Council of Europe
Conseil de l'Europe

European Union
Union européenne

www.coe.int/cybercrime-Georgia

Strasbourg, 26 November 2010

ECISD/2215(2009)46
Final

Project on Cybercrime in Georgia

FINAL NARRATIVE REPORT

(1 June 2009 - 31 May 2010)

Prepared by the Economic Crime Division
of the Directorate General of Human Rights and Legal Affairs

Project funded by the European Union and Council of Europe

Contact

For further information please contact:

Economic Crime Division
Directorate General of Human Rights and Legal Affairs
Council of Europe
Strasbourg, France

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

Disclaimer

Contents

Executive summary

This report summarises activities implemented and results achieved under the EU/COE Joint Project on Cybercrime in Georgia between 1 June 2009 and 31 May 2010, when it was completed.

About thirty activities and two joint activities with the Council of Europe Global Project on Cybercrime (phase 2) were carried out during the Project's implementation ranging from legislative reviews, "train the trainers" course, workshop on cooperation between law enforcement and internet service providers, translation of some relevant international documents related to cybercrime including training materials, and a regional event on international cooperation in cybercrime investigations.

The overall objective of the project was to contribute to the security of and confidence in information and communication technologies in Georgia and to help Georgia develop a consistent policy on cybercrime in view of implementing the Convention on Cybercrime (CETS 185).

Progress made specifically towards the four expected results can be summarised as follows:

Expected Result 1: Legislation - Legislative proposals will be available to bring Georgian legislation fully in line with the Convention on Cybercrime and related European standards on data protection

The Project gave special consideration to this output as it was clear from the beginning that adequate legislation is a prerequisite for the success of the other outputs. Thus, several activities (workshops and legal opinions) focused on the assessment of existing legislation on cybercrime and data protection in order to identify the provisions that need further reform. In the second stage, the Project supported the establishment or the ongoing work of the legislative working groups and reviewed the draft amendments prepared.

The assessment made by the first report on cybercrime legislation confirmed the Georgian's view that *'the gaps found (...) are too many to be dealt within the framework of this overview and should be subject to future, more focused work'.* Furthermore, the data protection analysis stated as well that although some provisions for the public sector provided a certain degree of protection to the citizens, there was a lack of a systematic and comprehensive approach, covering both the public and the private sectors, to the fundamental right to data protection in Georgia.

Taking advantage of the political context and the awareness about cybercrime further to the attacks in 2008, the Project was able to support complex legislative reforms (i.e. legislative amendments on cybercrime and data protection in line with the international standards) in a very short period while other countries have been struggling for years to draft similar legislation. The new legislation will have a great impact on fighting cybercrime in Georgia by providing the legal basis for investigating cybercrime at national and international level, including for public/private cooperation in such investigations.

The process of ratification of the Cybercrime Convention was initiated and will be completed in parallel with the adoption, by the Parliament, of the implementing legislation.

Expected Result 2: Training - Training policies and modules are available for standard training courses for law enforcement authorities, prosecutors and judges regarding the investigation, prosecution and adjudication of cybercrime

The questions of structured and sustainable training, certification of training modules and trainees as well as the different levels of knowledge required by the personnel working in this area have been of a great concern in the past years both at national and international level. It is a reality that while in many countries law enforcement authorities have been able to strengthen their capacities to investigate cybercrime and to secure electronic evidence, this is not the case of judges and prosecutors although they play an essential role in the criminal justice process. Relevant initiatives have been developed at the European level with regard to law enforcement training on cybercrime but, unfortunately, available training for judges and prosecutors that would enable them to deal with cybercrime cases and electronic evidence, is still far too limited.

In the framework of the Council of Europe Global Project on Cybercrime 2 a concept paper on institutionalising cybercrime training was developed with the purpose to help judicial training institutions to provide training for judges and prosecutors in cybercrime and electronic evidence matters and to integrate such training in regular initial and in-service training. By involving Georgia in this initiative synergies have been created from the beginning between the two projects. The two questionnaires received from Georgia for the concept paper provided important information on the existent training on cybercrime for judges and prosecutors.

Furthermore, it was agreed with the High School of Justice and the Ministry of Justice that once the new legislation on cybercrime is adopted, the cybercrime training concept will be implemented in Georgia. The initial training will include modules on electronic evidence and cybercrime and more sustainable in-service cybercrime training - at basic and advanced level - will be available for judges and prosecutors.

The major problems indentified in Georgia regarding cybercrime training were the lack of training materials and trainers. As in recent years tools against cybercrime, including training materials, have been developed and good practices are available, the Project supported Georgia to make use of these agreed upon tools and instruments, which were translated into Georgian.

A "train the trainers" course was developed and carried out specifically for Georgia. Considering that some staff members participated in this course, they should be able to transfer their experience to other judges and prosecutors dealing with cybercrime and digital evidence.

Expected result 3: Institution building - Proposals available for the creation of a 24/7 point of contact for international police cooperation, the establishment of a high-tech crime unit within the police and competent authorities for international judicial cooperation in cybercrime cases

Concrete examples of establishing high tech crime units and lesson learnt from Romania, Ireland, and Estonia were provided during the Project activities.

A report was provided to advise the authorities on the steps to be followed in establishing such unit. Subsequently, in November 2009 a decision to establish a high tech crime unit was made by the Minister of Internal Affairs within the Criminal Police Department, and three

investigators were selected to work in this unit, which will have also the function of 24/7 contact point.

Other activities carried out by the Project (e.g. regional workshop on cybercrime, workshop on law enforcement/internet service provider cooperation, legislative workshops, drafting new legislation and concluding of the Memorandum of Understanding between the law enforcement agencies and internet providers) are relevant for this output as well.

However, in order to ensure the functioning of the unit, equipment and trained personnel are required in addition to cybercrime legislation enforced. Without additional financial support it would have been unrealistic to aim at establishing a high tech crime unit. Although there is no functional cybercrime unit yet in Georgia, important steps have been made in this direction as well as strengthening multi-stakeholder cooperation against cybercrime.

Expected result 4: Law enforcement/internet service provider cooperation - Policy available regarding law enforcement authorities and Internet service provider cooperation in the investigation of cybercrime in line with Georgian legislation and the guidelines adopted at the Council of Europe in April 2008

The activities organised by the Project with the involvement of the private sector raised awareness on the need to develop a culture of trust and cooperation between public and private sector. Once entered into force, the new legislation will provide the legal basis for the service providers to cooperate with law enforcement in cybercrime investigations.

Conclusion of the Memorandum of Understanding between the law enforcement agencies and internet providers, based on the principles of the guidelines adopted by the global conference in Strasbourg in April 2008 and signed on 14 May 2010 is the most important achievement of this output.

In short, the major achievements of the Project that could yield considerable impact in Georgia are the drafting of the new legislation as well as the process triggered at different levels: raising awareness on the cybercrime threat, capacity building, cybercrime training for law enforcement, judges and prosecutors, cooperation among different institutions, including between law enforcement and internet service providers.

The overall assessment of the project stated that it helped the beneficiary to take a big and decisive step towards fighting cybercrime and protecting personal data in line with the international standards, and provided a solid basis for further measures. As fighting cybercrime depends to a great extent on international cooperation, *similar successful projects would be desirable, wherever states do not fully comply yet with the Convention on Cybercrime.*

1 Description

Name of beneficiary of grant contract:	Council of Europe
Name and title of the contract person:	Alexander Seger, Economic Crime Division, Directorate General of Human Rights and Legal Affairs
Counterpart institutions in the Action:	Ministry of Justice and Ministry of Internal Affairs of Georgia
Title of the Action:	Project on Cybercrime in Georgia (policy advice)
Contract number:	TACIS/2009/205431
Start date and end date of the Action:	12 months (1 June 2009 - 31 May 2010)
Target country:	Georgia
Final beneficiaries:	Georgian society

2 Assessment of the implementation of activities of the Action

2.1 Activities and results

List of completed activities (1 June 2009 – 31 May 2010)

Date	Place	Description
3-4 June 2009	Tbilisi	Project planning visit
15 July 2009	Tbilisi	Round table discussion on creation of a 24/7 point of contact for international cooperation on cybercrime cases and the establishment of a high-tech crime unit
16 July 2009	Tbilisi	Workshop on cybercrime legislation
August 2009	Strasbourg	Analysis of the questionnaires sent by Georgia in view of developing the Concept Paper on cybercrime training for judges and prosecutors
August 2009	Strasbourg	Analysis of the legislation on cybercrime in Georgia (drafting the report)
Aug-Sep 2009	Strasbourg	Report on the establishment of a high-tech crime unit in Georgia (drafting the report)
Aug-Sep 2009	Strasbourg	Analysis of the legislation on data protection in Georgia (drafting the report)
3-4 Sep 2009	Strasbourg	Workshop on institutionalizing training on cybercrime (global Project on Cybercrime 2)
5 Sep 2009	Strasbourg	Analysis of the legislation on cybercrime in Georgia (submitting the report to the Ministry of Justice and Ministry of Internal Affairs)
5 Sep 2009	Strasbourg	Report on the establishment of a high-tech crime unit in Georgia (submitting the report to the Ministry of Justice and Ministry of Internal Affairs)
28 Sep 2009	Tbilisi	Steering Committee meeting
28 Sep 2009	Tbilisi	Round table discussion on creation of a 24/7 point of contact for

		international cooperation on cybercrime cases and the establishment of a high-tech crime unit
29 Sep 2009	Tbilisi	Workshop on cybercrime and data protection legislation
16 Oct 2009	Tbilisi	The Working Group for drafting amendments to cybercrime legislation was established by a Decree of the Minister of Justice
October 2009 - February 2010	Tbilisi	Drafting the amendments on cybercrime and data protection
November 2009	Strasbourg	The reports on cybercrime and data protection legislation were translated into Georgian and sent to the working groups for drafting the amendments
27 Jan 2010	Strasbourg	The Guidelines on law enforcement - internet service providers cooperation available in Georgian
1 Feb 2010	Strasbourg	Concept Paper on cybercrime training for judges and prosecutors available in Georgian
Feb 2010	Tbilisi	Selection of the candidates for "train the trainer" course
Feb 2010	Strasbourg	Developing the "train the trainers" course for Georgia
Feb 2010	Tbilisi	Selection of 3 investigators to work within the HTC Unit
March 2010	Strasbourg	Comments on Georgian draft law implementing the Cybercrime Convention (drafting the report)
March 2010	Strasbourg	Second Report on the Draft Law on Personal Data Protection of the Republic of Georgia (drafting the report)
1 March 2010	Tbilisi	Steering Committee Meeting
1-3 March 2010	Tbilisi	"Train the Trainer" course (first module)
2 March 2010	Tbilisi	Workshop on law enforcement-ISP cooperation
2 Mar 2010	Tbilisi	Conference on cybercrime
March 2010	Strasbourg	Comments on Georgian draft law implementing the Cybercrime Convention (submitting the report to the Ministry of Justice and Ministry of Internal Affairs)
15 March 2010	Strasbourg	Second Report on the Draft Law on Personal Data Protection of the Republic of Georgia (submitting the report to the Ministry of Justice and Ministry of Internal Affairs)
March 2010	Strasbourg	Comments on Georgian draft law implementing the Cybercrime Convention available in Georgian
23-25 March 2010	Strasbourg	The Octopus Interface Conference Cooperation against cybercrime (global Project on Cybercrime 2)
6 April 2010	Strasbourg	Second Report on the Draft Law on Personal Data Protection of the Republic of Georgia available in Georgian
March - May 2010	Tbilisi	Finalising the draft the amendments on cybercrime and data protection in order to be submitted to the Government
May 2010	Strasbourg	Training manual on cybercrime training for judges - developed under the Council of Europe global Project on Cybercrime - available in Georgian
May 2010	Strasbourg	Search of e-evidence training material available in Georgian
10 May - 31 May 2010	Strasbourg /Tbilisi	Evaluation of the Project
13 May 2010	Tbilisi	Regional Workshop on Cybercrime
13 May 2010	Tbilisi	"Train the Trainer" course (second module)
14 May 2010	Tbilisi	Signing the Memorandum of Understanding between the Law Enforcement Agencies and Internet Providers based on the principles of cooperation in the field of cybercrime
May 2010	Strasbourg	Translation into English of the Memorandum of Understanding

		between the Law Enforcement Agencies and Internet Providers based on the principles of cooperation in the field of cybercrime
14 May 2010	Tbilisi	Closing Conference

2.2 Cross cutting activities

2.2.1 Project planning visit (3-4 June 2009, Tbilisi)

The first Project's visit took place on 3-4 June 2009 in Tbilisi to meet the counterparts from the Ministry of Justice and the Ministry of Internal Affairs of Georgia and plan the activities for the next 3 months.

Mr. Markko Kunnapu, Ministry of Justice of Estonia, vice-chair at that time and currently chair of the T/CY (Cybercrime Convention Committee) was involved in the Project to make use of Estonia's expertise and lessons learnt after Estonia experienced similar cyber attacks.

During the visit meetings were held with:

- Mr. Giorgi Jokhadze, Head of Analytical Department, Ministry of Justice;
- Ms. Natia Gvazava, Head of International Relations Main Division, Ministry of Internal Affairs;
- Ms. Ketevan Khutsishvili, Project Manager, European Union Delegation of the European Commission to Georgia;
- Mr. Borys Wódz, Special Representative of the Secretary General of the Council of Europe in Georgia.

The discussions provided an overview of the ongoing efforts in Georgia to fight against cybercrime, especially with regard to the new legislative amendments on cybercrime, child protection and data protection. It was agreed that in the first part of the implementation of the Project priority should be given to output 1 - strengthening of legislation and output 3 - proposals for establishing a high tech crime for investigating cybercrimes as both require time to be implemented. Thus, output 2 - training and output 4 - law enforcement/internet service provider cooperation will be tackled in the second part of the Project when the legislative process is more advanced.

Further to the visit the names and contact details of the persons responsible for the Project in Georgia were provided:

Ministry of Justice	Ministry of Internal Affairs
Giorgi Jokhadze Head of Analytical Department	Natia Gvazava Head of International Relations Main Division
Rusudan Mikhelidze Deputy Head of Analytical Department Head of Research and Analysis Unit	Ekaterine Machavariani Deputy Head of International Relations Main Division

2.2.2 Steering Committee Meeting (28 September 2009, Tbilisi)

The aim of the meeting was to review the activities implemented between 1 June and 27 September 2009 and to discuss further activities. Prior to the meeting, a draft progress report covering the period 1 June - 27 September 2009 was prepared and distributed to the members of the Steering Committee to facilitate the discussions.

Regarding output 1 - legislation the SC agreed:

- In addition to the already existing Working Group on data protection, a Working Group for drafting amendments to cybercrime legislation to be established (deadline 12 October 2009).
- The legislative amendments to be finalised by the end of December 2009.
- In order to facilitate drafting the amendments, the legal opinions to be translated into Georgian.
- Subsequently and subject to the Ministry of Justice's request, the Project to provide an expert opinion on the draft amendments and/or organise a meeting with the experts to discuss them and/or deliver an official opinion on the final amendments.

For the output 2 - training the SC took note that the relevant information on available cybercrime training for judges and prosecutors had been provided through Georgia's contribution to the concept paper on institutionalising cybercrime training for judges and prosecutors developed in parallel under the Council of Europe Global Project on Cybercrime 2.

The EU/COE Project funded the participation of Georgia representatives in the workshop aimed at finalising the above-mentioned concept paper (3-4 September 2009, Strasbourg).

Mr Shota Rukhadze, Deputy Director of the High School of Justice of Georgia was invited to participate in the next SC meetings for the implementation of this output.

It was agreed that:

- The "train the trainers" course to be organised in 2010.
- Training materials developed at international level and the concept paper on institutionalising cybercrime training to be translated into Georgian.

For the output 3 - institution building, the Ministry of Internal Affairs announced that a decision on this issue would be taken by mid-October 2009 and underlined the need to provide such unit with sufficient trained staff, adequate funds and equipment. The high-tech crime unit will also serve as the 24/7 contact point.

Discussions are held at the National Security Council to prepare a cyber security strategy, which includes the establishment of a specialised police unit.

It was agreed that:

- The expert report provided under the project to be translated into Georgian.
- The second round table would discuss the report on the creation of a specialised police unit, prepared by two consultants.

For the output 4 - Law enforcement/internet service provider cooperation, in view of implementing the principles of the Council of Europe "Guidelines for the cooperation between law enforcement and internet service providers against Cybercrime" the document will be made available in Georgian.

In conclusion, the SC agreed that the major next step is drafting legislative amendments and the project would continue to focus on output 1 and output 2 until the end of the year.

The European Commission Delegation stressed the importance of this project for the European Union as part of its wider involvement in Georgia regarding data protection. It was also suggested to organise a public event aimed at announcing the legislative amendments on cybercrime and data protection in 2010.

During the meeting, Ms Natia Gvazava (mid-2009) and Mr Giorgi Jokhadze (January 2010) announced that they would leave their ministries and the deputies, Ms Ekaterine Machavariani and Ms Rusudan Mikhelidze would take the responsibility for the project's implementation.

2.2.3 Steering Committee Meeting (1 March 2010, Tbilisi)

The aim of the meeting was to review the activities implemented between 1 June 2009 and 1 March 2010 and to discuss the calendar of activities.

The new members of the Project's team, Mr Otar Kakhidze, Head of Analytical Department, Ministry of Justice and Mr Shalva Kvinikhidze, Head of International Relations Main Division, Ministry of Internal Affairs joined the Steering Committee meeting and reiterated the commitment of their institutions to successfully implement the project.

The review of the fours outputs reflected that:

Output 1 – Legislation:

- The draft amendments had been endorsed by the Minister of Justice and Chief Prosecutor.
- The upcoming conference organised under the Project would discuss with the experts the amendments in order to finalise the draft laws.
- The amendments on criminal procedural law would be integrated into the new Criminal Procedures Code, which will enter in force in October 2010, and the draft laws will be submitted to the Parliament by June for adoption in September 2010.
- There would be a risk that the upcoming elections at the end of May 2010 slow down the process.

Output 2: Training:

- The first "train the trainer" module would take place on 1-3 March 2010 and the second module in mid-May 2010.

Output 3 - Institution building:

- The Minister of Internal Affairs took the decision to create a high tech crime unit within the police in November 2009. In this respect three investigators were selected to work in the Unit. However, it is needed to adopt the adequate legislative framework on cybercrime in order to make the unit fully operational.
- The need to identify resources for equipment was raised again and it was mentioned that the US Embassy assistance could be an option.

Output 4 - Law enforcement/internet service provider cooperation:

- The workshop on 2 March 2010 was intended to evaluate the existing situation regarding cooperation between law enforcement agencies and internet service providers.

The representative of the Delegation of the European Union stressed the growing interest of the Commission for cybercrime, electronic evidence and data protection and assured that EU will continue to provide support to the process initiated under the Project.

The Project Manager raised the issue of international cooperation on cybercrime, which is fundamental for cybercrime investigations, reminding that due to the budget limitation no international event was foreseen despite the fact that such an event had been discussed during negotiations. As all the events under the Project have been organised in the headquarters of the governmental institutions at low cost and with strong involvement of the Georgian counterparts, the budget of the Project allows the organisation of such an event.

The Steering Committee agreed that:

- Progress has been made in most of the project areas;
- The priority remains finalising the ongoing reform on legislation, especially in the context of the coming elections, which might delay the process;
- The next events would discuss the amendments on cybercrime and provide the opportunity for representatives of working groups to ask clarifications from the experts;
- The Working Group on data protection legislation would present in the meeting the amendments on data protection legislation.
- The workshop on law enforcement/internet service providers was intended to assess the existing situation and further steps to be taken on this issue;
- A regional workshop on cybercrime to be organised with the purpose to help the authorities establish contact points with other countries from the region and benefit from the experience of more advanced countries in fighting cybercrime. Moreover, it will be an excellent opportunity to offer a better visibility of the Project's achievements.

2.2.4 Participation in the Octopus Interface Conference on cybercrime (Strasbourg, 23-25 March 2010)

The Conference gathered more than 300 cybercrime experts representing countries from all continents, international organisations and the private sector. At the close of the conference participants adopted key messages aimed at guiding further action.

During the Conference participants shared a common interest in pursuing the most effective approaches against the growing threat of cybercrime that societies worldwide are faced with. Such approaches comprise a wide range of innovative initiatives and actions that need to be pursued in a dynamic and pragmatic manner by public and private sector stakeholders.

The progress made by Georgia with the support of the EU/COE Project on Cybercrime was presented in the conference by the representative of the Ministry of Justice in the update session (plenary session) and in the Workshop 5: Capacity building / technical assistance against cybercrime.

In the outcome of the Conference Georgia example and the EU/COE Project were mentioned as good practices and some participating countries expressed their intent to follow the Georgia's systematic approach.

2.2.5 Regional Workshop on Cybercrime (13 May 2010, Tbilisi)

The regional workshop was aimed at strengthening international cooperation on cybercrime investigations and sharing best practices and experiences in adopting a legislative framework in line with the Convention on Cybercrime. It gathered representatives from public and private sectors involved in fighting against cybercrime from Armenia, Azerbaijan, Estonia, Georgia, Italy, Moldova, the Netherlands, Norway, Romania, Spain, Turkey, Ukraine and United Kingdom as well as Interpol.

Session 1 of the workshop looked into the issues that prevent effective investigations identified at national and international level and examples of good practices. The need for cooperation between law enforcement and internet service providers was underlined as it was a mutual agreement that industry does not benefit from the illegal activities committed through computer systems.

The speakers presented different experiences in fighting cybercrime and underlined the importance of the legislation, including the value of the Cybercrime Convention in developing common standards and a framework for international cooperation.

Session 2 on cybercrime legislation provided the opportunity for participating countries to discuss the state of national cybercrime legislation, including plans for reforms. It resulted that although some participating countries ratified the Convention on Cybercrime additional legislative and institutional measures are required to fully implement the standards of the Convention. It seems that once the new cybercrime legislation adopted and the institutional measures planned are taken, Georgia will represent good practices in the region.

Session 3 dealt with the issue of developing a comprehensive national cyber security strategy.
Georgia is in the process of designing such strategy and the experience of Estonia in taking counter measures to prevent large scale cyber attacks attempting to destabilise the ICT sector was presented. Such attacks could target different levels: state, society, industry or individuals and the responses should be at both national and international level. The existing international governmental policies and initiatives, and among them the Council of Europe Convention on Cybercrime, provide guidance.

In addition to the exchange of information on various topics of interest for cybercrime investigations, the event was relevant for establishing direct contacts among law enforcement officials from the participating countries.

As it benefited from a large coverage in the media it provided also a high visibility of the Project's achievements.

2.3 Activities related to Result 1 (legislation)

Expected Result 1: Legislation - Legislative proposals will be available to bring Georgian legislation fully in line with the Convention on Cybercrime and related European standards on data protection Activities ▪ Review Georgian legislation against the provisions of the Convention on Cybercrime (ETS 185) ▪ Review Georgian legislation against the provisions of the Convention on the Protection of Personal Data (ETS 108) ▪ Advise the Georgian working group in the drafting of legislative amendments ▪ Up to 2 in-country workshops on cybercrime legislation

The Project envisaged addressing the need for effective legislation in line with the Convention on Cybercrime and ratification of this treaty by Georgia. A review was required to assess the compatibility of the existing legislation with the Convention based on good practices available. In connection with measures against cybercrime, it was considered also the reviewing and effectiveness of data protection legislation in line with the Council of Europe Convention ETS 108 on the protection of data and other instruments. Such legislation is relevant with regard to privacy issues and to enable Georgia to engage in broader law enforcement cooperation with Europol and EU Member States.

During negotiations of the Project, it was agreed with the European Commission to build on the legislative proposals elaborated in the recent past years through a group of experts from governmental institutions, ISPs, UNICEF and the US Department of Justice which focused on online child abuse and other measures. Similarly, draft laws related to data protection, prepared by a working group of experts from Civil Registry Agency and the Analytical Department of the Ministry of Justice with the support of the EC, will be taken into account.

The following activities were carried out to achieve this output:

2.3.1 Project planning visit (3-4 June 2009, Tbilisi)

See also section 2.2.1

The Steering Committee agreed during the planning visit that the main priority for the first part of the Project should be the legislation.

During the implementation it resulted that without adopting new legislation no progress can be made on the other segments relevant for the Project (i.e. establishing a specialised unit, providing cybercrime training for prosecutors and judge, and cooperation between public and private sector).

Considering the imperative need to commence the legislative process as soon as possible, it was decided to organise the first event on legislation in one month to gather the information on existing/or planned laws that need to be assessed. This would allow drafting the legal opinions on cybercrime and data protection legislation during the summer and make use of the summer break.

2.3.2 Workshop on cybercrime legislation (16 July 2009, Tbilisi)

On 16 July 2009, a workshop on cybercrime legislation was held with the objective to make a preliminary assessment of the existing legislation on cybercrime in Georgia and identify the provisions that need further reform in order to comply with the requirements of the Convention on Cybercrime.

Over 25 representatives from the Ministry of Justice, Ministry of Internal Affairs, National Security Council, Delegation of the European Union, the Embassy of United States, experts and the Council of Europe participated in the meeting.

The workshop focused, in particular, on:

- International standards on cybercrime: the Council of Europe Convention on Cybercrime and the advantages for Georgia to become Party to the Convention;
- The impact of cybercrime on Georgia and current efforts to combat cybercrime;
- The 2007 cyber attacks in Estonia: lesson learnt and new legislation;
- Challenges in investigating cybercrimes;
- The Convention on Cybercrime - a framework for international cooperation;
- The Network of 24/7 points of contact and other mechanisms for international cooperation;
- National legislation on cybercrime and international cooperation in Georgia.

The event created the opportunity for the participants to learn more about the standards of the Convention on Cybercrime and the work of the Council of Europe on cybercrime worldwide and discussed approaches to integrate Georgia in such efforts.

The representative from Ministry of Justice of Georgia provided a preliminary assessment of the legislation on cybercrime from the perspective of its compliance with the Convention on Cybercrime. The main conclusion was that the existent legislation is insufficient to deal with cybercrime investigations and it does not reflect the standards of the Convention.

The participants' interventions expressed the need for:

- harmonisation of the national legislation with the Convention on Cybercrime as a priority;
- increasing the awareness on threats posed by cybercrime;
- training on cybercrime for police and prosecutors.

During the tour de table the participants shared their interest to learn from other countries' experience, including Romania that went through a similar process ten years ago and Estonia that experienced cyber attacks in 2007.

2.3.3 Analysis of the legislation on cybercrime in Georgia (report drafted by Prof. Dr. Henrik W.K. Kaspersen Amsterdam, the Netherlands)

Based on the discussions in the workshop and the documents subsequently provided (i.e. existing provisions of criminal law, criminal procedural law and related laws, as well as an abstract of relevant provisions from pending Bills), an analysis was conducted aimed to assess to what extend the current Georgian legislation is in line with the principles and content of the Cybercrime Convention and its Additional Protocol.

The legal opinion drafted by the Council of Europe's consultant was submitted on 5 September 2009 to the Georgian authorities with the purpose to facilitate the drafting of the legislative amendments.

The report states that although the Cybercrime Convention does not contain provisions on evidence, the premise of the Convention is that the law of its Parties enables to use and present electronic material in court to prove a criminal act. However, the Georgian rules of criminal evidence are narrowly defined, and, in consequence, electronic material as such is not admissible as evidence. The possibility to submit to the court electronic material as evidence should be provided by law and not left to the discretion of the courts.

Furthermore, the Cybercrime Convention provides in Article 16-18 important powers, which are directed at making available certain computer data for criminal investigation, without the need of a preceding search of a computer system. The report states that *the gap between the powers (to be) defined in Criminal Code and the requirements of the Cybercrime Convention is too big to give specified recommendations for effective implementation of the latter.*

In its conclusions, the report quoted the expert from Georgian stating that *'the gaps found (...) are too many to be dealt within the framework of this overview and should be subject to future, more focused work'*. The provisions of the Cybercrime Convention are insufficiently implemented and *"if Georgia would have the ambition to become a serious and reliable partner in international cooperation on cybercrime, in the broadest possible sense as formulated in article 14 CCC, there is an urgent need for not only to draft amendments that adequately introduce the content and meaning of the articles of the Cybercrime Convention into domestic Georgian Law, but also for a review of existing law, if the existing regulation does not impede investigations and prosecution of cybercrime".*

Furthermore, the report recommends:

- *To include the definitions of computer system (including computer servers and networks) and computer data in the criminal procedural law;*
- *Substantive law provisions should be reconsidered in order to be in line with the Convention and some provisions should be reviewed in view of possible application in the electronic environment;*
- *To include electronic evidence in criminal evidence law;*
- *To apply the new and old powers of the criminal procedural code in case of criminal investigations of any kind and no restrict its use to the investigation of specific crimes;*
- *To fully implement Chapter I and II of the Cybercrime Convention along the lines of the recommendations given in the report;*
- *To implement the provisions on international cooperation as comprised in Chapter III of the Cybercrime Convention;*
- *To have a more structural approach when drafting new legislation.*

2.3.4 Report on the data protection legislation (drafted by Emilio Aced Félez, Spain)

The main part of the report was devoted to review the current Draft Law on Personal Data Protection as it will be the main piece of legislation regulating data protection in Georgia in the future. It pointed out its strengths and weaknesses by checking the European standards on data protection.

The report states that the Law on Personal Data Protection will provide a coherent and comprehensive regulation for data protection in Georgia. However, some important gaps were identified, such as:

- In the police sector, the provisions deal in most cases with confidentiality and procedural issues lacking to provide a complete and coherent legal framework for the protection of privacy when personal data are processed in this field.
- There is no regulation for the private sector tackling the processing of personal data, apart from the provisions of Article 8 of the Law on Electronic Communications that seem to apply both to the public and private sectors. This is an important drawback since nowadays private sector is also an intensive and massive user and processor of personal data for many purposes.
- There is a lack of data protection standards regulating the processing of personal data by law enforcement authorities – both in the current and would-be legal instruments.

2.3.5 Steering Committee Meeting (28 September 2009, Tbilisi)

See section 2.2.2

2.3.6 Second workshop on cybercrime and data protection legislation (29 September 2009)

The workshop was a follow up to the previous activities on legislation (i.e. one workshop on legislation and the reports assessing the Georgian legislation on cybercrime and data protection) aimed at discussing the conclusions of the two reports with the persons responsible for drafting amendments.

The meeting discussed in detail the findings of the reports and the recommendations made on improving data protection legislation.

On this occasion the Ministry of Justice announced that in addition to the existent Working Group on data protection, a Working Group would be established by 12 October 2009 for drafting amendments to cybercrime legislation in view of implementing Cybercrime Convention by taking into account the recommendations provided by the reports drafted under the Project.

2.3.7 Working Group for drafting amendments to cybercrime legislation

On 16 October 2009, by a Decree of the Minister of Justice, a Working Group for drafting amendments to cybercrime legislation was established. The deadline to present the draft laws fully implementing the Convention on Cybercrime to the Minister was 15 December 2009.

The same deadline applied for the existing Working Group with regard to the data protection amendments.

2.3.8 Steering Committee Meeting (1 March 2010, Tbilisi)

See section 2.2.3

2.3.9 Conference on cybercrime (2 March 2010, Tbilisi)

The Conference discussed the progress made by Georgia in fighting cybercrime during the 10 months of Project's implementation (i.e. the draft amendments, measures to establish high tech crime unit) and the remaining issues that need to be addressed.

Prior to the event the expert prepared draft comments on the amendments to the cybercrime legislation, which were discussed with representatives from the working group. Subsequently, based on the discussions and clarifications provided during the meeting a second legal opinion was submitted to the authorities.

During the workshop it was reported that implementation of the Additional Protocol to the Cybercrime Convention on Racism and Xenophobia would follow in a later stage and the implementation of article 22 of the Cybercrime Convention on jurisdiction would need to be studied a bit further, in particular with regard to the implications of the dedere aut iudicare principle and the consultation mechanism.

With regard to the data protection legislation, a representative of the working group presented the draft amendments in the meetings.

As previously a TAIEX mission had been in Tbilisi in February with the purpose to assess the data protection legislation and in order to avoid overlapping it was questioned if there was a need for a second legal opinion provided by the Project. The Ministry of Justice requested the Project to deliver a second opinion on the draft law on data protection as well.

On this occasion, the representative from the Ministry of Internal Affairs presented the progress made in establishing a high tech crime unit, including a 24/7 contact point and the next steps needed to make the unit fully operational.

Other measures that need to be taken by Georgia in the future (e.g. a national strategy) and the challenges in the police cooperation at the international level were also discussed.

The conference addressed all the outputs of the Project and, in parallel, the first module of the "train the trainers" was delivered. Following the conference, a workshop on law enforcement/internet service provider cooperation was organised.

The conclusion of the Conference was that significant progress has been made in implementing the EU/COE Project on Cybercrime in Georgia.

2.3.10 Comments on the draft law implementing the Cybercrime Convention (drafted by Prof. Dr. Henrik W.K. Kaspersen Amsterdam, the Netherlands)

The reports reflected that the recommendations made in the first analysis were considered to a large extend by the second draft law. Comparing to the first draft an important progress was made, the approach is more structured and attention was paid to the definitions and regulation of electronic evidence.

The observations, given in the form of comments, made suggestions for better implementation of the Cybercrime Convention's provisions and further improvement of the structure of the law, some concepts and the wording used in the text. Apart from these observations some provisions would still require additional work before finalizing the draft law in order to be fully in line with the international standards.

2.3.11 Second Report on the Draft Law on Personal Data Protection of the Republic of Georgia (report drafted by Emilio Aced Félez, Spain)

The report states that the entering into force of the Draft Law on Personal Data Protection (DLPDP) will provide a coherent and comprehensive regulation for data protection in Georgia (which does not exist at the moment).

On the content of the new draft, it was pointed out that several improvements were introduced in the line suggested by the first report and this is a positive and welcome development (for instance, in the structure of the principles of data processing).

There are still some points deserving attention and needing action:

- The first important point to note is the new draft completely excludes from its scope of application all personal data processing activities carried out by law enforcement authorities but without providing any additional regulation dealing with this crucial matter. Thus, it was strongly advised to reflect about this issue and put in place adequate safeguards, through the appropriate legal instruments (as indicated in the first report), regulating the processing of personal data by law enforcement authorities in order to respect the fundamental right to data protection in this field.
- One important omission in the regulation on sensitive data was health data, which is a serious lack of compliance with European legislation and must be addressed and corrected.
- Another point for concern was the suppression of the references to the role of Data Protection Officers. Although their existence is not mandatory, the legal framework established by the former draft was a good basis to set up this very interesting position in the Georgian data protection structure.

The report also states that a number of improvements have been introduced regarding the previous version and, in particular, a clearer structure of the three first chapters that contributes to better align the new draft of the Law on Personal Data Protection of the Republic of Georgia with the Convention 108 of the Council of Europe and the Directive 95/46/EC of the European Union.

2.3.12 Regional Workshop on Cybercrime (13 May 2010, Tbilisi)

See section 2.2.5

2.3.13 Translations of legal opinions provided under the Project

All the legal opinions provided under the Project were translated into Georgian.

2.3.14 Ratification by Georgia of the Convention on Cybercrime (CETS 185)

A letter was sent to the Deputy Minister of Foreign Affairs by the First Deputy Minister of Justice in May 2010. According to the letter *"on 1st of April, 2008 Georgia signed the Convention on Cybercrime dated November 23, 2001. Taking into consideration the reforms against cybercrime, the Ministry of Justice of Georgia considers reasonable to take necessary steps to ensure binding nature of the above Convention [...]. The joint project of European Commission and the Council of Europe, on the issue of cybercrime started on 1st of June, 2009 and shall be completed on 30th of May, 2010. The above project has been carried out with significant success, the set goals have been achieved in four directions: drafting legal amendments; steps, taken to form Special Service Units to combat cybercrime; trainings;*

cooperation between the Law Enforcement Authorities and internet providers [...] I request your good self to take the legal actions in order to finish the domestic procedures necessary for the mandatory recognition of the Convention".

Achievements:

- During the 12 months of the Project, the relevant provisions on cybercrime and data protection in Georgia were assessed from the perspective of their compliance with the international standards.

- Based on the input provided in two rounds – initially on the existing legislation and draft laws and in a second stage on the amendments proposed – new draft legislation in line with the international standards is now in the process of adoption.

- Entering into force of the new legislation will have a great impact on the strengthening of legislation on the matter in Georgia and provide the legal basis for investigating cybercrime.

- The process of ratification of the Cybercrime Convention has been initiated in May 2010 and will be completed in parallel with the adoption by the Parliament of the implementing legislation.

2.4 Activities related to result 2 (training)

Expected Result 2: Training: Training policies and modules are available for standard training courses for law enforcement authorities, prosecutors and judges regarding the investigation, prosecution and adjudication of cybercrime Activities ▪ Analysis of training needs for law enforcement, prosecutors and judges ▪ Review internationally available training materials and adapt them to Georgian needs ▪ Support up to 2 pilot training workshops ▪ Support the drafting of a training policy

The Project recognised the need for an approach to provide structured and sustainable training of law enforcement, prosecutors and judges. This includes standardized training modules for law enforcement (standard and possibly advanced courses on cybercrime investigations and forensic computing), prosecutors (standard courses on cybercrime investigations, electronic evidence and legal measures) and judges (standard courses on legal measures and electronic evidence).

The issues of certification of training and trainees, different levels of knowledge required by different people involved in prosecution of cybercrime offences and the sustainability and replicability of such training have been of concern for both European Union and the Council of Europe.

Important initiatives have been developed at the European level and the Project addressed the need to be adapted and implemented in Georgia.

The following activities were carried out to achieve this output:

2.4.1 Concept paper on institutionalising cybercrime training for judges and prosecutors

It is a reality that in many countries law enforcement authorities have been able to strengthen their capacities to investigate cybercrime and secure electronic evidence unlike judges and prosecutors who play an essential role in the criminal justice process. More efforts are required to change this situation and enable judges and prosecutors to prosecute and adjudicate cybercrime and make use of electronic evidence through training, networking and specialisation.

One of the initiatives taken by the Council of Europe Global Project on Cybercrime 2[1] was to draft a concept paper on institutionalising cybercrime training to help judicial training institutions develop training programmes on cybercrime and electronic evidence for judges and prosecutors and to integrate such training in regular initial and in-service training. It will furthermore facilitate networking among judges and prosecutors to enhance their knowledge as well as consistent – rather than ad hoc – support to training initiatives by interested partners.

The concept was drafted based on information received from training institutions in Belgium, Croatia, Georgia, Germany, France, Netherlands, Poland, Portugal, Romania, Spain, "the

[1] For more information see www.coe.int/cybercrime

former Yugoslav Republic of Macedonia" and the United Kingdom (replies to a questionnaire received in June 2009), a workshop held in Portugal in July 2009 with representatives from Belgium, Ireland, Italy, Netherlands and the United Kingdom, as well as the private sector, including Cybex, Ebay, EuroISPA, Google and Microsoft. On 3-4 September 2009, a workshop was held in Strasbourg with representatives of training institutions, judges and prosecutors from the above mentioned countries, the private sector as well as the European Judicial Training Network and the Lisbon Network of the Council of Europe.

The objectives of the concept are:

- To enable training institutes to deliver initial and in-service cybercrime training based on international standards,
- To equip the largest possible number of future and practicing judges and prosecutors with basic knowledge on cybercrime and electronic evidence,
- To provide advanced training to a critical number of judges and prosecutors,
- To support the continued specialisation and technical training of judges and prosecutors,
- To contribute to enhanced knowledge through networking among judges and prosecutors,
- To facilitate access to different training initiatives and networks.

Measures in the following areas should help achieve these objectives:

- Institutionalising initial training,
- Institutionalising in-service training,
- Standardised and replicable courses/modules,
- Access to training/self-training materials,
- Pilot centres for basic and advanced training,
- Enhancing knowledge through networking,
- Public/private cooperation.

The Council of Europe recommends widely dissemination and implementation by judicial training institutions of this concept. Georgia was involved in developing this concept paper in view of implementing it with the support of the EU/COE Project on Cybercrime.

According to the discussion with the Deputy Director of the High School of Justice of Georgia, the HSOJ expects to start implementation of the concept in 2011, which is feasible provided that the new legislation is adopted by then (training modules on substantive law, procedural law, including electronic evidence, need to consider the new legislation adopted and in the future case study).

2.4.2 Information on cybercrime training for judges and prosecutors

The replies of the authorities from Georgia to the questionnaire[2] on cybercrime training provided important information on the existent training and needs to be addressed under the Project.

It resulted that the High School of Justice (established in April 2006) is the institution in charge with initial and in-service training for judges. Trainers are from academia and judges from the Supreme Court or courts of appeal.

[2] The questionnaire was drafted under the CoE global Project on cybercrime 2 to gather information used later on in drafting the concept paper on institutionalising cybercrime training for judges and prosecutors

Prosecutors are trained by the Training Unit of the Analytical Department of the Ministry of Justice.

Information received suggested that:

- There is a need to increase awareness among authorities regarding the urgency of taking measures against cybercrime, including on cybercrime training.
- Initial training on cybercrime covers basic levels and advanced or specialist training is not foreseen.
- Training on cybercrime and/or electronic evidence had not been provided in the last 3 years.
- Standardised training materials are not available.
- Budgetary resources to provide training are limited and private sector support is not possible.
- External donor support from NGOs and international players/governments is delivered on a project basis.
- No trainers on cybercrime for prosecutors are identified.
- Given the goal of providing all judges and prosecutors with a basic level of knowledge of cybercrime and electronic evidence, the training offer is far too limited.
- Some of the issues addressed by the questionnaire (i.e. topics to be addressed in basic short and advanced training) were considered premature at this stage.
- Other topics are in higher demand for judges than the training on cybercrime/electronic evidence.
- Prosecutors receive initial training as a part of the internship program (both preparatory training and work assignments) and in-service training on a regular basis.

According to the questionnaire, the HSOJ can increase or decrease the number and duration of these trainings in accordance with the needs of the judiciary but the problem will still remain the training materials and trainers.

It was suggested:

- to involve investigators and prosecutors in the training to develop a common understanding;
- that the training to focus on theory and practice and involve practical skills in IT environment (e.g. exercises, recent cases, mock trials, etc.);
- to combine such training with study visits to investigative/prosecutorial agencies from more advanced countries;
- the topics to be determined by analysing the situation in a country and focus on specific crimes that are most widespread/problematic, as well as on the new legislation adopted.

This information was very useful for the Project's approach regarding output 2.

2.4.3 "Train the Trainer" course (1-3 March 2010, Tbilisi and 13-14 May 2010, Tbilisi)

It is essential to provide prosecutors, judges and investigators with an insight into the criminal use of technology and to strengthen their capacities to investigate and prosecute cybercrime as well as secure electronic evidence. In this respect, a minimum number of trainers would need to be trained in order to ensure the sustainable delivery of such training, preferably in local languages and with only limited needs of international trainers.

The resources available for the project allowed developing a short programme (course) involving judges, prosecutors and law enforcement. This course was designed to provide delegates with an insight into the criminal use of technology and the extent of the response of the criminal justice system. In addition, it provided delegates with skills to enable them to prepare presentations on the subject for their peers and included also a short course on the fundamentals of law, procedure, technology and some of the skills required to become an effective trainer.

The course was hosted by the High School of Justice and delivered in two parts: first part (1-3 March 2010, Tbilisi) as a learning module and in the second module (13-14 May 2010, Tbilisi) all the students were tasked to prepare a presentation.

Benefiting from a diverse audience (judges, prosecutors and police) in the same room this added value to the training, in particular, the judges seemed to benefit greatly from the technical and investigative presentations. It resulted that there is clearly an existing skill base amongst the police officers and a real desire to take on such cases by the prosecutors. Moreover, the judges attended the course have a much greater awareness of the issues.

The new legislation was of interest to all participants and the course provided also the opportunity of all three groups to discuss the issues from their different perspectives. It would be advantageous for these three groups to continue to discuss the issues as Georgia moves towards the legislative and investigative capabilities.

At the end of the course a report of the participants was provided by the trainers, which analyses the presentations delivered by each participant based on some criteria: preparation, outline the objectives, material used, structure, personal appearance, interaction etc. It was sent informally to the authorities to help them select future trainers.

2.4.4 Training materials and documents made available in Georgian

2.4.4.1 Training manual on cybercrime training for judges (developed under the Council of Europe global Project on Cybercrime 2)[3]

The purpose of the manual is to facilitate the organisation of basic training courses for judges in cybercrime matters and is designed to provide the material for a basic, introductory training course which should last for a minimum of two days. Obviously, it is possible to reduce or omit some of the topics and organise a one-day training course, or to expand it to one week or more by exploiting other materials referred to in the footnotes.

The structure of the manual follows the structure of the proposed course, namely:

- Chapter 2 provides an introduction to the phenomenon of cybercrime and the challenges it poses, in particular for judges. It furthermore introduces the Budapest Convention on Cybercrime which is the primary international standard ensuring a harmonisation of cybercrime legislation around the globe.
- Chapter 3 provides judges with a basic understanding of information technologies.

[3] The initial version of this manual has been prepared by Dr. Marco Gercke (Germany) for the Economic Crime Division of the Council of Europe (Directorate General of Human Rights and Legal Affairs) within the framework of the Project on Cybercrime. Inputs have been received from Nigel Jones (Technology Risk Limited, UK) Fredesvinda Insa (CYBEX, Spain), Jan Spoenle (Max-Planck Institute, Freiburg, Germany) and other experts. It has furthermore been reviewed in connection with the PROSECO project of the European Commission and the Council of Europe on judicial networking in South-eastern Europe (www.coe.int/economiccrime).

- Chapter 4 shows how the different types of conduct are defined as criminal offences. This chapter is very much based on the provisions of the Convention on Cybercrime, but it is important during a training course to relate these to the actual provisions under the respective national legislation.
- Chapter 5 offers a basic introduction to computer forensics and the question of electronic evidence.
- Chapter 6 outlines the procedural law measures that are at the disposal of criminal justice authorities in order to investigate cybercrime cases and to secure volatile electronic evidence in an efficient manner.
- Chapter 7 addresses international cooperation as cybercrime is the most transnational of all crime and cannot be addressed without efficient international cooperation. Judges play an important role in making such cooperation possible.

The appendix provides case examples that can be used to illustrate the issues dealt with in other chapters as well as a glossary of terms.

By the end of this training course judges should be able to understand why cybercrime is an important concern, what substantive and procedural laws can be applied, and why often urgent and efficient measures as well as extensive international cooperation are necessary.

2.4.4.2 Seizure of e-evidence guide

The guide was developed under the EU Project from the Programme Oisin II - the Directorate-General of Justice and Home Affairs, considering the need for suitable guidelines and instructions for an effective seizure of e-evidence and to guarantee the correct forensic handling of e-evidence. Such rules not only ensure that evidence is accepted in court, but also reduce the opportunity for claims for damages.

The guide conforms to the relevant EU directives and provides all frontline officers with a valuable aid for preventing and fighting crime.

The primary target groups for this Guide are first responders – i.e. the initial responding law enforcement officer and/or other public safety official arriving at the crime scene – and other non-IT experts. It should help them recognize, collect and preserve e-evidence when expert support is not available. The first responders may not always be able to obtain the expert assistance when handling e-evidence. Thus they need to be trained how to correctly seize and preserve e-evidence.

The adoption of good practices can minimize the risk of losing or damaging e-evidence due to the lack of expert availability at the crime scene. The purpose of the document is to recommend such good practices in search for, recognition of, collection of, and documentation of e-evidence and can be very useful for law enforcement agencies in Georgia as well.

It is organised as follows:

- Chapter 2 presents the general principles that should be followed when handling e-evidence;
- Chapter 3 defines the basic types of e-evidence seizure;
- Chapter 4 describes the main phases of a general seizure procedure;
- Chapter 5 provides more detailed instructions for handling various types of electronic equipment.

2.4.4.3 Concept Paper on cybercrime training for judges and prosecutors

See section 2.4.1

Achievements:

- The concept paper on institutionalising cybercrime training was developed with the participation of Georgia and this facilitates the process of its implementation once the legislation on cybercrime and electronic evidence is in place.

- Specific "train the trainer" course was developed and delivered in Georgian language to 14 participants (police officers, judges and prosecutors). Some of the participants attending the course could be selected as future trainers.

- Training materials are available in Georgian and can be used by the training institutions.

2.5 Activities related to result 3 (institution building):

Expected Result 3: Institution building: Proposals available for the creation of a 24/7 point of contact for international police cooperation, the establishment of a high-tech crime unit within the police and competent authorities for international judicial cooperation in cybercrime cases

Activities

- Review the capacities of the criminal police regarding cybercrime investigations and cyberforensics
- Propose a design for a high-tech crime unit or a similar specialized unit within the criminal police, including equipment required
- Prepare a proposal for the creation of a 24/7 point of contact for international police cooperation in line with article 35 of the Convention on Cybercrime
- Develop a proposal for competent authorities and efficient procedures for international judicial cooperation against cybercrime

The need for efficient institutions against cybercrime includes the establishment of a high-tech crime unit within the Criminal Police or a similar specialized unit. It also includes the creation of a well-functioning 24/7 point of contact for international police cooperation in line with Article 35 of the Convention on Cybercrime and measures to establish confidence and working relationships with contact points of other countries. In addition, there is a need to ensure that immediate and urgent measures at the level of police cooperation are followed up by efficient judicial cooperation by the competent authorities of the Ministry of Justice and the prosecution service in line with Chapter III of the Convention on Cybercrime.

The following activities were carried out to achieve this output:

2.5.1 Project planning visit on 3-4 June 2009, Tbilisi

See section 2.2.1

2.5.2 Round table discussion on creation of a 24/7 point of contact for international cooperation on cybercrime cases and the establishment of a high-tech crime unit (15 July 2009,Tbilisi)

On 15 July 2009, a round table discussion on establishing a high tech crime unit within police was organised in Tbilisi. Over 20 representatives from the Ministry of Justice, Ministry of Internal Affairs, National Security Council, European Commission and Council of Europe participated in the meeting.

Different models and experiences on high tech crime units from Romania, Ireland and Estonia were presented.

The purpose of the meeting was to help the experts evaluate the existing situation in Georgia in order to draft the report on the creation of a 24/7 point of contact for international cooperation and the establishment of a high-tech crime unit within the police.

2.5.3 Proposals for the establishment of a High Tech Crime Unit (report drafted by Nigel Jones, United Kingdom and Virgil Spiridon, Romania)

Further to the discussions during the Round Table, a report was drafted in order to make available proposals for establishing a high tech crime unit.

The report concluded that Georgia currently has a limited investigative capability to combat attacks such as those that took place in 2008, and to deal with digital evidence. The computer attacks against Georgia proved the fragility of computer systems at governmental level as well as at civil institutions or business level.

Furthermore the report recommends:

1. Prevention and combating cybercrime must be a priority taking into account the following features:
   - creation and assurance of a safe business environment both for ITC activity and for others who use computer systems for their businesses;
   - ensuring the trust of the population and the legal entities in the Internet as a safe means of communication and method of conducting business activities and using electronic means of payment;
   - ensuring safety for children's use of the Internet;
   - protection of critical infrastructure;
   - establishing a public-private partnership and efficient international cooperation structures aimed primarily at supporting the operational segment activities.

2. Completion of the national legal framework and harmonization with the European standards. The legislation must be looked from several angles:
   - the acts that should be criminalised (in this area new ways of committing crimes or new types of crimes appear all the time);
   - the procedures for investigating and researching these crimes (computer search, access to computer systems, etc.);
   - the definition of the international cooperation framework (the point of contact 24/7, spontaneous exchange of data and information, sending and responding to the mutual assistance requests, extradition, etc.)

3. Development of the national strategy for the security to define the security of computer systems, the critical infrastructure, the institution with responsibilities in this field and a joint working method for these institutions for preventing and taking the first measures in case that computer attacks occur.
4. The creation of a response centre for incidents – CERT.
5. Modernization and specialization of police structures for preventing and combating this phenomenon.
6. Creation of a specialized unit for cybercrime investigation.
7. Development of instruments and procedures needed for investigating and researching these crimes.
8. Provision of a training programme and equipping the new unit.
9. Development of cooperation relations with private sector and creation of proper mechanisms for international cooperation.
10. The establishment of the 24/7 contact point, in order to provide exchange of information in emergency situations in the area of cybercrime.

2.5.4 Steering Committee Meeting on 28 September 2009, Tbilisi

See section 2.2.2

2.5.5 Second Round Table (28 September 2009)

During the event, the experts presented the conclusions of the report, followed by discussion with representatives from the relevant authorities on further steps. The Head of the International Department of the Ministry of Internal Affairs announced that a decision to create such a unit could be made soon.

2.5.6 Second workshop on cybercrime and data protection legislation (29 September 2009)

In order to raise awareness on the need to strengthen the institutional capacity of Georgia against cybercrime at different levels, a session in the second legislative workshop was dedicated to the High Tech Crime Unit to move forward with the recommendations of the report. Current capability of Georgia to investigate cybercrime, a vision for creation of a specialised unit to investigate cybercrime, specialised police unit requirements and main tasks were some of the issues discussed.

In November 2009 the Deputy Minister of Interior agreed on initiating measures to create a high tech crime unit within the Criminal Police Department of the Ministry of Internal Affairs and the normative acts necessary for its creation to be prepared.

2.5.7 Steering Committee Meeting on 1 March 2010, Tbilisi

See section 2.2.3

2.5.8 Train the Trainer" course

The three investigators selected to work within the high tech crime unit participated in the "train de trainer" course, which included an insight into the criminal use of technology and the extent of the response of the criminal justice system.

See section 2.4.3

2.5.9 Workshop on law enforcement-ISP cooperation (2 March 2010, Tbilisi)

The workshop gathered representatives from law enforcement authorities and internet service providers to discuss current challenges of their cooperation and identify the ways to strengthen it.

The Council of Europe "Guidelines on cooperation between law enforcement and ISP against cybercrime" served as a basis for discussion.

After intensive debate between legislators, law enforcement officials and representatives of ISPs on how such cooperation should be developed, the conclusion was that the private sector is willing to cooperate with law enforcement provided that the adequate legal framework is in place.

The conference pointed at the need to establish trust between public and private sector and recommended to the representatives from the Ministry of Justice to have discussions on the draft laws also with the private sector.

Further to this event, the negotiation between the Ministry of Justice, the National Communications Commission, the Ministry of Internal Affairs and important service providers in Georgia started and ended with the conclusion of an agreement on cooperation, which was signed on 14 May 2010.

2.5.10 The Octopus Interface Conference Cooperation against cybercrime, Strasbourg, 23-25 March 2010 (global Project on Cybercrime 2)

See section 2.2.4

2.5.11 Regional Workshop on Cybercrime on 13 May 2010, Tbilisi

See section 2.3.5

2.5.12 Concluding of the Memorandum of Understanding between the Law Enforcement Agencies and Internet Providers based on the principles of cooperation in the field of cybercrime

See section 2.6.3

Achievements:

- The round table discussion and the report on high tech crime unit provided an assessment on the capability of Georgia to investigate cybercrime, collect and secure digital evidence and advised the authorities on establishing a high tech crime unit.
- The draft laws on substantive law and procedural law related to cybercrime will ensure the legal framework for cybercrime investigations, including the investigative powers for law enforcement.
- Three investigators were selected to work in the specialised unit and they were included in the "train the trainer" course.
- The specialised unit will have also the function of 24/7 points of contact established under the Cybercrime Convention.
- Signing the Memorandum of Understanding between the law enforcement agencies and internet providers.
- Increased the awareness of authorities and strengthening of multi-stakeholder cooperation against cybercrime.

2.6 Activities related to result 4 (law enforcement/service provider cooperation)

Expected Result 4: Law enforcement/internet service provider cooperation - Policy available regarding law enforcement authorities and internet service provider cooperation in the investigation of cybercrime in line with Georgian legislation and the guidelines adopted at the Council of Europe in April 2008 Activities ▪ Workshop on law enforcement – ISP cooperation to review current practices and challenges ▪ Develop proposals for regulations and other measures to help law enforcement and ISPs to organize their cooperation based on the guidelines developed by the Council of Europe in April 2008

A particular problem that law enforcement authorities face when investigating cybercrime is their cooperation with internet service providers. In order to help law enforcement and ISPs to structure their cooperation, the Council of Europe – under its Project on Cybercrime – elaborated and adopted guidelines to this effect.[4] The 2987th Justice and Home Affairs Council meeting (Brussels, 27-28 November 2008) recommended *strengthening the partnership between public authorities and the private sector, in particular, that the Commission work on the details of the guidelines adopted by the Conference on Global Cooperation Against Cybercrime, in April 2008.*

There is a clear need to establish trust between different public and private sector stakeholders involved in anti-cybercrime and other measures and to build bridges between law enforcement, internet industry, financial services and others.

The following activities were relevant for this output:

2.6.1 Steering Committee Meeting (1 March 2010, Tbilisi)

See section 2.2.3

2.6.2 Workshop on law enforcement-ISP cooperation (2 March 2010, Tbilisi)

See section 2.5.9

2.6.3 The Octopus Interface Conference Cooperation against cybercrime, Strasbourg, 23-25 March 2010 (global Project on Cybercrime 2)

See section 2.2.4

2.6.4 Regional Workshop on Cybercrime (13 May 2010, Tbilisi)

See section 2.2.5

---

[4] For these and other documents see www.coe.int/cybercrime

2.6.5 Guidelines on law enforcement - internet service providers cooperation available in Georgian

The Guidelines for the cooperation between law enforcement and internet service providers against cybercrime were adopted by the global Conference "Cooperation against Cybercrime" (Council of Europe) on 1-2 April 2008 to help law enforcement and service providers to organise their cooperation while respecting each others' roles and responsibilities as well as the rights of internet users.

The translation into Georgian has been provided by EU/CoE Project.

2.6.6 Memorandum of Understanding between the Law Enforcement Agencies and Internet Providers based on the principles of cooperation in the field of cybercrime

The purpose of the Memorandum of Understanding (MOU) is to define the principles of cooperation between the Internet Providers and Law Enforcement Agencies in cybercrime investigations in accordance with the provisions of the Criminal Procedures Code of Georgia.

It recognises the need to coordinate the efforts of both law enforcement agencies and internet providers without interfering with the users' rights. The document sets for:

- exchanging information;
- ensuring regular technical and legal trainings;
- the rights and responsibilities of each party;
- the depositary (Georgian National Communications Commission);
- possibility to join the agreement by other service providers.

Signing of the MOU between LE and industry and establish an effective relationship is one of the keys elements in a country to combat cybercrime. This is an excellent step for Georgia that needs to be followed by concrete action to develop effective working practices.

2.6.7 Involvement of private sector

The private and NGOs from Tbilisi were invited in the relevant activities carried out under the Project. Moreover, Microsoft's expertise was used in the Project activities to raise awareness on the challenges of fighting cybercrime and use of electronic evidence and to share good practices on public-private cooperation on cybercrime.

On several occasions the presentations made by the representative of Microsoft generated intensive discussions and interest on the practices and mechanisms used by Microsoft to cooperate with authorities at national and international level in criminal investigations, including the effort to reduce the risks of malware worldwide.

The experience shared by Microsoft working worldwide on these issues increased the value of the expertise provided by the Project.

Achievements:

- Raised awareness on the need to develop a culture of trust and cooperation between public and private sector.
- The new legislation provides the legal basis for the LEA -ISPs cooperation

- Concluding of the memorandum of understanding between law enforcement and service providers 14th May, 2010 based on the principles of the guidelines.
- Strengthening of multi-stakeholder cooperation against cybercrime.

3 Relation with the donor

The European Union Delegation was regularly invited to Project activities and kept informed on the progress made.

The Delegation of the European Union - through the Project Manager - provided valuable inputs during the implementation of the Project, participated and contributed in all activities organised.

4 Visibility

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_in_georgia/projectcyber_en.asp

Press releases of the events organised by the project were submitted to the press section of the European Commission Delegation to Georgia.

The most important events were announced also through the CoE Newsletter launched in October 2009, which has the purpose to send periodically an update on the activities carried out under the Global Project on Cybercrime and it is addressed to a large contact list of people working in this area.

The presentation of project results in the global Octopus Interface conference at the Council of Europe in Strasbourg (March 2010) helped make the project known to key stakeholders.

Several events organised under the Project (e.g. the conference on cybercrime, the regional event)[5] benefited from wide media coverage.

The donor was represented in all events organised within the project and addressed to the audience in the opening sessions, which contributed to the acknowledgment of the financial contribution made by the European Union to this Project. In addition, all the events used elements of static visibility.

[5] The Project's visibility continued even after its completion: the representative of Ministry of Justice form Georgia was invited in the Internet Governance Forum (September, 2010) to contribute and share the experience of implementing the Project in Workshop 23: Cybercrime – common standards and joint action, which was organized by the Council of Europe and focused on joint action against cybercrime, and Workshop 172 - Public-private cooperation on Internet safety/cybercrime.

5 Conclusions and recommendations

5.1 Conclusions

It is clear that in Georgia the authorities and society in general have become more aware of the driving force of the Internet, which plays an important role for the democratic process and is of utmost importance to contemporary society, but that it also requires measures against the illegal use of computer systems and data.

Countering cybercrime requires to meet various needs (e.g. policies and awareness of decision-makers, harmonised and effective legislation, regional and international cooperation), which were addressed by the EU/CoE Project on Cybercrime in Georgia.

In a rather difficult political context, all the expected results of the project have been achieved and the authorities - with the support of the Project as well - made significant progress to strengthen their capacity to deal with cybercrime. Important steps have been taken to bring the legislation on cybercrime and data protection in line with European standards, to create a high tech crime unit for investigating cybercrime, to ensure that adequate training for police, prosecutors and judges is available, and to develop public-private cooperation. Moreover, it is now under discussion that the Georgian Government designs a comprehensive national strategy on cyber security.

In addition to the initially planned activities, the Project management organised two activities: a conference on cybercrime and a regional workshop on cybercrime. Both events had a great impact on strengthening the cooperation against cybercrime at national and international level.

The final Evaluation Report of the EU/CoE Project on Cybercrime in Georgia states:

"The project has reached substantial impact in a very short time compared to other technical assistance projects: According to the indicators of the workplan, all results have been fully achieved [...]
The project created impact that goes even beyond the field of cybercrime: the new tools and procedures provided by the cybercrime draft law will be useful in investigating, prosecuting and adjudicating not only the specific cybercrime offences (i.e. illegal access, data and system interference, computer fraud, data interception, etc.), but also the traditional offences committed by means of a computer system (diffusion of child pornography, defamation, money laundering, distribution of racist and xenophobic material, etc.). The same holds true for the Memorandum between LEA and ISP. The draft law on data protection provides human rights safeguards not only for investigations of cybercrime but also for state agencies' actions in general. Besides, the training courses supplied the participants with information on collecting digital evidence for traditional criminal offences.

On several occasions the value of the Project and the impact of the work done were recognised[6].

It should be underlined that the work under the Project benefited substantially from the experience and lesson learnt gained by the Economic Crime Division during the work on cybercrime with a large number of countries worldwide under the Global Project on Cybercrime and it built on its achievements.

[6] The Octopus Conference Cooperation against Cybercrime (Strasbourg, 23-25 May 2010; letter sent by the Permanent Representation of Georgia to the Council of Europe)

The counterparts in Tbilisi – the Ministry of Justice, Ministry of Internal Affairs and the High School of Justice - played the key role in sustaining the efforts done under the Project demonstrating a clear resolve to integrate the country into European and international efforts to combat cybercrime.

A significant contribution to the changing of the situation in Georgia with regard to developing a policy to cope with cybercrime and manage electronic evidence was made by the Delegation of the European Union, which not only provided the main funding of this Project in a timely political context, but also - through the Project Manager - had a valuable contribution to its implementation.

It has to be underlined, however, that the current capability of Georgia to investigate cybercrime and collect and secure digital evidence is still limited. It is just a matter of time until the impact of new ICT technology in committing cybercrimes will affect Georgia and until the authorities will have to face increases in cybercrime (e.g. certain types of computer frauds, online child pornography or other type of offences related to ICT). In order to face this challenge it is necessary to ensure that the process will continue.

By becoming a party to the Convention on Cybercrime, Georgia will remain involved in international efforts against cybercrime (including the Consultations of the Parties to the Convention) and this will help sustain efforts within Georgia. The Council of Europe will continue to provide assistance within the framework of ongoing or future projects on cybercrime.

The group of experts involved in this project are internationally recognised. Their contribution to the success of the Project was crucial. As further recommendations have been made by the experts at the final event, the last section of the report resumes this valuable input.

5.2 Recommendations and the way ahead for Georgia

5.2.1 Legislation policy and raising awareness on the cybercrime threat

- During the process of amending the legislation and adoption procedure, to consult with all the relevant stakeholders (police, prosecutor, judge) to achieve a common understanding of the new legislation. This is very important in order to safeguard future cooperation between different authorities and prevent possible problem in courts. Such consultations should continue after the legislation has entered into force as well, including on possible need for further amendments based on case law.
- The Budapest Convention sets the necessary minimum, standards but any country can consider going beyond and establishing higher standards where appropriate.
- Raise awareness of different authorities with regard to new policies, including of the politicians and people responsible for policy planning.
- Establish a common understanding between IT sector and political sector.

5.2.2 National strategy against cybercrime

- The strategy should enable all the institutions responsible to protect Georgia to work regionally and nationally.
- Consider developing a policy and strategy concerning cyber threats and cyber security in general with a consideration on the fact that sometimes cybercrimes are

not just common offences, but a threat to the whole economy and national security.

- Nominate authorities to be responsible, start collecting information and start analyses concerning critical services and interdependencies between them, in particular dependency from the Internet.
- Actions that can be taken to make Georgia a hostile environment for the cyber criminal:
  - An effective police investigative capacity, including by allocating the necessary resources to the new high tech crime unit;
  - Robust criminal justice response in terms of the prosecutions and convictions;
  - Reporting systems for public and business, making business confident that reporting will not adversely effect their business or reputation;
  - Reporting systems to identify threats to children;
  - Close links with industry to enable the preservation and obtaining of information for use in identifying and locating perpetrators;
  - ISPs to consider, if not already, aligning themselves with international bodies such as INHOPE;
  - Educate public and raise awareness of security issues;
  - Ensure that industry uses secure systems;
  - Develop links with overseas partners to facilitate administrative and mutual legal assistance.

5.2.3 Training on cybercrime

- It is essential for Georgia to develop its own trainers to deliver its own programmes that meet its own requirements. Very often training courses are offered by other countries/donors who do not take into account the needs of the host country or are designed for countries with different problems. There are many training courses in the cybercrime area but not enough trainers, so this should be a key objective in the future.

- There are two valuable initiatives that could be useful for Georgian authorities:

  1) The programme of training courses that has been developed over a long period of time by the EU countries. These are designed and developed by and for cybercrime investigators and digital forensic investigators. There will shortly be a total of 19 courses that are made freely available to law enforcement on a global basis. These courses have academic accreditation and can lead to academic awards. Such courses could be a foundation for what has to be a structured training programme for the staff of the new cybercrime unit and suitable to be cascaded to others in Georgia as the need arises. The ability of Georgian trainers to adapt the training to local needs will be essential to the success of any training programme.
  2) The second initiative is the Council of Europe strategy for the training of judges and prosecutors. This gives the framework for a sound programme of training at initial and in service levels.

5.2.4 Institution building and cooperation at national and international level

- The members of the new cybercrime unit to have the opportunity to communicate with their international colleagues and attend regional and international events on

cybercrime. This will increase their network and allow them to share experiences and enhance their knowledge of matters that will affect them.

- As soon as the law and the anti cyber crime unit team is in place start with an "easy" case. This trains the team and gains the needed experience for harder cases.
- It will also help to get the necessary support from others involved, e.g. decision makers, budget setters, etc.
- Learn from the experience and make use of the trial and error of other countries, including by joining groups that you can learn from, e.g. Europol and London Action Plan.
- Create a pro-active environment in which threats are exchanged in time and industry becomes a part of the solution.
- Establish relations with other parties involved in the internet: registries of domain names and IP addresses, telephone companies, data transaction companies, internet exchange, etc.
- The reporting system for the illegal activities has to be developed in parallel with the unit.
- The cyber crime unit has to be promoted within the organization and to the public;
- Learn which are the unit needs: types of training and equipment needed, internal procedures for investigations, cooperation with the private sector (financial sector, ISPs etc).
- The 24/7 contact point established as a cannel for cooperation in the cybercrime cases and developed in the same time with the unit and with clear procedures defined on how to proceed with the request.
- International and regional cooperation is crucial for data information on different cases, best practices, common events, common training, sharing experiences on cybercrime trends, etc.
- As a minimum, countries should make use of possibilities for direct cooperation between authorities that are provided for in a number of European instruments.

Name of the contact person for the Action: Alexander SEGER

Signature: 

Location: Strasbourg

Date report due: 30 November 2010

Date report sent: 30 November 2010

6 Appendix - List of reports and other documents

6.1 Analysis of the legislation on cybercrime in Georgia (report drafted by Prof. Dr. Henrik W.K. Kaspersen Amsterdam, the Netherlands)

6.2 Comments on the draft law implementing the Cybercrime Convention (drafted by Prof. Dr. Henrik W.K. Kaspersen Amsterdam, the Netherlands)

6.3 Report on the data protection legislation (drafted by Emilio Aced Félez, Spain)

6.4 Second Report on the Draft Law on Personal Data Protection of the Republic of Georgia (report drafted by Emilio Aced Félez, Spain)

6.5 Proposals for the establishment of a High Tech Crime Unit (report drafted by Nigel Jones, United Kingdom and Virgil Spiridon, Romania)

6.6 Memorandum of Understanding between the Law Enforcement Agencies and Internet Providers based on the principles of cooperation in the field of cybercrime