software and other products to assist the efforts against cybercrime. These products should be free for law enforcement agencies.
- Create a list of existing software and other relevant programs.
- Establish a platform to share the experience among project countries.
- Develop tailor-made projects by international organisations to develop specialised software for law enforcement agencies.
- Standardisation of international requests.
- Improve national legislation in order that information gained through international cooperation could serve as evidence when prosecuting, adjudicating crimes.
- Establish a protected database (electronic signature keys, IP addresses etc.
- Automated analysis of information by different stakeholders in order to further enhance inter-agency cooperation.
- Develop online training materials in a trusted fora.
- Determine the approximate timing for international cooperation with regard to requests.

3.6.3 Follow up

- Include the experience of Eastern Partnership countries in the Good practice study on specialised cybercrime units;
- Advise project countries to establish/strengthen specialised cybercrime units within the law enforcement agencies (police, prosecution service);
- Advise project countries to establish or further develop cyber forensic laboratories or cyber forensic experts;
- Support project countries in their efforts to provide sustainable training for law enforcement and judicial training
- Support a follow-up to the recommendations drafted in the workshop.

3.7 Activity: Expert opinion provided on National Centre of Cybercrime Investigation of the Republic of Moldova

The Prosecutor General of Republic of Moldova requested the Council of Europe for an opinion on the law establishing the National Centre of Cybercrime Investigations in the Republic of Moldova. Therefore, an expert opinion was conducted under the CyberCrime@EAP project, which provided an assessment of the position, powers and responsibilities of this Centre in view of compliance with international standards, including Article 15 (Conditions and Safeguards) of the Convention on Cybercrime.

The Expert Opinion was submitted to the General Prosecutors' Office on 6 December 2011.

Many inconsistencies of the draft Law on the Approval of the Regulations of the National Centre of Cybercrime Investigations have been identified in the Expert Opinion.

In Article 8 of the Draft Law there is only a very general list of powers of the Centre and no grounds and conditions are given for their application. Only a general reference is made ("according to the legislation"). Measures that can be applied on the basis of the Law No. 20-XVI from February 3, 2009 on Preventing and Combating of Cybercrime (and which basically follow articles 16 – 21 of the Convention on Cybercrime) are not listed in the Draft Law. There is only a general provision of Article 1 of the Draft Law, authorising the Centre to exercise tasks in accordance to the mentioned Law.

The Centre will have almost unlimited powers, which differs significantly from the modern drafting methods, which are clearly and precisely describing the law-enforcement powers, grounds and conditions for their application, limitation of the scope and the duration of such powers.

Future National Centre of Cybercrime Investigations of the Republic Moldova is intended to be a law-enforcement body. Worldwide, law-enforcement bodies are usually part of the executive branch of power. The Centre of Cybercrime Investigations is neither part of the executive branch of power nor it is completely independent. Moreover, on the basis of some elements it is possible to speculate that the intention of the drafters was to include the Centre into the legislative branch of power.

Parliament has extensive powers in relation to the Centre (which, in a certain way makes the Centre part of the legislative branch) but those powers are far from being sufficient to ensure proper monitoring in the area where there should be a real and strong monitoring – in the area of Centre's (almost) unlimited powers.

Having a typical executive body with extremely strong law-enforcement powers in the legislative branch of power without legal provisions on its real liability might cause serious negative consequences in the areas of protection of human rights, separation of powers and functioning of basic elements of a democratic society.

The exert opinion strongly suggested that Moldovan authorities undertake another effort and produce a new draft law on the future National Centre of Cybercrime Investigations, while taking into account observations made and fully respecting Article 15 of the Council of Europe Convention on Cybercrime, Council of Europe Convention for the Protection of Human Rights and Fundamental Freedoms and Article 6 of the Constitution of the Republic of Moldova on the "separation and cooperation of powers".

3.8 Activity: Documents made available in project countries languages

The following documents, which are relevant for the implementation of the project, were translated into project countries languages:

- Guidelines for the cooperation between law enforcement and internet service providers[14] was made available in Azerbaijani
- Functioning of 24/7 points of contact for cybercrime in Russian.

The Law on International Cooperation in Criminal Matters of Georgia was translated into English for the purpose of the analysis made in the Situation Report (Part I).

[14] http://www.coe.int/t/dghl/cooperation/economiccrime/cybercrime/Documents/LEA_ISP/default_en.asp

3.9 Activity: Support participation in different events

Under Result 3, Eastern Partnership countries were supported to participate in the following international activities against cybercrime:

- Annual Octopus Conference and the Cybercrime Convention Committee (T-CY) Plenary meeting (21-24 November 2011 Strasbourg, France). The Octopus Conference gathered experts representing countries from all continents, international organisations and the private sector to review the global cybercrime situation, to share experience on effective responses and to enhance cooperation against cybercrime at all levels.

- G8 High-Tech Crime Sub-Group training events for 24/7 points of contact (participation of one representative from each country) (8-11 November 2011, Rome, Italy), which provided the opportunity for the points of contact from project countries to establish links among themselves as well as to network with the countries that are members in the G8 network.

- OSCE National Expert Conference: Tackling Cybercrime – A Key Challenge To Comprehensive Cybersecurity (6-7 October, Baku, Azerbaijan). The joint EU/COE Cybercrime@EAP project was presented in the Conference.

4 Visibility

High visibility of the CyberCrime@EAP project and the European Union involvement was ensured at all levels, including in the United Nations and OSCE meetings where the Council of Europe presents this project as an example of cooperation.

The visibility of the project and the EU contribution is ensured by:

- Producing and distributing different materials, such as the brochures, folders and short description (leaflet) containing all relevant information, as well as promotional items.
- Using the EU and the project logo on all documents or items related to the project, such as programmes of meetings or conferences, lists of participants, project reports, letters, other written documents as well as on any promotional material.
- The publication of press releases for all major project events.
- Informing EU Delegation representatives to project countries about all project meetings and events in their respective country. A regular communication with the EU Delegations is sought by informing EU delegation representatives about all upcoming project activities and events in their respective countries.

Information on the project activities were disseminated through the webpage, which was regularly updated and contains all information and documents of relevance to the project:

http://www.coe.int/t/DGHL/cooperation/economiccrime/cybercrime/cy_Project_EaP/Default_EaP_en.asp

Several events organised under the Project, in particular the event on international cooperation in Chisinau with the Prosecutor General of Moldova benefited from wide media coverage, which contributed to the acknowledgment of the financial contribution made by the European Union to this Project.

Representatives of European Union Delegations were invited in all events and opened the events organised in Chisinau and Baku.

5 Conclusions

Following the inception phase, the CyberCrime@EAP project made considerable progress towards achieving its objectives between June 2011 and March 2012. The project already is producing results in terms of strengthening legislation and institutional capacity to investigate and prosecute cybercrime in project countries.

Good practices were shared, strategies and practical tools have been presented, four regional events (including one joint, intra-regional EAP region – IPA region) were organised. The participation of representatives of project countries in international meetings was ensured and the project itself is presenting in different fora as an example of good practice. Increasing cooperation against cybercrime at regional and international level and develop a culture of cooperation between law enforcement and private sector have been taken up in several activities organised under the project.

Important international instruments promoted by the project were considered by EAP countries e.g. Ukraine ratified the Second Additional Protocol to the European Convention on Mutual Assistance in Criminal Matters (CETS No. 182) on 14 September 2011. Moldova ratified the Convention on the Protection of Children against Sexual Exploitation and Sexual Abuse (CETS 201) on 12 March 2012 and signed on 13 March 2012 the second Additional Protocol to the MLA Convention (CETS 182).

Based on the shortcomings identified and good practices available important recommendations have been made under the project. Among them:

- Improve the capacity to keep such statistics. It would be in line with the spirit of the CyberCrime@EAP Project to coordinate such an activity and to decide what information will have to be collected, how and where it will be stored and how it will be made available;
- Support – where no dedicated units exist – to consider the benefits of creating such units based on the guidance provided by the Good Practices on Specialised Cybercrime Units, developed under CyberCrime@IPA. (e.g. Armenia is in the process of establishing such a unit);
- The development at country and regional level of a law enforcement cybercrime training strategy incorporating the requirements of cybercrime investigators, digital forensics examiners and mainstream law enforcement staff relating to their role specific functions;
- Develop a cybercrime training strategy for judges and prosecutors. The concept paper on cybercrime training for judges and prosecutors prepared by the Council of Europe[15] and the Lisbon Network can be used for guidance.
- Improve capability at regional and country level to combat illegal money flows on the Internet by adoption of the relevant findings of the Council of Europe project "Criminal money flows on the Internet: methods, trends and multi-stakeholder counteraction". The development of solutions should involve the relevant public sector, law enforcement departments and industry players.
- Develop a framework for improved cooperation between law enforcement and Internet Service Providers using as a model, the "Guidelines for Cooperation between Law Enforcement and Internet Service Providers against Cybercrime" developed by the Council of Europe under its Project on Cybercrime.
- Involve EAP countries in the drafting of the Electronic Evidence Guide to be developed under EU/COE CyberCrime@IPA project.

[15] http://www.coe.int/t/dghl/cooperation/economiccrime/cybercrime/Documents/Training/2079_train_concept_4_provisional_8oct09.pdf

The approach of working at all levels and involving all institutions responsible proved extremely valuable. Thus CyberCrime@EAP enjoys much support and interest not only at the level of practitioners but also at the level of decision-makers.

The achievements so far of the project show that it advanced under each of the expected results. A broad process is now underway, and this can be considered the main strategic achievement at this point. This will bring project countries closer to European Union and Council of Europe standards and practices.

The project created synergies with other relevant projects, initiatives and organisations (such as the Council of Europe Global Project on Cybercrime[16], the CyberCrime@IPA Project on Cooperation against Cybercrime under the Joint project of the European Union and the Council of Europe[17], EUCTF, OSCE etc.).

The project places great emphasis on sustainability and strategic and lasting approaches. In each activity participants are required to prepare recommendations to be implemented in their respective countries. The implementation of the activities and the evolution of the project show that recommendations made are being implemented.

[16] See www.coe.int/cybercrime

[17] See http://www.coe.int/t/dghl/cooperation/economiccrime/cybercrime/cy%20project%20balkan/Default_IPA_en.asp

Name of the contact person for the Action: Alexander Seger

Signature: ………………………………………

Location: Strasbourg

Date report due: 30 April 2012

Date report sent: …25 April 2012

6 Appendices

6.1 Logical framework and workplan

	Intervention logic	*Details*	*Timeline*
Overall objective	**The overall objective of the Council of Europe Facility is to enhance the reform processes in the six partner countries through a multilateral approach and to bring them closer to Council of Europe and EU standards in core areas covered by the Eastern Partnership Platform 1**		
Specific objective	**The specific objective of the present project is to strengthen the capacities of criminal justice authorities of Eastern Partnership countries to cooperate effectively against cybercrime in line with European and international instruments and practices**	***Indicators:*** - The standards and practices of Eastern Partnership countries are more in line with international standards, including in particular the Budapest Convention on Cybercrime - Document (declaration or similar) on regional and domestic priorities regarding cybercrime adopted by Eastern Partnership countries - Assessment reports adopted for each Eastern Partnership country	
Inception phase & horizontal activities		- Establishment of working groups comprising representatives of the relevant institutions responsible for the implementation of the project - Collecting information about the implementation of the provisions of the Convention on Cybercrime and related international standards - Elaboration and adoption of the workplan - 1st Steering Committee meeting (combined with Regional conference – Activity 1.1)	April-May 2011 March-Sep 2011 31 May 2011 Tallinn, Estonia, 30-31 May 2011
		- Assessment of the legislation in project countries regarding its compliance with the Convention on Cybercrime and related international standards	15 June – 20 September 2011

	Intervention logic	*Details*	*Timeline*
		- Drafting and sending to the working groups a questionnaire to obtain baseline information with respect to cybercrime situation in project countries - Drafting a situation report based on the information received through the questionnaire - 2nd Steering Committee meeting (combined with Regional conference – Activity 1.2) - 3rd Steering Committee meeting (combined with Regional conference – Activity 1.3)	May- 6 June 2011 15 July -31 Oct 2011 Tbilisi, Georgia June 2012 Kyiv, Ukraine July 2013
Result 1	**Eastern Partnership countries have defined strategic priorities regarding cybercrime and assessed measures taken**	***Indicators:*** - Participation of senior representatives in regional meetings - Document (declaration or similar) on regional and domestic priorities regarding cybercrime adopted by month 16 - Assessment reports on the effectiveness of measures and subsequent recommendations adopted by month 30	
Activities		*Details:*	
1.1	Regional conference (launching event of the project) on effective measures against cybercrime	- A 2-day regional conference for representatives of the key institutions involved in the project (ministries of justice and interior, prosecutor's offices, bodies responsible for cybersecurity) to discuss cybercrime measures and priorities and themes to covered by the project	Tallinn, Estonia 30-31 May 2011
1.2	Regional conference on strategic priorities regarding cybercrime	- A 2.5-day regional conference for policy- and decision-makers (combined with Regional seminar – Activity 2.2) to define strategic priorities regarding cybercrime and adopt a relevant document (declaration or other)	Tbilisi, Georgia June 2012
1.3	Regional conference on the assessment of progress made (closing event of the project)	- A 2.5-day regional conference for representatives of all relevant institutions to review the measures taken and progress achieved by the Eastern Partnership countries and adopt an assessment report (outcome of Peer-to-peer assessments – Activity 2.7)	Kyiv, Ukraine July 2013

	Intervention logic	*Details*	*Timeline*
Result 2	**Eastern Partnership countries are provided with the tools for action against cybercrime**	***Indicators:*** - 6 regional seminars on specific tools against cybercrime carried out by month 16 - Recommendations adopted regarding steps to be taken in each country by month 28 - Country-specific advice provided and progress assessed by month 29	
Activities 2.1	Regional seminar on cybercrime legislation	*Details:* - A 2.5-day regional seminar for representatives of ministries of justice, prosecution and judiciary to discuss areas where national legislation needs to be strengthened and harmonised between countries with respect to cybercrime, discuss challenges in implementing the Budapest Convention (including on the basis of prosecution practice/case-law/criminal statistics) and define country-specific needs to be addressed by the project. - Legal opinion on draft amendments to the Criminal Code of Republic of Azerbaijan provided	Baku, Azerbaijan 13 -14 December 2011 May, 2011
2.2	Regional seminar on specialised cybercrime units (high-tech crime, cyberforensics, prosecution services)	- A 2.5-day regional seminar (combined with Regional conference – Activity 1.2) for representatives of ministries of interior/police and prosecution services to assess the situation with respect to specialised cybercrime crime units (status, set-up, staffing, availability of skills and resources) and provide advice on strengthening these.	Tbilisi, Georgia 20-21 March 2012
2.3	Regional seminar on judicial and law enforcement training	- A 2.5-day regional seminar for representatives of training institutions for judges, prosecutors and LEA to evaluate the training on cybercrime available, identify needs, formulate training strategies and guidelines for sustainable, scalable and harmonised training.	-Tbilisi, Georgia 25-29 June 2012

	Intervention logic	***Details***	***Timeline***
2.4	Regional seminar on law enforcement – ISP cooperation	- A 2.5-day regional seminar for LEA, prosecutors (specialised in cybercrime) and ISP/private sector representatives on information exchange, contact points/fora for trusted cooperation and cooperation procedures.	Yerevan, Armenia 25-27 April 2012
2.5	Regional seminar on international cooperation against cybercrime	- A 2.5-day regional seminar representatives of ministries of justice, interior/police (specialised in cybercrime), prosecution and 24/7 points of contact on various aspects on international cooperation against cybercrime (24/7 points of contact, police and judicial cooperation, mutual legal assistance and other measures under the Budapest Convention), difficulties encountered and sustainable solutions for improving it.	Chisinau, Moldova 5-6 September 2011
2.6	Regional seminar on financial investigations	- A 2.5-day regional seminar for representatives of FIUs, asset recovery and financial investigation bodies, police and prosecution dealing with high-tech and economic crime and corruption, financial and supervisory authorities, banks and ISPs to raise awareness to confiscate proceeds from crime on the internet, strengthen interagency and public-private cooperation in this area and identify countermeasures and good practices.	Kyiv, Ukraine 27-29 February 2012
2.7	Peer-to-peer assessment and advisory visits to each Eastern Partnership country	- 6 peer-to-peer in-country visits by mixed teams of experts from project countries and other CoE member states to assess the effectiveness of measures undertaken (in terms of legislation, specialised high-tech crime units, LEA and judicial training, international and public-private cooperation, financial investigations) and formulate recommendations for the policy makers.	All countries November 2012 – April 2013
Result 3	**Eastern Partnership countries participate more actively in international**	***Indicators:*** - Level of participation of Eastern Partnership countries in international	

	Intervention logic	***Details***	***Timeline***
	cybercrime efforts	activities on cybercrime	
Activities 3.1	Support the participation of Eastern Partnership countries in international activities against cybercrime (Octopus conferences, G8 training events for 24/7 points of contact, Internet Governance Forum and others)	*Details:* - Participation in various international events and activities against cybercrime, for example: • Annual Octopus Conference (one/two representative/s from each country) and the Cybercrime Convention Committee (T-CY) Plenary meeting • G8 High-Tech Crime Sub-Group training events for 24/7 points of contact (participation of one representative from each country) • OSCE National Expert Conference: Tackling Cybercrime – A Key Challenge To Comprehensive Cybersecurity • Annual Octopus Conference and the Cybercrime Convention Committee (T-CY) Plenary meeting (one/two representative/s from each country)	Strasbourg, France 21-24 November 2011 Rome, Italy 8-11 November 2011 6-7 October, Baku, Azerbaijan) Strasbourg, France 4-8 June 2012

6.2 Calendar of activities

Date	Place	Activity	Status	Related result #	Activity #
April-May 2011	Strasbourg	Establishment of the working groups comprising representatives of the relevant institutions responsible with the implementation of the project	completed	All results	All activities
March-Sep 2011	Strasbourg	Collecting information about the implementation of the provisions of the Convention on Cybercrime and related international standards in EAP countries/legislative country profiles	completed	Result 2	All activities
30-31 May 2011	Tallinn, Estonia	Project Launching Conference on effective measures against cybercrime	completed	Result 1	Activity 1.1
		1st Project Steering Committee meeting	completed	All results	All activities
15 June-31 Oct 2011	Strasbourg	Assessment of the legislation from project countries regarding their compliance with the Budapest Convention and related international standards	completed	Result 2	All activities
May-6 June 2011	Strasbourg	Drafting and sending to the working groups a questionnaire to obtain baseline information with respect to cybercrime situation in project countries	completed	All results	All activities
May 2011 – Oct 2012	Strasbourg and EAP countries	Providing country-specific advice on the different topics covered by the regional seminars (legal opinions, desk studies, reports, etc.)	planned	Result 2	All activities
		- May 2011: Provide legal advice on draft amendments to the Criminal Code of Republic of Azerbaijan	completed	Result 2	Activity 2.1
		- Provide advice to project countries on the institutional set up, responsibilities and authority of 24/7 points contact (in line with article 35 of the Budapest Convention on Cybercrime) and on the set up high-tech crime units	planned	Result 2	Activity 2.5
		- Translation of the Guidelines for the cooperation between law enforcement and internet service providers adopted in Strasbourg in 2008 into Azeri (translations into Russian, Ukrainian, Georgian,	completed	Result 2	Activity 2.4

Date	Place	Activity	Status	Related result #	Activity #
		Armenian and Romanian languages are available) - December 2011: Expert opinion provided on the National Investigation Centre of Cybercrime of the Republic of Moldova	completed		
15 July – 31 Oct 2011	Strasbourg	Drafting a situation report based on information collected through the questionnaire	complete	All results	All activities
5-6 Sep 2011	Chisinau, Moldova	Regional seminar on international cooperation against cybercrime	completed	Result 2	Activity 2.5
6-7 Oct 2011	Baku, Azerbaijan	Participation in the OSCE National Expert Conference: Tackling Cybercrime – A Key Challenge To Comprehensive Cybersecurity	completed	Result 3	Activity 2.1 Activity 2.4
8-11 Nov 2011	Rome, Italy	G8 High-Tech Crime Sub-Group training event for 24/7 points of contact	completed	Result 3	Activity 3.1
21-23 Nov 2011	Strasbourg, France	Participation in the Octopus Conference	completed	Result 3	All activities
		Organise a regional and international training meetings for 24/7 points of contact and high-tech crime units with regard to international law enforcement cooperation and information exchange	completed	Result 2	Activity 2.2 Activity 2.5
				Result 2	Activity 2.2 Activity 2.5
13-14 Dec 2011	Baku, Azerbaijan	Regional seminar on cybercrime legislation	completed	Result 2	Activity 2.1
December 2011	Strasbourg, France	Expert opinion provided on the National Investigation Centre of Cybercrime of the Republic of Moldova			
27-29 Feb 2012	Kyiv, Ukraine	Regional seminar on financial investigations	completed	Result 2	Activity 2.6
20-21 March 2012	Tbilisi, Georgia	Regional seminar on specialised cybercrime units	completed	Result 2	Activity 2.3
25 -27 April 2012	Yerevan, Armenia	Regional seminar on law enforcement – ISP cooperation	underway	Result 2	Activity 2.4

Date	Place	Activity	Status	Related result #	Activity #
4-8 June 2012	Strasbourg, France	Participation in the Annual Octopus Conference and the Cybercrime Convention Committee (T-CY) Plenary meeting (one/two representative/s from each country)	planned	Result 3	Activity 3.1
		International workshop on transborder access to data	planned	Result 3	Activity 2.3
		International workshop on public-private information sharing	planned	Result 2	Activity 2.4 – 2.6
25- 29 June 2012	Tbilisi, Georgia	Regional conference on strategic priorities regarding cybercrime	planned	Result 1	Activity 1.2
		Regional seminar on judicial and law enforcement training	planned	Result 2	Activity 2.2
		2nd Project Steering Committee meeting	planned	All results	All activities
November 2012 – April 2013	All EAP countries	Peer-to-peer assessment and advisory visits	planned	Result 2	Activity 2.7
4-5 September 2012[18]	Skopje, "The Former Yugoslav Republic of Macedonia''	Workshop on electronic evidence (legal and practical aspects) for institutions of the criminal justice chain (investigators, forensic experts, prosecutors, judges)	planned	Result 2	
5-9 November 2012[19]	Turkey (TBC)	Regional workshop to support the establishment of trusted fora for regular information exchange between financial investigators, FIU and the private sector (including financial sector)	planned	Result 2	
May-June 2013	Strasbourg	Preparing a report on the assessment visits with recommendations	planned	Result 2	Activity 2.7
July 2013	Kyiv, Ukraine	Regional conference on the assessment of progress made/Project Closing Conference	planned	Result 1	Activity 1.3
		3rd Project Steering Committee meeting	planned	All results	All activities

[18] To be confirmed in the 2nd Steering Committee Meeting 25-29 June 2012 in Tbilisi, Georgia

[19] To be confirmed in the 2nd Steering Committee Meeting 25-29 June 2012 in Tbilisi, Georgia

6.3 Indicative action plan

Activity		*Year 1*												*Year 2*												*Year 3*					
	Month	*1*	*2*	*3*	*4*	*5*	*6*	*7*	*8*	*9*	*10*	*11*	*12*	*13*	*14*	*15*	*16*	*17*	*18*	*19*	*20*	*21*	*22*	*23*	*24*	*25*	*26*	*27*	*28*	*29*	*30*
Res 1	**Eastern Partnership countries have defined strategic priorities regarding cybercrime and assessed measures taken**																														
1.1	Regional conference (launching event of the project) on effective measures against cybercrime			■																											
1.2	Regional conference on strategic priorities regarding cybercrime																■														
1.3	Regional conference on the assessment of progress made (closing event of the project)																														■
Res 2	**Eastern Partnership countries are provided with the tools for action against cybercrime**																														
2.1	Regional seminar on cybercrime legislation										■																				
2.2	Regional seminar on specialised cybercrime units (high-tech crime, cyberforensics, prosecution services)													■																	
2.3	Regional seminar on judicial and law enforcement training																■														
2.4	Regional seminar on law enforcement – ISP cooperation														■																
2.5	Regional seminar on international cooperation against cybercrime							■																							
2.6	Regional seminar on financial investigations												■																		
2.7	Peer-to-peer assessment and advisory visits to each Eastern Partnership country																					■	■	■	■	■	■				
Res 3	**Eastern Partnership countries participate more actively in international cybercrime efforts**																														
3.1	Support the participation of Eastern Partnership countries in international activities against cybercrime						■				■					■			■										■		