Council of Europe
Conseil de l'Europe

European Union
Union européenne

28 May 2010 (final)

Project on Cybercrime in Georgia

Council of Europe Project No. ECISD/2215(2009)46

Evaluation Report

by

Ivan Salvadori

in co-operation with Tilman Hoppe

The views expressed in this report are those of the author and do not necessarily reflect official positions of the Council of Europe or of the donors funding this project.

The Project is implemented by the Council of Europe and funded by the European Commission and Council of Europe

www.coe.int/economiccrime

Table of Contents

1. Summary and Recommendations

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.

Under **Output 1,** two draft laws will be adopted soon, bringing the Georgian legal system virtually in line with the Council of Europe and the European Union standards on cybercrime and protection of personal data. These two laws will bring along a major advancement as many core regulations hitherto are missing in Georgia.

As for **Output 2**, the project developed comprehensive and professional training material including training curricula for judges, prosecutors and investigators. According to the trainees, the material remains a bit general and should be adapted more specifically to the Georgian legal system. Some staff has already been trained as trainers and should be able to transfer their experience to other judges and prosecutors dealing with cybercrime and digital evidence. The sustainability of the impact of this Output depends on the extent, to which the beneficiary will carry out initial and in-service training in line with the "Concept on cybercrime training for judges and prosecutors", developed by the Council of Europe. A possible need on the part of law enforcement agencies (LAE) and internet service providers (ISP) for training on the procedures of cooperation should also be taken into account.

The project delivered all proposals foreseen under **Output 3**. The practical impact of these proposals still needs to be unfolded. The cybercrime unit (including the 24/7 contact point) was formally established. However, its practical implementation depends on the adoption of the cybercrime law under Output 1. The cybercrime unit should be supported by a strategy on the available means to systematically fight cybercrime. Adequate advanced hard- and software is still not available to the cybercrime unit (a need, a future possible extension or follow-up project should take into account). As soon as the necessary technical tools are available, the staff will need specialised training courses to take full advantage of such tools.

As a result of the project's efforts under **Output 4**, ISP and LEA formally signed a Memorandum of Understanding ("Principles of Cooperation"). The Memorandum is mostly in line with the Council of Europe guidelines and will be an acceptable tool to give LEA and the judiciary access to the necessary data.

In order to achieve full **sustainability** of the project's impact, the beneficiary should take the following steps:

- Adopt the draft law implementing the Cybercrime Convention and the draft law on data protection as soon as possible.

- Based on the adopted law, implement the cybercrime unit and a 24/7 contact point.
- Develop a strategy on cybercrime and on cyber security in view of implementing the Convention on Cybercrime.
- Further adapt the training material to the specific Georgian legal and technical structure.
- Apply the ”Concept on cybercrime training” to train all staff dealing with cybercrime and digital evidence.

Additional outside advice and support would be a significant factor for the success of the above-mentioned measures, as the introduction of cybercrime standards is new to the beneficiary:

- Advice and support on the procurement of the necessary hard- and software tools for cybercrime investigation.
- Follow-up training on the implementation and use of such new technical tools.
- Advice on best practices for the daily work of a 24/7 contact point and a cybercrime unit.
- Training for ISP on the new legislation and the new Memorandum.
- Advice on the cybercrime and cyber security strategies.
- Plan study visits by members of the new cybercrime unit to comparable foreign units to enhance international co-operation and to share experiences on best practices.

The **project design** properly covers the four major needs of Georgia in the fight against cybercrime. The project was designed in response to an urgent need for legal and technical countermeasures against cybercrime and cyber-attacks, such as those happening immediately before the war in 2008; fortunately, the donor made it possible for the project to be quickly in place by making funds available on very short notice. The tight timeframe reflects the urgency; however, it might seem too ambitious, in one year’s time: a) to plan a full legislative process from assessing the legislative needs; b) to draft a complex law and to adopt it in Parliament and c) to plan further Outputs based on the passage of this legislation. Besides a more extended timeframe, future projects might want to consider the above-mentioned additional advice and support when drafting a timeframe. To facilitate cooperation between LEA and ISP, it might be worth considering including trainings for LEA and ISP on new cybercrime and personal data legislation and agreements. The project could have also included under Output 2 the drafting of a training strategy, which would complement the training policy and which would show, how and within what timeframe all criminal law judges, prosecutors and investigators, or most of them, from all Georgian regions will be trained on cybercrime and digital evidence. Such a comparatively small strategic step would already enhance

the sustainability of the training materials' impact. Besides, the indicators of "results" could have been a little more detailed and point beyond the mere delivery of outputs to their impact.

The project team **delivered** the Outputs in a professional manner and in close co-operation with the EU Delegation in Georgia and the beneficiary. The project team was located in Strasbourg and no long-term advisor was present in Tbilisi; however, this seems not to have been a problem, as the project team constantly communicated with and regularly visited the counterparts. Thanks also to the continuous support and active participation of the local EU Delegation, all activities were carried out as scheduled; in some cases more activities than initially planned.

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

2. Project Impact

2.1. Outputs 1: Legislation

"Indicator of Result: 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 most relevant impact of the project was achieved under Output 1. The final draft laws on **cybercrime** and on personal data protection are virtually consistent with the Council of Europe and the European Union standards on cybercrime and on protection of personal data. Both legislative drafts are ready for adoption by Parliament, which is expected in June-July 2010. In the meantime, the Ministry of Foreign Affairs of Georgia has already started the ratification process of the Convention on Cybercrime. With regard to the substantive criminal law, the cybercrime draft law covers all offences against confidentiality, integrity and availability of computer data and systems as well as computer-related offences and content-related offences, as required by the Convention on Cybercrime. It also provides substantial amendments to the Criminal Procedure Code in order to allow efficient investigation and adjudication of cybercrime. The main novelties concern expeditious preservation, search and seizure of stored computer data.

The final draft law on **personal data protection** was significantly improved compared to the first version. It provides a coherent and comprehensive regulation for data protection in Georgia. Nevertheless some changes and amendments - especially with regard to the protection of health data and the role of the Data Protection Officers -, should be considered by Parliament in order to bring the Georgian law fully in line with the European standards on personal data protection.

Other amendments contained in the draft cybercrime law concern the Code of Administrative Offences, the Law on Operative-Investigative Measures and the Law on Electronic Communications. A separate draft law on **Mutual Legal Assistance** in Criminal Matters was also elaborated, but is still not ready for adoption.

The impact under Output 1 goes directly down to the project. The project team supported the local working group in drafting the cybercrime and the data protection legislation. In particular, two independent consultants supplied legal opinions assessing Georgian legislation and making proposals to bring the domestic legislation fully in line with the Cybercrime Convention standards. The working group took into account the majority of the proposals when preparing the draft laws.

2.2. Output 2: Training

"Indicator of Result: 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 first activity concerned the preparation of comprehensive and professional **training material**. The beneficiary collaborated actively with the project team in the preparation of such material. The training material reflecting international standards was translated into Georgian to ensure that all the practising and future judges, prosecutors and investigators, or most of them, can achieve basic knowledge on cybercrime and digital evidence. The international documents (i.e. the "Cybercrime Training for judges: Training Manual"; and the "Guide on seizure of e-evidence") gave an overall picture of the topics relevant to the training on cybercrime. The "Concept on cybercrime training for judges and prosecutors" provided useful advices for the training institutions in order to develop training programmes on cybercrime and digital evidence and institutionalise them in the future. Nevertheless, it is still advisable to adapt them to the domestic criminal and procedure legislation on cybercrime. Even if the case law on cybercrime in Georgia is still limited[1] with no specific criminal law until now, some reference in a comparative perspective to the "law in action" of other countries with a long tradition in the fight against cybercrime could improve the trainees' understanding.

The second activity concerned the organization of **train-the-trainer** courses for judges, prosecutors and investigators. The training courses were delivered in two different modules by the same expert trainer, assisted by another independent trainer for the legal aspects. The first three-day basic level module provided an insight into the criminal use of new information technologies and into the possible responses of the criminal justice system. In addition, the first module provided delegates with skills for holding presentations on cybercrime for their peers. The aim of the second one-day module was to enable delegates to demonstrate how much they had learnt from the first module.

From the report on participant training delivery, drawn up by the organizers of the train-the-trainers courses, most trainers seem to show promising capacity to train their peers in the future. The number of trainers seems sufficient with three trained investigators and a total of 69 investigators in the Criminal Police Departments, but fairly limited – only two – related to 388 prosecutors employed in the Prosecution Service and also only three related to about 100 criminal law judges.

The informal evaluation given by one of the trainees on the quality and the contents of the training courses was basically positive. The only possible problem was the English

1 According to the information provided by a representative of the Ministry of Internal Affairs, 13 criminal cybercrime cases have been initiated in 2009.

language used during the training courses, but was properly addressed by the simultaneous translation.

The sustainability of the impact of this Output depends on the extent, to which the beneficiary will carry out initial and in-service training and institutionalise them in line with the "**Concept** on cybercrime training for judges and prosecutors".

Beyond the scope of the project, the beneficiary might want to consider including new courses on Criminal Information Law, Intellectual Property, etc. to the study plan of the Faculties of Law in order to provide some knowledge already to law students, as it is the case in other countries (e.g. United States, Germany, Italy).

2.3. Output 3: Institution building

"Indicator of Result: Proposals available for the creation of a 24/7 point of contact for international police co-operation, the establishment of a high-tech crime unit ['cybercrime unit'] within the police and competent authorities for international judicial cooperation in cybercrime cases"

According to the Indicator of Result, the impact of Output 3 was fully achieved: the project provided the counterparts with practicable proposals for the creation of a cybercrime unit (including a 24/7 point of contact), which would also be able to co-operate internationally. This proposals go back to a round table discussion on establishing a cybercrime unit from a comparative perspective, presenting different models and experiences on the creation and organization of such a unit. Moreover, two independent consultants made proposals for the creation of a cybercrime unit and a cyber security strategy in line with the international standards.

The impact of Output 3 will only be of practical use, once the unit is staffed and starts working; this will follow the adoption of the cybercrime draft law by Parliament. Three detective investigators of the criminal police and two IT experts have already been appointed for the future cybercrime unit. They have been trained as trainers and should be able to transfer their knowledge to their future colleagues.

At present, the cybercrime unit is not provided with adequate advanced **hard**- and **software** equipment, a need, a future possible extension or follow-up project should take into consideration. As soon as the necessary technical tools are available, the staff will need specialised training to make fully exploit such tools. In this context, targeted study visits by members of the new cybercrime unit to comparable foreign units would enhance efficient international police collaboration and the sharing of experiences and knowledge on best practices to investigate cyber attacks and to deal with digital evidence.

The cybercrime unit should be embedded into a national **strategy** on cybercrime and cyber security. This strategy could be drafted including the expertise of the private IT sector and should aim at protecting the critical cyber infrastructure.

2.4. Output 4: LEA/ISP co-operation

"*Indicator of Result: available policy regarding law enforcement authorities and Internet service provider co-operation in the investigation of cybercrime in line with Georgian legislation and the guidelines adopted at the Council of Europe in April 2008"*

The project achieved full impact under Output 4. Representatives of the Ministry of Justice and ten of the most relevant ISP formally signed a **Memorandum** of Understanding. It is mostly in line with the Council of Europe guidelines and therefore will be one of the corner stones for providing a public-private co-operation, and hence for giving LEA and the judiciary access to the necessary data to effectively fight cybercrime. In order to achieve a profitable cooperation and interaction among LEA and ISP, it is be also advisable to organize regular technical and legal training courses and workshops, not only for the LEA but also for ISP on the new cybercrime legislation and on the new Memorandum, a need also recognized by the Memorandum itself.

2.5. Impact beyond cybercrime

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.

2.6. Sustainability

At the end of the project, the beneficiary should **adopt** the **draft law** implementing the Cybercrime Convention and the draft law on personal data protection as soon as possible. The adoption of both laws by Parliament will be a significant factor for the success of the other outputs. The existence of a domestic legislation on cybercrime in line with the Convention on Cybercrime is a prerequisite for the future development of an effective training strategy, for the implementation of the cybercrime unit (including the 24/7 point of contact) and for the co-operation between LEA and ISP.

For the full achievement of the objective of Output 2, the beneficiary should further adapt the **training material** to the specific Georgian legal and technical structure and apply the “Concept on cybercrime training” on actual trainings.

For a full sustainability of Output 3, the Council of Europe/donors could offer advice and support on obtaining the necessary hard- and software tools for **cybercrime unit** and for a follow-up training on the implementation and use of such new technical tools. Advice on the organisational set-up and the daily practice of the unit also seems recommendable. Study visits by members of the new cybercrime unit to comparable foreign high tech crime units would enhance international co-operation and the sharing of experiences on best practices.

To achieve a broad and strategic co-operation with the **ISP**, the law enforcement agencies and the private/industry sector should organize technical and legal workshops to train the staff of the ISP in charge of the implementation of the cooperation procedures in line with the requirements of personal data protection. Training for ISP and LEA on the new legislation and the new Memorandum would also be recommendable.

Additional outside advice and support would seem a significant factor for the success of the above-mentioned measures, the introduction of cybercrime standards being new to the beneficiary.

3. Project Design

The **project design** answers an urgent need for legal and technical countermeasures against cybercrime and cyber-attacks, such as those happening before the war in 2008. Fortunately, the donor made it possible for the project to be quickly in place by making funds available on very short notice. The project properly addresses the four major needs of Georgia in the fight against cybercrime: legislation, training, institution building, LEA/ISP co-operation. The main objective of the project was the development of proposals for each of these outputs, while direct support for obtaining hard- and software or assistance on IT was not part of the project. This makes sense, as it would have been too early to procure equipment without the beneficiary first having made the necessary steps to provide a legal and organisational framework.

The timeframe, of the project was very tight. Planning a full legislative process from assessing the legislative needs, drafting the law and adopting it in Parliament on such new and complex issues, and then planning further outputs based on the adoption of this legislation in only one year's time seems a bit too ambitious.

The project could have also included under **Output 2** the drafting of a training strategy, which would complement the training policy and which would show, how and within what timeframe all criminal law judges, prosecutors and investigators from all Georgian regions will be trained on cybercrime and digital evidence. Such a comparatively small strategic step would already enhance the sustainability of the training materials' impact.

For future projects containing a corner stone similar to **Output 3**, it could be considered to embed the 24/7 contact point and the cybercrime unit into a national strategy for the security of the information systems and of the critical infrastructure. Future projects should also meet the need on the part of such units for adequate advanced hard- and software equipment in order to investigate with full technical capacity and to co-operate internationally.

The project chose the term "indicators of results" instead of "**indicators of impact**". The "indicators of results" are a description of the activities carried out in each Output. These indicators could have described in more details and point a little further the mere delivery of outputs. More detailed and impact-oriented indicators could provide additional guidance for the implementation of activities. For example, it makes a difference whether the "indicator of result" simply requires "a training policy" being available by the end of the project, or whether an "indicator of impact" will provide specific aims, such as "training policy covering all aspects of investigating and adjudicating cybercrime as initial and in-service training and providing a reasonable timetable on how all officials concerned with cybercrimes will be trained."

All “indicators of results” use only qualitative criteria. **Quantitative** criteria could have been used, such as for Output 1 the percentage of implementation of the Convention on Cybercrime, or for Output 2 the number of people trained as trainers with respect to the amount of staff to be trained in the country.

4. Project Delivery

The project team **delivered** all the outputs in a professional manner and in close co-operation with the EU Delegation in Georgia and beneficiary/counterparts. The **project team** was located in Strasbourg and no long-term advisor was present in Tbilisi; this seems not to have been a substantial problem to the planning and delivery of the project's activities. At the same time, the project team had the opportunity to meet representatives from the Ministries of Justice and Internal Affairs of Georgia each time/when they were in Strasbourg for the Committee of Ministers from the Council of Europe.

All of the **planned activities** of all Outputs were carried out as scheduled with the continuous support and active participation of local EU Delegation. The decision on the part of the project team and of the beneficiary to concentrate efforts on bringing quickly the domestic legal system in line with the Cybercrime Convention through a draft law was reasonable: the implementation of a domestic legislation on cybercrime is necessary for carrying out the activities of the Outputs 2 to 4. In some cases, the project team delivered more activities, than were initially planned, such as a regional workshop on cybercrime focused on strengthening international co-operation in cybercrime investigation.

Independent international experts chosen by the project team of the Council of Europe provided various **technical papers** and **legal advice** that were taken into account by the beneficiary in order to meet the objectives of each output. According to the evaluator and the counterparts, the technical papers have high utility, quality and clarity. All the reports and training material were translated into Georgian to ensure the largest diffusion among the counterparts.

With regard to **trainings**, feedback forms were used with regard to the presentations by trainees, but not with regard to the trainings themselves. The evaluators recommend using standardised feedback forms for all Council of Europe technical assistance trainings.

The private **internet sector** and **NGOs** have been involved in most of the activities, and particularly in the activities carried out under Output 4, contributing significantly to the final signing of the Memorandum of Understanding. Representatives from the academic field were involved in drafting the cybercrime law. Future projects should maintain such an effective cooperation with the private sector, benefiting from its expertise. The support of the private sector and industry could ensure that the staff attending the training courses receives adequate and updated information on the fight against cybercrime.

The **visibility** of the project and of its donors is apparent thanks to project references on the Ministry of Justice of Georgia website on cybercrime and data protection; this visibility is also confirmed by the counterparts interviewed with reportedly wide media coverage on some activities. The project's presentation on the Council of Europe website provides comprehensive information. Funding by the donor is mentioned on all technical papers and on the training material.

There was no need to coordinate the project's activities with other **donors**. All the donors present in Georgia (e.g. GTZ, Sida or USAID) do not fund projects related to cybercrime or data protection. This reflects the forefront Council of Europe position on an international level as far as comprehensive technical assistance projects on cybercrime are concerned: e.g. UNODC delivered a project that covered "only" law enforcement training in EU member and candidate states[2]; USAID apparently funded one cybercrime activity in Indonesia in 2006[3]; OECD concentrates their efforts less on the adjudication of cybercrime, but more on private sector issues of internet[4]. Despite the project team's efforts to coordinate its activities with the US Embassy on a possible donation in the future of equipment for high tech crime unit, such cooperation did not take place.

2 www.unodc.org/unodc/en/frontpage/2009/June/law-enforcement-officers-trained-in-tackling-cybercrime.html.

3 www.usaid.gov/policy/budget/cbj2006/ane/pdf/id_complete06.pdf.

4 www.oecd.org/department/0,3355,en_2649_34255_1_1_1_1_1,00.html.

4.1. External Factors

The Project Document makes assumptions about how external factors support the delivery of the outputs.[5] These assumptions materialised as follows:

Out-put	Assumption	Materialisation
1	Legislation: Draft laws are processed, submitted to and adopted by Parliament.	A draft law on cybercrime and one on personal data protection are ready for adoption by Parliament. A separate draft law on Mutual Legal Assistance in Criminal Matters is not ready for adoption by Parliament yet.
2	Training: Law enforcement and judicial training institutions will make use of the material developed and continue the training. The draft policy will be adopted by the Government and training institutions.	The High School of Justice, the Ministry of Justice and the Police Academy are using, or planning to make use of, the translated material when training staff dealing with cybercrimes. The beneficiary/the project did draft a training policy (see above chapter 2.2).
3	Institution building: The proposals will be adopted and implemented by Government.	The Government formally established a 24/7 point of contact and a cybercrime unit based on the project's proposals, but their practical implementation depends on the adoption of the cybercrime draft law.
4	Law enforcement/ISP co-operation: The code of conduct is adopted by the Ministry of Interior and ISPs	A Memorandum of Understanding ("Principles of Co-operation") between Law Enforcement Agencies and Internet Service Providers was formally adopted by the representative of the Ministry of Interior and the ISPs.

5 Logical Framework (p. 14 ff.).

5. Annexes

5.1. Evaluation Assignment

The Agreement on the Project foresees an evaluation exercise to be carried out. The assessment of the achievements of the Project was the responsibility and assignment of the main evaluator, Ivan Salvadori, who carried out the on-site mission to Strasbourg and Tbilisi. The co-operating evaluator, Tilman Hoppe, provided the main evaluator with advice on the methodology, structure and drafting of the evaluation (report). The evaluation is defined by Council of Europe's Terms of Reference on the "Evaluation of the Project on Cybercrime in Georgia" as follows:

i) Overall Objective

The assignment is to provide an evaluation of the overall project progress from its start in June 2009 to date against the objectives and indicators of achievement as set out in the Annex I ("the Action") of the Agreement, as well as its overall impact.

ii) Specific Objectives

The evaluation should address the following issues:

a) Results and Impact Produced

- Results produced (against the "objectively verifiable indicators" of success),
- Achievement of project objectives (against the "objectively verifiable indicators" of success),
- Actual or likely impact of the project on the legislation and institutions on cybercrime in Georgia,
- Overall impact of assistance provided through the project.

b) Relevance of Project Design

- To what extent was the initial needs assessment relevant to the project structure and design?
- How was it translated into the rationale for specific project objectives and activities?
- Which other inputs could/should have been used at the project design stage?
- To what extent did the project Workplan and calendar of activities take into account the need for possible adjustments?

- How were quantifiable indicators of performance used?

- To what extent did the project address needs of beneficiaries/counterpart institutions?

c) Efficiency/Effectiveness of Implementation

- To what extent have the activities as defined in the original logframe and the Workplans been implemented?

- To what extent were the beneficiaries receptive to the project proposals and assistance provided, and to what extent did they participate in/contribute to the project?

- Activities of which type proved to be most effective throughout the project implementation?

d) Assumptions/Influence of External Factors

- What were the external factors that had a positive/negative influence of the course of project implementation?

- To what extent was the project influenced by them?

- To what extent have the assumptions indicated in the logframe materialised?

e) Sustainability Potential

- What kind of effort will be required from the beneficiaries in order to prolong the project impact after its conclusion? Is it feasible?

- How can the CoE/other donors assist in ensuring the sustainability of impact beyond the project completion date?

f) Relationship With Other Projects/Donor Actions

- How efficient/relevant/visible was the project's placement amongst other actions in the field?

- What were its relationships with other projects?

g) Conclusions and Implications for Future Projects

- What are the overall conclusions regarding this project?

- What lessons can be drawn, what recommendations could be made to the Project Management for future projects/interventions as such?

- Which areas/institutions should be addressed in the future through Technical Assistance or as follow up project?

5.2. Methodology

This report is the result of work carried out in May 2010. The work included:

- Desk review of relevant country background information;
- Available project documents (primarily forwarded by the Council of Europe secretariat in Strasbourg and by the local Project Team in Tbilisi; some information was also taken from the project website);
- A meeting of the main evaluator with representatives of Council of Europe's Economic Crime Division in Strasbourg on 11 May 2010;
- An in-country visit to Tbilisi of the main evaluator from 13 to 14 May 2010 consisting of semi-structured interviews with various beneficiaries and the donors (see Annex 5.3 for list of interviewees); The counterparts of the interviews were chosen by the Project Team and a provisional timetable for the interviews scheduled before the in-country visit;
- E-mail exchanges with the Project Team before and after the completion of the in-country visit;
- E-mail exchange interview with other interviewees.

5.3. Meetings/Interviews

The main evaluator met or interviewed the following persons:

Tuesday, 11 May 2010, Strasbourg
- Mr Alexander Seger, Head of Economic Crime Division, Council of Europe - Ms Cristina Schulman, Head of Cybercrime Unit, Council of Europe - Ms Lucile Sengler, Assistant Project Officer, Council of Europe
Thursday, 13 May 2010, Tbilisi
- Ms Rusudan Mikhelidze, Deputy Head of Analytical Department, Head of Research and Analysis Unit, Ministry of Justice - Mr Shalva Kvinikhidze, Head of International relations main Division, Ministry of Internal Affairs of Georgia - Participation at the Regional Workshop on Cybercrime
Friday, 14 May 2010, Tbilisi
- Ms Rusudan Mikhelidze, Deputy Head of Analytical Department, Head of Research and Analysis Unit, Ministry of Justice - Mr Shalva Kvinikhidze, Head of International relations main Division, Ministry of Internal Affairs of Georgia - Mr Nika Kabakhidze, Detective of Criminal Police Department, MIA Georgia - Mr Shota Rukhadze, Deputy Director of the High School of Justice of Georgia - Ms Ketevan Khutsishvili, Project manager, Delegation of the European Union to Georgia and Armenia - Mr Nigel Jones, UK, CoE consultant - Participation at the Project Closing Conference
Email Interviews
- Mr Emilio Aced Felez, Spain, CoE consultant

5.4. Reports, Technical Papers and other Documents

The main evaluator reviewed all of the following documents; the co-operating evaluator reviewed only the key documents:

Project-Documents (as provided by Council of Europe)
Agreement between the European Union and The Council of Europe (April 2009)
Report on the activities carried out between 1 June 2009 and 27 September 2009
Report on participant training delivery (Tbilisi, 13-14 May 2010)
Questionnaire on institutionalising cybercrime training for judges and prosecutors (28 August 2009)
Project on Cybercrime in Georgia, Work Plan 2009-2010 (10 May 2010)
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)
Technical Papers
Analysis of the cybercrime legislation of Georgia against the provisions of the Convention on Cybercrime of the Council of Europe, Prof. Henrik W.K. Kaspersen, August 2009 (Output 1)
Report on the Data Protection Legislation of Georgia, Emilio Aced Félez, Spain, September 2009 (Output 1)
Comments on Georgian Draft Law implementing the Cybercrime Convention, Prof. Dr. Henrik W.K. Kaspersen, Netherlands, March 2010 (Output 1)
Second Report on the Draft Law on Personal Data Protection of the Republic of Georgia, Emilio Aced Félez, Spain, March 2010 (Output 1)
Various Training Material (Output 2)
Proposals for the establishment of a High Tech Crime Unit, Nigel Jones, United Kingdom, and Virgil Spiridon, Romania, September 2009 (Output 3)
Guidelines for the co-operation between law enforcement and Internet Service providers against cybercrime, Council of Europe, April 2009, (Output 4)
Cybercrime training for judges and prosecutors: a concept, Council of Europe, October 2009 (Output 2)
Presentations
Closing Conference on Cybercrime (14 May 2010)
Cristina Schulman: Overview on the project achievements
Rusudan Mikhelidze: CoE/EU Project on Cybercrime in Georgia

Regional Workshop on Cybercrime (13 May 2010)
Wout de Natris: Spam fighting in the Netherlands
Eirik Tronnes Hansen: The experience of Norway in fighting cybercrime
César Lorenzana Gonzalez: The experience of Spain in fighting cybercrime
Bilal Sen: The experience of Turkey in fighting cybercrime
Wout de Natris: Law enforcement and co-operation
Graham Sutton: Data protection and cybercrime investigations
Markko Künnapu: Strategies for enhancing cyber security
Conference on Cybercrime (2 March 2010)
Prof. Dr W.K Henrik Kaspersen: Challenges in implementing the Convention on Cybercrime and progress made by Georgia
Virgil Spiridon: Investigating cybercrime: lessons learnt and recommendations (Romania experience)
Worskhop on law enforcement authorities and Internet service providers cooperation (2 March 2010)
Cristina Schulman: The CoE Guidelines for the cooperation between law enforcement and Internet service providers against cybercrime
Uwe Manuel Rasmussen: Investigation of computer crimes and the role of service providers
Virgil Spiridon: LEA-ISP cooperation: examples of good practices
Workshop on cybercrime and data protection legislation (29 September 2009)
Uwe Manuel Rasmussen: Challenges of fighting cybercrime and using digital evidence
Nigel Jones and Virgil Spiridon: Proposals for the establishment of a High Tech Crime Unit in Georgia
Prof. Dr W.K Henrik Kaspersen: Analysis of the cybercrime legislation of Georgia against the provisions of the Convention on Cybercrime
Emilio Aced Félez: Analysis of the data protection legislation of Georgia
Round table discussion on High Tech Crime unit (28 September 2009)
Nigel Jones and Virgil Spiridon: Proposals for the establishment of a High Tech Crime unit in Georgia
Virgil Spiridon: Practical examples of investigating cybercrime

Workshop on cybercrime legislation (16 July 2009)
Markko Künnapu: Estonian experience against cybercrime
Virgil Spiridon: Challenges in investigating cybercrime
Givi Baghdavadze: International cooperation provisions in Georgia
Cristina Schulman: Council of Europe Convention on cybercrime and the advantages for Georgia to become Party to the Convention
Cristina Schulman: Council of Europe Convention on cybercrime and national implementation
Round table on the creation of a 24/7 contact point and a high tech crime unit in Georgia (15 July 2009)
Markko Künnapu: 24/7 network and contact points
Virgil Spiridon: The Cybercrime police unit of Romania
Miscellaneous
Minutes 1st Steering Group Meeting 28 September 2009
Minutes 2nd Steering Group Meeting 1 March 2010
Project Budget
Financial Report (as of 31 March 2010)