Cybercrime@EAP

EU/COE Eastern Partnership Facility

# Assessment report

## Criminal justice capacities on cybercrime and electronic evidence in the Eastern Partnership region

## Results of the peer-to-peer assessments under the CyberCrime@EAP project

Adopted at the CyberCrime@EAP Conference on Strategic Priorities

Kyiv, 29/30 November 2013

**www.coe.int/cybercrime**

Strasbourg, version 8 March 2014

Funded by the European Union

EUROPEAN UNION

COUNCIL OF EUROPE

CONSEIL DE L'EUROPE

Implemented by the Council of Europe

**CONTACT**

Data Protection and Cybercrime Division
Directorate General of Human Rights and Rule of Law
Council of Europe, F-67075 Strasbourg Cedex (France)

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

# Contents

# 1 Introduction

The present report provides a brief assessment of the capacity of Eastern Partnership countries to cooperate against cybercrime.

During a summit with Eastern European countries (Prague, 7 May 2009), the European Union launched the Eastern Partnership with the goal of enhancing cooperation with Armenia, Azerbaijan, Belarus, Georgia, the Republic of Moldova and Ukraine, through both bilateral and multilateral dimensions. The Council of Europe supports this initiative through the Europe Eastern Partnership Facility[1] which was launched in March 2011. CyberCrime@EAP is one of four projects funded by the European Union under this Facility.

Between March 2011 and March 2013, CyberCrime@EAP supported participating countries in the following fields:

- Raising awareness among decision-makers and help them determine strategic priorities regarding cybercrime and electronic evidence;
- Strengthening legislation based on the Budapest Convention on Cybercrime;
- Encouraging the creation of specialised cybercrime units;
- Judicial and law enforcement training on cybercrime and electronic evidence;
- Law enforcement – Internet service provider cooperation in the investigation of cybercrime;
- International cooperation, including judicial and police cooperation and strengthening of 24/7 points of contact;
- Promoting financial investigations to prevent and control money laundering and to search, seize and confiscate crime proceeds on the Internet.

The methodology of the project included the preparation of a Situation Report comprising an initial assessment of the fields covered by the project (legislation, specialised units, judicial and law enforcement training, law enforcement/ISP cooperation, international cooperation and financial investigations). The draft situation report had been prepared by December 2011 and finalised by April 2012.

The Situation Report and the delivery of project activities were then followed by country visits for peer-to-peer assessments. These visits to Armenia, Belarus, Georgia, the Republic of Moldova and Ukraine took place in March/April 2013. The assessment process involved conducting interviews with relevant teams in each area in order to establish progress made against previous recommendations and to obtain an update on project progress overall. In each project area, in addition to meetings organised with the project teams responsible for the implementation of the project, a number of institutions were visited, including Ministry of Justice, prosecution services, high-tech crime units (including 24/7 point of contact), financial intelligence and/or investigation units, judicial training institutions, and law enforcement training institutions.

The present Assessment Report summarises the results of these visit and updates the earlier Situation Report. It also takes into account other project reports as well as reports of the Cybercrime Convention Committee (T-CY) and of MONEYVAL with respect to financial investigations.[2]

The Assessment Report in turn informed "strategic priorities on cybercrime" which – together with this report – were adopted in the CyberCrime@EAP Conference on 30-31 October 2013 in Kyiv, Ukraine.[3]

---

[1] http://www.coe.int/t/dgap/eap-facility/

[2] www.coe.int/tcy and www.coe.int/moneyval

[3] The Strategic Priorities are attached in the Appendix.

**CyberCrime@EAP Project Summary**

| | |
|---|---|
| Project title | CyberCrime@EAP joint EU/COE Joint Project on Regional Cooperation against Cybercrime in Eastern Partnership countries |
| Area | Armenia, Azerbaijan, Belarus, Georgia, Republic of Moldova, and Ukraine |
| Duration | 1 March 2011 – 31 December 2014[4] |
| Budget | EUR 894,000 |
| Funding | European Union |
| Overall objective of CoE Facility | To enhance the reform processes in the six partner countries through a multilateral approach and to bring them closer to Council of Europe and EU standards in core areas covered by the Eastern Partnership Platform 1. |
| Specific project objective | To strengthen the capacities of criminal justice authorities of Eastern Partnership countries to cooperate effectively against cybercrime in line with European and international instruments and practices |
| Result 1 | Eastern Partnership countries have defined strategic priorities regarding cybercrime and assessed measures taken |
| 1.1<br>1.2<br>1.3 | Regional conference (launching event of the project) on effective measures against cybercrime<br>Regional conference on strategic priorities regarding cybercrime<br>Regional conference on the assessment of progress made (closing event of the project) |
| Result 2 | Eastern Partnership countries are provided with the tools for action against cybercrime |
| 2.1<br>2.2<br>2.3<br>2.4<br>2.5<br>2.6<br>2.7 | Regional seminar on cybercrime legislation<br>Regional seminar on specialised cybercrime units (high-tech crime, cyberforensics, prosecution services)<br>Regional seminar on judicial and law enforcement training<br>Regional seminar on law enforcement – ISP cooperation<br>Regional seminar on international cooperation against cybercrime<br>Regional seminar on financial investigations<br>Peer-to-peer assessment and advisory visits to each Eastern Partnership country |
| Result 3 | Eastern Partnership countries participate more actively in international cybercrime efforts |
| 3.1 | Support the participation of Eastern Partnership countries in international activities against cybercrime (Octopus conferences, G8 training events for 24/7 points of contact, Internet Governance Forum and others) |

[4] The Eastern Partnership Facility was to end on 31 August 2013 but was extended to 31 December 2014 with limited additional funding.

# 2 Armenia

## 2.1 The threat of cybercrime

### 2.1.1 The situation

At the outset of the project, Armenia identified the following areas of cybercrime as being an issue. No statistical information was provided to allow for analysis of the overall effect of the illegal activities or the impact on the capabilities for investigation and prosecution:

- Hacking attacks on websites and other resources in the Armenian segment of the Internet;
- Embezzlement and distribution of personal data;
- Development, use and distribution of malware;
- Distribution of pornography in the Internet;
- Misappropriation of computer data;
- Fraud by means of computer devices;
- Illegal enterprise providing telecommunications services.

### 2.1.2 Assessment and summary of progress made

The high-tech crime unit of the Organised Crime Department indicated the following:

- In 2011, 15 cases resulted in criminal proceedings (misappropriation of computer data and malware use);
- In 2012, 30 cases resulted in criminal proceedings (distribution of pornography, misappropriation of computer data and malware use);
- In 2013, 45 criminal cases had been investigated by October.

Armenia reports that there are a lack of appropriate hardware and gaps in laws. They are actively taking steps to correct these gaps. Cybercrime, along with trafficking and migration are on the highest level of priority for the Armenian Police.

## 2.2 Legislation

### 2.2.1 The situation

Armenia ratified the Budapest Convention (CETS 185) and its Additional Protocol (CETS 189) on 12 October 2006. No reservations were made in this respect. Armenia signed the Convention on the Protection of Children against Sexual Exploitation and Sexual Abuse (CETS 201) on 29 September 2010 but has not ratified it yet.

Armenia is considering the enactment of a new Criminal Code and a new Criminal Procedure Code. The CPC is to enter into force in the beginning of 2014.

The legislation largely complies with the provisions of the Budapest Convention. Most definitions of the Convention can be found in article 251 ff. of the Armenian Criminal Code. Some domestic provisions may go beyond the scope of the Convention, while others may be too restrictive (e.g. notion of illegal access, article 251 ArCC). Other provisions may need to be clarified (e.g. illegal interception, article 254).

Many procedural tools are already implemented in domestic law. The Situation Report (December 2011) identified some gaps, including regarding search and seizure, the collection of traffic data and the interception of e-communications. Changes in the Electronic Communications Act are also still needed to keep up with improvements regarding data preservation.

The Armenian police outline the importance of appropriate legislation to address cybercrime and to facilitate cooperation with the private sector in the investigation of cybercrime.

The analysis of the legislation identified the need for a review of Armenian criminal and criminal procedural law, specifically regarding:

- Application of correct and consistent definitions, preferably as part of the law, both concerning substantive law, as well as procedural law.
- Review of Articles 251-254 ArCC.
- Critical review of Article 263 ArCC, as well in view of implementing the Lanzarote Convention.
- Apply corporate liability to any applicable crime or, as a minimum, to the crimes related to Articles 2-11 of the Convention.
- Implement specific provisions in accordance with Articles 16 and 17 of the Convention enable expedited application of these powers.
- Enact specific provisions concerning Articles 18 and 19 dealing with all additional powers and taking into account the specific qualities of computer systems and data.
- Enact specific provisions concerning the collection of traffic data and the interception of e-communications taking into account the special role of service providers and the technical requirements for the execution of such powers.

### 2.2.2 Assessment and summary of progress made

A working group has been established to bring Armenian legislation in line with the Budapest Convention. It works in close cooperation with the Organization for Security and Cooperation in Europe (OSCE) in Yerevan.

Specific support was provided to Armenia on strengthening cybercrime legislation. A roundtable (Yerevan, 25 April 2012) reviewed the Armenian cybercrime legislation. A study visit to Lisbon, Portugal, in December 2012 provided the Armenian authorities with knowledge and experience in the implementation of the Budapest Convention (Portugal represents a good example). It is expected that the current review will finalise the proposals for new legislation.

Amendments are also desirable in view of the full implementation of Article 15 on conditions and safeguards. Specific procedural law provisions should be enacted in order to enhance conditions and safeguards, especially regarding powers under articles 16, 17 and 18[5].

The Assessment Report of the Cybercrime Convention Committee (T-CY) on expedited preservation (December 2012) confirmed the importance of amending, in cooperation with the Council of Europe, the legislation governing preservation orders and corresponding provisions on mutual assistance[6]. Among other things, powers under article 16 need to be implemented to allow for more expeditious action.

The new CPC is to enter into force in the beginning of 2014 and is to include specific provisions for preservation and other powers.

[5] See CyberCrime@EAP draft discussion paper on "Article 15 – Safeguards in the Eastern Partnership region" (version 11 June 2013), p.18 ff.

[6] See the Cybercrime Convention Committee Assessment Report (December 2012), available at http://www.coe.int/t/dghl/cooperation/economiccrime/cybercrime/T-CY/TCY2013/TCYreports/TCY_2012_10_Assess_report_v30_public.pdf

Recommendations for consideration by the Armenian authorities include the following:

- Amending the legislation in line with the recommendations made in the Situation Report on legislation drafted during the project as well as with The Assessment Report of the Cybercrime Convention Committee (T-CY) on expedited preservation (December 2012).
- Reviewing special investigative measures (legal restrictions, safeguards and conditions etc.)

## 2.3 Specialised institutions

### 2.3.1 The situation

Armenia has specialised units within the State Security Service and the Police's Organized Crime Department ("OCD"). The police are in charge of most of the cases, pursuant to the Criminal Procedure Code. They report cases to the specialised prosecutors, who then take prosecutorial action and defend the cases in the court. No specialised local units have been set up. Where necessary, additional resources of the Police's Organized Crime Department are used.

Specialised units collect and process digital evidence. In the absence of dedicated laboratories within the Police, specialised centres (esp. the non-profit National Bureau of Expert Evaluation) perform expert evaluations and process electronic evidence when needed — by means of licensed software and hardware complying with international standards. Since no specialised equipment is at the disposal of the cybercrime unit, Encase forensic software as well as some other hardware and software are to be purchased with the support of the US Embassy in Armenia.

Eight staff work within the OCD's specialised unit. Their background (mainly Master's degree) and hierarchical level varies. A training course for first responders to cybercrime is in preparation and will soon be available.

The State Security Service cooperates with foreign authorities on the basis of interstate agreements. It dealt with 10 cases and requests in 2010. The Police OCD's hi-tech crime unit operates on the basis of interstate agreements, as well as 24/7 G-8, Interpol, and the 24/7 contact points under the Budapest Convention.

The main challenges faced by the high-tech crime unit fall into the following categories:

- External factors: Ability to receive information from certain servers outside Armenia and to interact with 24/7 contact points of certain countries.
- Internal factors: Discrepancies in Armenian law (e.g. between the scope of the Law on Operational and Search Activities and the Criminal Code).
- No specialised equipment or software in use by the specialised unit.

### 2.3.2 Assessment and summary of progress made

The Cybercrime@EAP project has had a positive impact on Armenia's capacity to fight cybercrime. This is exemplified by the decisive role that the project played in the creation of a specialised department (renamed in April 2012) within the Office of the Prosecutor General. By providing for specialised expertise, the project also empowered the staff to deal with cybercrime offences.

In collaboration with the private sector, new training schemes are being developed (in particular, in the field of live data forensics) for the police staff. Armenia stressed that additional training workshops, including with the support of the Council of Europe, would be most welcomed.

Within the framework of an "electronic society" initiative launched in 2012, the National Security Service and the Police work closely to improve the protection of critical national infrastructures.

Overall, interagency cooperation between the Police, the Prosecutor General and the National Security Service seems to be very effective.

Issues for consideration by the Armenian authorities include the following:

- Reviewing special investigative measures (legal restrictions);
- Reviewing electronic evidence (methodology; staff involved);
- Strengthening of the prosecution services (local specialised prosecutors; increase of specialised staff within the Prosecutor General's Office);
- Creating a Computer Emergency Response Team (CERT) in Armenia.

## 2.4 International cooperation

### 2.4.1 The situation

Mutual assistance requests are governed by article 499-6 of the Criminal Procedure Code. The competent authority is the General Prosecutor's Office. The 24/7 contact point is established within the Division for Fighting against High Tech Crimes, and has no competence to send or receive mutual assistance requests.

Police-to-police cooperation is conducted by using 24/7 networks.

The main obstacle to cooperation was seen as being an insufficient legal basis in this field. The procedure for law enforcement to obtain traffic, subscriber and content information from ISPs is regulated by the Law on Operational and Search Activities. The law establishes that such action belongs to the category "monitoring of telephone communication"; it requires a court order based on request of the head of the authority or the head of the separate unit. There were no specific contact points nominated by law enforcement and ISPs.

### 2.4.2 Assessment and summary of progress made

In 2010-2011, the 24/7 contact point handled 52 requests for assistance and received 32 requests. In both ways, traffic data is the type of data most commonly sought. Around 50 requests are received each year. In 2013 (by October), 60 requests had been dealt with.

Armenia cooperates actively with the OSCE office in Yerevan as well as the US Embassy, which formally assisted the country and provided for equipment.

Whilst international cooperation is successful in some instances (e.g. with the Netherlands in one case mentioned), the Situation Report identified various obstacles faced by Armenia:

- Discrepancies between legal systems;
- Lack of replies from requested countries (esp. non-Parties to the Budapest Convention);
- Lack of information on the foreign competent authority;
- Difficulty to cooperate with certain ISPs (e.g. Google).

In its replies to the T-CY Questionnaire on international cooperation, Armenia urged for a simplification of cooperation schemes. Armenia's experience with the USA illustrates that LEA should be able to obtain expeditiously subscriber information (IP addresses) without an MLA request.

## 2.5 Law enforcement training

### 2.5.1 The situation

Prospective police officers are mainly educated in institutions of higher education; police officers are educated at the Police Academy of Armenia. In-service training and qualification upgrades are provided by the Police Academy, the Police Training Centre, Research and Training Centre of the National Security Service of Armenia.

The Situation Report emphasised that Armenia needed a national training strategy, as well as methodical guidelines on the fight against cybercrime and the collection of digital evidence.

No national training strategy on cybercrime has been adopted so far. A methodology of training and professional upgrade is under development, even though the training centre responsible for this training has still to be determined. Newly enrolled staffs already receive practical training on the handling of electronic devices that may contain evidence. Thanks to the support of the OSCE, the Police Training Centre now has an equipped training room for new recruits. In-service training on cybercrime is also in place at the Police Training Centre. No training is available for investigators on the use of open source research or covert activities.

The staff receives additional training at the International Law Enforcement Academy (ILEA) in Budapest, the Qualification Upgrade Institute of the Ministry of Interior of Russia and the Cisco Networking Academy. Specialised training will be organised soon with the assistance of the Internet Association (ISOC) and Microsoft. No information was provided regarding possible arrangements with academic bodies.

### 2.5.2 Assessment and summary of progress made

Armenia is willing to improve the training of law enforcement officers in the regions. For this purpose, an Armenian (territorial) officer took part in the training course organised by the Council of Europe in Oslo. Building on the CoE template, Armenia has already taken steps to consolidate the training with the assistance of the Police Academy. Activities under development include:

- A basic training course on computer systems, networks and electronic evidence, as well as search and seizure,
- A guide on search and seizure.

The national cybercrime unit will train the staff recently set in the regions during one month, with the help of a dedicated guide.

Joint training with Georgia on specific issues is under consideration. More generally, Armenia's authorities support the organisation of training courses, seminars, and activities to share experiences with all criminal justice stakeholders and with foreign counterparts.

## 2.6 Judicial training

### 2.6.1 The situation

Until recently, the organisations responsible for training judges and prosecutors in Armenia were the Judicial School of the Republic of Armenia and the Prosecutors School of the Republic of Armenia. Both were recently dissolved and a new joint academy for prosecutors and judges was created. This academy will operate from 2014.

As the Situation Report (2011) highlighted, no documented training strategy for judges and prosecutors has been adopted on cybercrime investigation and digital evidence – neither for initial

nor for in-service training. There are no arrangements with the academia or the private sector to support such training.

For these reasons, practical seminars, conferences and joint training activities with other countries would be desirable, particularly to identify procedural difficulties and exchange experience with cybercrime investigators and digital forensics specialists.

### 2.6.2 Assessment and summary of progress made

The Prosecutor General's Office has developed important materials on cybercrime and international cooperation, included in a guide prepared for prosecutors. The Office has also delivered training courses on electronic evidence at the School of Prosecutors, where all prosecutors have training twice a year. This training will possibly be included in the initial training.

On 7-8 August 2013, the General Prosecutor's Office of Armenia – with the assistance of the US Embassy – held a conference on cybercrime. Participants included also prosecutors of the Republic of Armenia.

## 2.7 LEA/ISP cooperation

### 2.7.1 The situation

As the Situation Report highlighted, cooperation between LEA and ISPs seems to be mainly hindered by the insufficient legal framework in this field. Until a very recent time, the cooperation was indeed only based on goodwill (see below). It was recommended that ISPs be licensed to provide the required services and take on responsibilities – especially for the retention of data.

The Internet Community Ltd. is the main body responsible for the administration of domain names in Armenia's segment of the Internet. Until recently, ISPs licenses were issued in Armenia by the Public Services Regulation Commission. The types of licenses available were as follows:

- License to use radio frequencies;
- License to operate public telecommunication networks (68 companies licensed);
- License for voice communication services (58 companies);
- License to transmit data and provide Internet access (70 companies).

However, following a recent decision by the Public Services Regulation Commission, licenses are no longer required for data transmission and Internet access services.

The Law on Operational and Search Activities regulates the procedure for the law enforcement to obtain traffic, subscriber and content information from ISPs. It requires a court order, based on a request of the head of the authority or of the specific unit concerned. For the time being, ISPs are not required to retain data. A law on this matter is being developed.

No specific contact points have been designated by law enforcement and ISPs for their communications. Cooperation arrangements are in place between the State Security Service and the Internet community, although no details of this were provided in the Situation Report. There are no such arrangements with the police.

There are no joint training programmes in place for law enforcement and ISPs.

### 2.7.2 Assessment and summary of progress made

It is expected that the new Criminal Procedure Code and the Electronic Communications Law will improve the situation. Pursuant to the Law on Operational and Search Activities and the Electronic

Communications Act, ISPs are now legally required to enable the MSS and Police to 'capture' and intercept data. A party may object to the measures taken at a later stage. The data obtained on the basis of a court order is classified: the ISP is not informed of its content and the approval of the issuing authority is required to use the data in court. Non-useful information is destroyed, under the responsibility of the interceptor and the court issuing the order.

Under Expected results 2, the project supports measures to strengthen cooperation between law enforcement authorities and Internet service providers. A Roundtable organised in Yerevan in April 2012 reviewed the current state of LEA and ISPs cooperation in Armenia and the feasibility of concluding cooperation agreements based on the Council of Europe Guidelines for the cooperation between law enforcement and internet service providers against cybercrime (2008)[7]. Several gaps have been identified in the Armenian legislation in the implementation of the Cybercrime Convention, including the lack of definitions of the terms "service provider" and "traffic data". The meeting discussed in detail with the participants the relevant procedural provisions (Article 16-21) of the Budapest Convention and their implementation at the domestic level.

In order to develop cooperation patterns, Armenia plans to build on the Memorandum of Understanding developed in Georgia with the assistance of the Council of Europe.

## 2.8 Financial investigations

### 2.8.1 The situation

Financial investigations are the responsibility of the Police of Armenia, the State Security Service, the State Proceeds Committee, and the General Prosecutor's Office. The same bodies are responsible for asset seizure and the confiscation of proceeds of crimes committed on the Internet. The Central Bank of Armenia, its Finance Monitoring Centre (Armenia's Financial Intelligence Unit) and commercial banks are also involved in activities on this matter.

The Situation Report of 2011 identified several types of fraud and other offences on the Internet that involve crime proceeds: embezzlement of bank cards details; embezzlement of funds from bank accounts; use of e-purses to cash money; Internet fraud, in particular, sexual services, sale of various goods and services, etc.

Low supervision, low levels of awareness and identification of users are considered the main problems for the prevention and control of criminal money flows on the Internet.

The following are mentioned as examples of interagency cooperation in relation to this activity:

- Activities of the inter-agency commission to fight counterfeiting, embezzlement of bank cards and other payment instruments, money laundering and financing of terrorism;
- Cooperation between the Finance Monitoring Centre (Central Bank of Armenia) and the police, based on a written Memorandum of understanding.

Armenia made considerable improvements in its AML/CFT framework in a relatively short timeframe, particularly by replacing a first AML/CFT law enacted in 2005, with a more comprehensive law passed in 2008. In its Mutual Evaluation report[8] of 22 December 2009 on Armenia, the MONEYVAL Committee considered the FIU (the Financial Monitoring Centre) as a young though very knowledgeable and active FIU. The report also stressed that the FIU was understaffed.

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

[8] MONEYVAL reports are available at: http://www.coe.int/t/dghl/monitoring/moneyval/

### 2.8.2 Assessment and summary of progress made

The new Criminal Procedure Code has strengthened capacities in terms of financial investigations. The supervising role of the Prosecutor General for all actions of law enforcement also favours interagency cooperation and effective investigations.

Armenia's FIU began to cooperate with the Prosecutor General and the Ministry of State Security to develop a common database. The same department of the Prosecutor General's Office manages both the FIU and cybercrime units, hence favouring inter-agency action against illegal money flows on the Internet.

The MONEYVAL Report of 2009 considered the creation of an Interagency Commission as a boost for the coordination among the various AML/FT authorities. Since the adoption of this report, the Interagency Commission has approved an AML/CFT National Strategy for 2010-2013. A draft package on amendments in 17 laws was discussed and introduced to the Government in 2010. It is expected that the Government will further it to the National Assembly (Parliament) shortly.

As financial crimes on the Internet commonly have an international character, it should be recalled that international cooperation between the various states and organisations involved is of prime importance.

## 2.9 Progress made against previous recommendations

| **Cybercrime situation report March 2011** | **Progress reported** |
|---|---|
| Collection of statistics that would provide an insight in the seriousness of cybercrime in the national territory. Such statistics could e.g. concern the number of victims, the number of cases reported to the police, the number of cases prosecuted and the relevant criminal provisions. Such statistics could also provide information about the modus operandi applied in those cases for internal police use only. | Completed as statistics are collated centrally by the Information Centre |
| Consideration of the formation of specific prosecution unit to combat cybercrime in accordance with the needs of the country. As a minimum requirement, it is necessary for a selected number of prosecutors within Armenia to become specialised in cybercrime prosecutions. | Completed – Prosecutors Dept. now has a cybercrime unit |
| Review of national criminal law and criminal procedural law in the domain of cybercrime taking into account the observations made in the country report. | Completed – The current review will finalise the proposals for new legislation |
| Development of a cybercrime training strategy for law enforcement incorporating the requirements of cybercrime investigators, digital forensics examiners and mainstream law enforcement staff relating to their role specific functions. This should include the development of individual training, education and continuous professional development programmes for the specialist cybercrime investigators. | Partially Completed. Further work needed to bring training into the mainstream programme |
| Development of a cybercrime training strategy for judges and prosecutors that will include training at the initial and in service levels and specific advanced training for selected individuals and roles within the Criminal Justice System. Utilise the concept paper developed by the Council of Europe and the Lisbon Network on training for judges and prosecutors. | Partially Completed. Further work needed to bring training into the mainstream programme |
| Develop a framework for improved cooperation between law enforcement and Internet Service Providers using as a model, the "Guidelines for Cooperation between Law Enforcement and Internet Service Providers against Cybercrime" | Partially Completed – Plans to use the Georgian example as |

| | |
|---|---|
| developed by the Council of Europe under the global Project on Cybercrime. | a template |
| Improve capability to combat illegal money flows on the Internet by adoption of the relevant findings of the Council of Europe typology study "Criminal money flows on the Internet: methods, trends and multi-stakeholder counteraction" | Completed |
| Incorporate good practice in the handling of electronic evidence in criminal investigations; examining existing guides such as those developed by Interpol and Europol. | Partially Completed |
| Engage with regional partners in an analysis of the issues adversely affecting international cooperation in cybercrime investigations and make recommendations for improvements, including methods for improving direct contact between law enforcement investigators. | Partially Completed |

## 2.10 New recommendations

1. Continuing the ongoing harmonisation of legislation with the Budapest Convention with the assistance of the Council of Europe and the OSCE.

2. Developing international cooperation with foreign countries, including by sharing best practices.

3. Organising further study visits abroad.

4. Developing training for the judiciary.

5. Continuing the ongoing process of incorporating cybercrime training into the mainstream training delivered by the Police Academy.

6. Continuing the ongoing development of the Memorandum of Understanding for LEA/ISP cooperation, based on the Georgian model.

7. Developing cooperation with the private sector.

# 3 Belarus

## 3.1 The threat of cybercrime

### 3.1.1 The situation

At the outset of the project, the National Security Concept of Belarus of 2010 mentioned several threats facing the ICT field:

- Rise of crime using ICT technology within Belarus;
- Unauthorised access from outside to the information resources of Belarus that harm its national interests;
- Insufficient safety arrangements protecting the vital information facilities.

As indicated in the Situation Report of December 2011, the overall number of computer-related crimes registered was increasing (334 in 2006; 1,614 in 2008; 2,514 in 2010).

Embezzlement via computer systems is the most common form of cybercrime committed in Belarus (approx. 90% of cybercrime acts). This form of crime –1,000 to 1,500 per year on average – is expected to keep rising in the next years.

Unauthorised access, alteration or misappropriation of computer data as well as distribution of malware amount to respectively 3% and 1% of the total numbers of cybercrime offences. So-called telecom crimes (e.g. roaming fraud, illegal provision of telecom services) are not a widespread phenomenon at the moment.

As regards acts against national interests, the Ministry of State Security reported that attacks against government institutions and activities of cyber-espionage are severely affecting Belarus.

### 3.1.2 Assessment and summary of progress made

Certain criminal behaviours have evolved: skimming, illegal online payments and the production of false cards have now replaced the online use of stolen credit card as a popular criminal activity. As a response, additional steps have been taken to secure ATM payments. A group of experts has been established under the auspices of the National Bank. It has already developed recommendations on the use of online payments systems – for instance, making test transactions for online purchases.

Another significant initiative led to the creation of an investigation committee in 2011, bringing together investigators from the Ministry of Interior, officers of the Ministry of State Security, administrators and prosecutors. It has already positively impacted on inter-agency cooperation in the fight against cybercrime. Further developments may lead to the creation of a Computer Emergency Response Team (CERT) to strengthen the protection of critical national infrastructures.

In June 2012, the CERT.BY was created as the National Computer Emergency Response Team of the Belarus. The main task of the Team is to reduce the level of the informational security threats of the national segment of the Internet. CERT.BY carries out accumulation, storage and handling of statistical data related to malware dissemination and network attacks on the territory of the Republic of Belarus, as well as incidents response in the informational systems of the state bodies and organizations so as in the informational systems of the subjects of the national segment of the Internet that addressed to the Team independently.

International cooperation can raise challenges, and there are cases where the information sought cannot be obtained by Belarus from the requested country.

## 3.2 Legislation

### 3.2.1 The situation

Belarus is not a member State of the Council of Europe. Participation by Belarus in CyberCrime@EAP and other projects may facilitate a request to accede to the Budapest Convention in the future.

Requirements of articles 1 to 6 of the Budapest Convention are addressed in Belarus' Criminal Code (Title XII). Certain definitions are also included in the Law on Informat(izat)ion and Protection of Information (2008), although its application to criminal matters is unclear. Draft laws, including possible amendments of criminal substantive and procedural law, are in preparation.

Belarus has set a mechanism of data retention pursuant to Decree of 1 February 2010, No. 60. The same Decree authorises the disclosure of data at the request of LEA, prosecutors and other competent authorities. A Decree of 3 March 2010 regulates the cooperation between LEA and ISPs.

The Situation Report of 2011 recommended with regard to substantive law:

- Specific attention to be given to the implementation of the definitions (also in relation with the procedural provisions).
- Correct implementation of Articles 2, 6 and 9 of the Convention.
- Implementation of Article 12 (corporate liability).
- Review of other provisions according to thr observations made.

With regard to procedural law:

- Implementation of Article 15 (Conditions and safeguards) of the Cybercrime Convention.
- Implement preliminary measures. The applied system of data retention does not take away the need to avail over a power of Article 16 of the Convention.
- Implement Article 18 of the Convention.
- Fully implement Article 19 and review to what extent these powers can be executed in an expedited manner.
- Article 20 is not implemented, because of the system of data retention. It is not clear to which kind of service providers that system applies. Apart from the applied definitions, it remains a need for a power as provided by Article 20.
- The scope and praxis around implementation of Article 21 could not be evaluated on the basis of the information provided.

### 3.2.2 Assessment and summary of progress made

The authorities of Belarus consider that the current legal framework allows Belarus to address cybercrime in all its aspects. However, ongoing reforms under consideration include a plan to amend Belarus' legislation on unauthorised access and the drafting of a new law to govern the use of electronic evidence in criminal proceedings.

It is understood that draft laws to amend the Criminal Procedure Code are in preparation but that this process may take up to two years.

Recommendations to improve the legal framework:

- As the Situation Report (December 2011) identified several gaps in domestic substantive legislation certain provisions would need to be amended or expanded, especially where

the threshold set by the Convention is not reached (e.g. provisions on misuse of devices of Article 6 Budapest Convention).

- Criminal liability of legal persons would also benefit from further review so as to establish a clear legal framework applying to corporate liability; provisions going beyond the Convention's standards (e.g. breach of operation rules of ICT-systems) should also need to be reconsidered.

- Belarus would in particular require more specific procedural powers as set out in Articles 16 to 19 Budapest Convention. Such powers should then be subject to conditions and safeguards as foreseen in Article 15 Budapest Convention.

## 3.3 Specialised institutions

### 3.3.1 The situation

A specialised cybercrime unit was established in 2002 within the Ministry of Interior (the "K" Department). It collects information on a wide range of cybercrime acts and hands over the materials to the units of the Investigative Committee of the Republic of Belarus (department on investigation of crimes against information security and intellectual property of Main Investigative Department of Investigative Committee of the Republic of Belarus). Upon completion of the investigation, the case is transmitted to the supervising prosecution office before the possible initiation of criminal proceedings.

In 2000, an independent IT security unit (ITSU) was established within the State Security Committee of Belarus. It deals with offences against state information systems and transmits cases to the department on investigation of crimes against information security and intellectual property of Main Investigative Department of Investigative Committee of the Republic of Belarus. Criminal proceedings may follow.

The Prosecution office has prosecutors to deal with acts of cybercrime. Two prosecutors within the Ministry of Interior, two prosecutors within the Investigative Committee are in charge of cybercrime cases.

The collection and analyse of digital evidence is carried out by the "K" Department and by the department on investigation of crimes against information security and intellectual property of Main Investigative Department of Investigative Committee of the Republic of Belarus in its field of competence, although it has no laboratory for this purpose. The Department's experts may also carry out analyses at the request of other LEA. Qualified experts of the Forensic Centre may provide specialised expert examination of digital evidence.

Hardware and software used by the hi-tech crime units include EnCase Forensic solutions, NetResident software for intercepted traffic data, open software and in-house applications.

The staff include:

- 25 officers within the cybercrime unit of the Ministry of Interior
- 6-7 staff within MoI's territorial units of the five regional centres
- 10 staff within the by the department on investigation of crimes against information security and intellectual property of Main Investigative Department of Investigative Committee of the Republic of Belarus
- 2 investigatory officers for each region
- 5 staff in the cybercrime unit of the local police of Minsk
- 5 staff in the cybercrime unit of the State Security Committee, and 2 experts in digital forensics.

The personnel of specialised units have qualifications in law and engineering, with some members having considerable experience in specialised international training, including on child pornography on the Internet.

The Situation Report reflected that the police officers of Belarus would need specialised training on cybercrime issues on a continuous basis. Specialised expertise seemed to raise concerns, with a backlog of requests of several months at the expertise centre.

### 3.3.2 Assessment and summary of progress made

Several measures are being discussed as regard the prosecution and judicial authorities. It is expected that specialised prosecutors will be established in the future in Belarus' regions, building on the training of prosecutors on cybercrime issues. More specialised judges should be introduced at the Supreme Court; positions of specialised judges in the regions are also being considered.

With regard to specialised expertise, certain solutions have been developed, in particular the enhancement of in-house expertise (e.g. within the State Security Committee), and the assistance of other organisations, especially banks and computer security companies.

## 3.4 International cooperation

### 3.4.1 The situation

International cooperation is regulated by section XV of the Criminal Code. When foreign cooperation is needed, the department on investigation of crimes against information security and intellectual property of Main Investigative Department of Investigative Committee of the Republic of Belarus sends a mutual assistance request through the General Prosecutor's Office to the LEA of foreign countries. Belarus has bilateral treaties with several countries throughout the world. Countries without a formal agreement with Belarus may also provide mutual assistance. While the Ministry of Justice signs agreements, the Investigative Committee is competent for mutual assistance applications.

The contact point is established in the Ministry of Interior's "K" Department. Since 2008, Belarus belongs to the international network of contact points established under the G8 Rome–Lyon Group. The resources of the national bureau of Interpol in Belarus are often used as well.

The "K" Department also cooperates with foreign LEA in the form of joint international operations against cybercrime, in particular in the field of child pornography and bankcard fraud. Police-to-police cooperation is possible, but the daily practice of LEA was not described in detail.

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

The Ministry of Interior, Investigative Committee and the Ministry of State Security seem to share the same concerns. Despite successful cases of cooperation, as was experienced with respect to the attack of Minsk' metro, international cooperation is not effective with certain countries. The same concern applies to cooperation with many ISPs, including Google. Among other reasons, the fact that Belarus is not a Party to the Budapest Convention directly hinders formal cooperation. Political considerations have also been mentioned by Belarus as a possible explanation for the current situation.

### 3.4.2 Assessment and summary of progress made

In 2011, the statistics for requests handled by the contact point were the following:

- Outgoing requests: 226 requests sent (including 172 to Russia, 14 to Lithuania and 13 to Ukraine); 188 answers received;
- Incoming requests: 10 answers and other information sent (Russia, Ukraine, Italy, and Germany).

The recommendation of the Situation Report of 2011 to review some substantive and procedural law provisions in order to create favourable conditions for international cooperation should be considered, as well as to continue the cooperation under the project in view of meeting the requirements for accession to the Budapest Convention.

## 3.5 Law enforcement training

### 3.5.1 The situation

The Academy of the Ministry of Interior provides for university degrees in law (5-year course) with specialisations in various fields related to law enforcement; it provides for most staffs of the Ministry's agencies, of the Investigative Committee. The Institute of State Security trains the personnel of the State Security agencies. Certain officers have a degree in Information Security from the Russian Institute of cryptography, communication and information (Federal Security Service of Russia).

As the Situation Report (2011) noted, there is neither a documented training strategy in Belarus, nor any specialised educational institution providing training to the LEA personnel on cybercrime investigation and digital forensics. Law enforcement officers engaged in these activities do not have any specific professional or academic qualifications.

The Training Academy (Ministry of Interior) provides training on cybercrime issues for new recruits and international students. The courses, approved by international specialists, include training on child abuse on the Internet and other cybercrime issues.

Within the high-tech crime unit (Ministry of Interior) the new staff already have certain skills in the handling of electronic evidence. Training is organised on a regular basis to upgrade the knowledge and improve professional skills. The unit frequently prepares guidelines for other units of the Ministry on the handling of electronic devices, interacting with ISPs and telecom providers.

Belarus considers that all forms of international cooperation, including joint training, are useful. Arrangements with academic institutes or industry bodies – provided they are not yet in place – would also be an asset to develop and deliver training courses on cybercrime and digital forensics.

### 3.5.2 Assessment and summary of progress made

A course on high-tech crime was introduced at the Academy in 2011 and at the international training centre. It deals with international cooperation, national and international legal framework, investigation measures, interview of suspects and specific cybercrime offences.

The course comprises lectures and workshops. It lasts from 2 weeks (professionals) to 1 month or more (lower level). About 500 students have been trained so far, as well as several groups of practitioners dealing with high-tech crime. For instance, five students are learning methods to locate telecom devices used by suspects and present the information to investigators.

The Department on Investigation of Crimes against Information Security and Intellectual Property of Main Investigative Department of Investigative Committee of the Republic of Belarus currently organises another training on electronic evidence, use of special investigative measures and other, as well as on methodology and practice of investigations. The Investigative Committee approved this course and provided for the trainers.

In 2013, 2 courses have been implemented at the international training centre, including one on child pornography. A British expert provided valuable assistance in this regard.

## 3.6 Judicial training

### 3.6.1 The situation

Judges and prosecutors are initially educated within Belarus' institutions of higher education providing legal qualifications (esp. the Belarus State University, Academy of Management of the President of Belarus). Specialized training is provided for prospective judges. Training for a judge pertaining to a general or commercial court includes an up to one-year course in a specialised establishment along with an internship at a court under the supervision of a judge.

The key institution providing qualification upgrades for judges and prosecutors is the Institute of Further Training for judges, members of the prosecution office, the court, and institutions of justice (Belarus State University), established in 1998.

Given the transborder nature of cybercrime, Belarus supports the organisation of joint training for judges and prosecutors, both with other criminal justice stakeholders at the national level and with foreign counterparts. Workshops and conferences are also seen as valuable.

### 3.6.2 Assessment and summary of progress made

Judges, prosecutors and the investigative committee receive their training at the Institute of Further Training for Judges and the Training Academy of the Ministry of Interior. The Judicial Institute provides a basic training for investigators. Since 2006, cybercrime lectures are given for judges and prosecutors; these initiatives remain under further development, in cooperation with the relevant institutions.

In March 2013, 94 persons attended a seminar on cybercrime. Many governmental bodies, including the Academy, the Ministry of Justice, the Prosecutor General and the Ministry of Interior took part to the event. Other events are being organised:

- An international conference on cybercrime will be held in July 2013 at the Institute for National Security, for the main benefit of the Ministry of State Security;
- A conference on information security should take place in 2014.

In total, some 300 persons attended the conferences.

## 3.7 LEA/ISP cooperation

### 3.7.1 The situation

The Regulation on Licensing for Certain Activities, approved on 1 September 2010, addresses licensing procedures in the telecom sector. With regard to the Internet, data transmission service (e.g. Internet access), IP telephone service and IP TV are licensed, while Internet services such as hosting services are not concerned. The licensing authority is the Ministry of Communication and Information of Belarus. 187 licenses for data services have been issued so far, although the actual

number of operating providers is much lower. Currently, approx. 36 ISPs provide for paid access to the Internet in Belarus.

BelTelecom is the only provider in Belarus having technical capacities to establish network connections between providers and provide them with access to the international network. BelTelecom is the only "national operator", the other 35 providers being only subproviders as they need BelTelecom gateways. In 2012, it lost its monopoly over the interconnections for the providers' networks and over the access to international network.

Pursuant to a Presidential Decree of 30 September 2010, a state-owned National Centre of Traffic Exchange has been established to further develop the data transmission infrastructure in Belarus. The same Decree appoints the Operative Analytical Centre (OAC) of the President of Belarus as an independent regulator in the sector of ICTs, with the Centre being in charge of the organization of operations and supervision over the NCTE and its "united national network of data transmission".

A key problem in the investigation of cybercrime is related to technical properties of networks of individual service providers (usually, mobile communication companies, and TV companies); in certain cases they do not allow for identification of a suspected user due to the technical and financial capabilities of the operator.

Traffic data from communication channels can be collected by the law enforcement, pursuant to the Law of Belarus of 9 July 1999 on Investigation Activities and agency and inter-agency guidelines enacted thereof. It is organised by the specialised technical unit of Ministry of Interior, which uses a technical system enabling remote reception of ISPs' traffic data for investigative purposes (regulated by Decree of the President, 3 March 2010). The approval of the Prosecutor's Office is required. However, no cooperation of ISP is needed.

Subscriber data and other information (e.g. log files) can be obtained as part of the "collection of preliminary data" or "examination of items and documents", provided such action does not infringe constitutional rights. In principle, such activities can be held outside the scope of any criminal case and without the issuance of an order. A written request, signed and stamped by the head of the investigation authority or a department/service thereof, shall be sent to the head of the ISP. If the information requested includes information protected by law (e.g. content of correspondence), the measure must be related to a criminal case and requires the approval of the prosecution. In such case, an Order is issued instead of a request, its copy being sent to the head of the ISP.

An ISP can also perform actions not directly specified in the list of on-the-spot investigation activities (e.g. preservation of data), based on the instructions of the investigation authority. Article 14 of the Law of Belarus of 3 December 1997 on Agencies of the State Security of Belarus provides that state security agencies have a right to issue binding instructions to legal entities, including ISPs, "to eradicate grounds that can lead to threats to the national security of Belarus, to committing offence". Such instructions contain a demand to perform certain actions, specify the time period thereof and the method of reporting. It shall be signed and stamped by the head of the competent authority and sent to the head of the ISP.

Pursuant to a Decree of the President of 1 February 2010, ISPs are under a duty to identify subscribers' terminals when providing Internet services, as well as to record and store data on the subscribers' terminals and information regarding the services provided. Owners of Internet sharepoints or persons authorised by them must provide the identification of Internet users in Internet sharepoints, registration and storage of personal data of Internet users and information on Internet services provided by such sharepoints. Such information is to be stored for one year from the date of the service.

Rules of Telecom Services established by the Decree of the Council of Ministers of Belarus of 17 August 2006 (amended in 2010) stipulate that telecom providers shall keep information on the

fixed and cellular telecom services provided and bills paid for 5 years from the date of such services, as well as personal data of people using data transmission services and data on sharepoints" users (full name, ID details) for one year; and data on users' terminals identified in the course of data transmission service for 5 years.

There are no regular meetings, common trainings, designated contact points or standardised request forms. The prosecution service decides with regard to the requests sent to ISPs, which are sent/received by email, fax and DVDs.

### 3.7.2 Assessment and summary of progress made

Belarus law seems to fully regulate the legal and organizational issues related to LEA/ISPs cooperation. It is considered that most interactions should not be labelled as "cooperation", since they are conducted on a compulsory basis.

Technical properties of networks of certain service providers (usually, mobile communication and TV companies) still raise concerns to law enforcement, since they do not necessarily allow for the precise identification of the user.

There are no specialised contact points for the LEA/ISP interaction in Belarus. Traditionally, officers of the specialised cybercrime units of the Ministry of Interior, the Investigative Committee and the State Security Committee carry out such interaction with ISPs. It should also be noted that some ISP has a black box connected to the some law enforcement authorities. The approval of the Prosecutor's Office is required.

There are no neither formalised agreements, nor specifically designed training for the interaction between the law enforcement agencies and ISPs in Belarus. However, the "K" Department has well-established relations with ISPs, cellular networks operators, banks and other financial institutions. Such partnerships are not formalised.

It is not clear what conditions and safeguards regarding law enforcement access to data are in place.

## 3.8 Financial investigations

### 3.8.1 The situation

Embezzlement through the use of computer devices (including use of bank card details and forged cards), and advertising and distribution of child pornography are the main types of fraud and other offences on the Internet that involve crime proceeds in Belarus.

Challenges faced by the LEAs include the online and transborder nature of the crimes; limitations related to bank secrecy; multi-turn schemes to transfer money through shell companies; fake identity of account holders; negligence or complicity of bank employees in criminal arrangements.

Financial investigations are considered as a distinct law enforcement activity, for which the competent body are the Investigative Committee and the Financial Investigation Department of the State Controlling Committee of Belarus. The "K" Department can investigate financial offences, provided they are connected to an offence being investigated by the Department. Where necessary, resources of the economic crime unit, organized crime and corruption unit of the Ministry of Interior can be used, as well as resources of the Financial Investigation Department and Financial Monitoring Department of the State Controlling Committee of Belarus.

According to the "K" Department, criminals in Belarus do not often use domestic financial and bank institutions for their activities. They favour foreign payment systems, e-billing facilities,

accounts of shell companies in off-shores, and accounts in Baltic banks. There are no examples of full-scale cooperation with the private sector.

### 3.8.2 Assessment and summary of progress made

A department of financial monitoring reports suspicious transborder transactions to the law enforcement. Yet, Belarus considers that such monitoring is almost impossible as regard activities on the Internet. The monitoring can be facilitated in some cases, for instance when the company concerned is controlled by Belarussian authorities (e.g. Easypay).

Belarus has had successful cooperation activities in the past, as the "Tornado" operation illustrates. Accounts of commercial companies registered in Cyprus and Marshall Islands were used for the money laundering of incomes obtained by distributing child pornography on the Internet. The "K" Department asked the Financial Monitoring Department of the State Controlling Committee (member of the Egmont group) to send requests to the companies concerned. The information received helped in understanding the money-laundering scheme. In another case, transferred to the court in 2013, a joint operation was undertaken by the law enforcement agencies of the United States, Czech Republic and Lithuania.

Belarus reports that the Council of Europe's typology study on criminal money flows on the Internet provides an interesting input.

## 3.9 Progress Made Against Previous Recommendations

| **Cybercrime situation report March 2011** | Progress reported |
|---|---|
| Consideration of the observations made in the situation report on criminal law and criminal procedural law in view of amendment where appropriate. | Not Completed. Further work to be done on situation report recommendations. |
| Consideration of the formation of specific prosecution unit to combat cybercrime in accordance with the needs of the country. As a minimum requirement, it is necessary for a selected number of prosecutors within Belarus to become specialised in cybercrime prosecutions | Completed. |
| Development of a cybercrime training strategy incorporating the requirements of cybercrime investigators, digital forensics examiners and mainstream law enforcement staff relating to their role specific functions. This should include the development of individual training, education and continuous professional development programmes for the specialist cybercrime investigators. | Partially completed. Work to be done to develop a strategy |
| Development of a cybercrime training strategy for judges and prosecutors that will include training at the initial and in service levels and specific advanced training for selected individuals and roles within the Criminal Justice System. Utilise the concept paper developed by the Council of Europe and the Lisbon Network on training for judges and prosecutors. | Partially completed. Work to be done to develop a strategy |
| While Belarus has significant legal powers in relation to collection of Internet traffic, it is important that it develops a framework for improved cooperation between law enforcement and Internet Service Providers using as a model, the "Guidelines for Cooperation between Law Enforcement and Internet Service Providers against Cybercrime" developed by the Council of Europe under its Project on Cybercrime. | Not completed. |
| The lack of information provided in the responses to the questionnaire indicates the need to improve the capability to combat illegal money flows | Not completed. |

| | |
|---|---|
| on the Internet by adoption of the relevant findings of the Council of Europe project "Criminal money flows on the Internet: methods, trends and multi-stakeholder counteraction" | |
| Even though electronic evidence is not considered separately in Belarus, consideration should be given to incorporating good practice in the handling of electronic evidence in criminal investigations; examining existing guides such as those developed by Interpol and Europol. | Partially completed. Needs incorporating in legislation |
| Engage with regional partners in an analysis of the issues adversely affecting international cooperation in cybercrime investigations and make recommendations for improvements, including methods for improving direct contact between law enforcement investigators | Partially completed. Need to engage more to learn from experience of others |

## 3.10 New recommendations

1. Continuing the ongoing harmonisation of the legislation with the Budapest convention.

2. Implementing the recommendations of the Cybercrime@EAP discussion paper on "Article 15 – Safeguards in the Eastern Partnership Region" of 11 June 2013.

3. Developing cooperation on specific criminal cases.

4. Creating adequate conditions for the reception of evidence from abroad (by implementing the Situation Report's recommendations on legislative amendments; by developing bilateral agreements).

5. Organising thematic seminars on specific areas of criminality and international joint training.

6. Organising meetings with other training academies of the region, to exchange of information and training materials.

7. Adopting a training strategy for the law enforcement.

8. Developing training for the judiciary, and a later stage a training strategy for the judiciary.

9. Considering the development of a non-coercive relationship between LEAs and ISPs, especially regarding ISPs located abroad.

10. Building capacities in the fight against criminal money flows on the Internet, including on the basis of the CoE guide and the experience of neighbouring States.

# 4 Georgia

## 4.1 The threat of cybercrime

### 4.1.1 The situation

At the outset, the Situation Report identified cyberattacks against critical infrastructures as a major threat in Georgia. A 'cyber-campaign' was conducted against Georgia in 2008, leading to the attack of many governmental as well as news media websites, via botnets and command and control systems. It was then expanded to financial institutions, business associations and educational institutions by way of posts on the Internet calling for DoS attacks and websites defacements.

These attacks raised awareness of the potential damage – both physical and financial – faced by the public and private sectors in such situations. The protection of critical national infrastructures (CNI) is now one of the top priorities of Georgia's security policy.

Georgia had benefited from a specific joint Council of Europe and European Union Project on cybercrime implemented in 2009-2010 [9], which initiated legal reforms and helped the authorities to strengthen their capacitates to fight cybercrime.

### 4.1.2 Assessment and summary of progress made

Numbers for 2010-2011 indicate a possible increase in the number of cases handled by LEA and judicial authorities[10]. Most actions taken in the first months of 2011 concerned illegal access and data or system interference.

Georgia has prepared a cybersecurity strategy with an action plan for 2013-2015 to enhance to protection of critical (public) infrastructures.

The Data Exchange Agency (DEA) is the competent body on cybersecurity. It acts as the national CERT and receives daily reports of infected IPs. The DEA is considering the drafting of a MoU with the Ministry of Interior on the exchange of data.

Steps taken demonstrate the significant progress made by Georgia in the field of cybersecurity and CNI protection.

## 4.2 Legislation

### 4.2.1 The situation

Georgia ratified the Budapest Convention on 6 June 2012. Georgia did not sign the Additional Protocol to the Convention on Racism and Xenophobia. It signed Lanzarote Convention (CETS 201) on 12 March 2009. On 25 March 2013, Georgia signed the Second Additional Protocol to the European Convention on Mutual Legal Assistance (CETS 182).

The joint EU/CoE Project on cybercrime in Georgia included legal advice on cybercrime legislation. The project directly contributed to the adoption of the relevant legislation by the Parliament and facilitated ratification of the Convention.

---

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

[10] The overall number of investigations, prosecutions and convictions is almost the same for the first five months of 2011 as for 2010 as whole.

To follow up the significant advances made under the EU/CoE Project 2009-2010, the Situation Report suggests several amendments of substantive law. A further review of some aspects of procedural law is also desirable — e.g. on digital evidence, for which proposals are being developed.

### 4.2.2 Assessment and summary of progress made

Most definitions and provisions of criminal substantive law of the Convention are now covered by Georgia's legislation, especially chapter XXXV of the Criminal Code. Other relevant texts include a Law on Data Protection (2012) and a Law on Information Security (2012).

The Assessment Report of the Cybercrime Convention Committee on expedited preservation (December 2012)[11] stresses that specific provisions are needed to fully implement the powers set out under articles 16 and 17 of the Budapest Convention and the corresponding provisions on international cooperation. This is corroborated by the CyberCrime@EAP draft discussion paper on conditions and safeguards: in addition to recommendations on Articles 16 and 17, the discussion paper calls for the adoption of specific provisions to implement Article 19 enumerating explicitly different options of seizing and similarly securing computer data.

On 2 October 2013, Georgia adopted an organized crime strategy and action plan for 2014/15. In this connection, reforms are also envisaged regarding substantive and procedural law aspects related to cybercrime and electronic evidence. Regarding the procedural law a draft law has been prepared to amend the Criminal Procedure Code as well as the law on Operation Search Activities.

Amendments to the CPC and other laws are underway to provide for specific powers and to make these subject to safeguards and conditions.

## 4.3 Specialised institutions

### 4.3.1 The situation

Following an amendment of June 2011, the 3rd Division of the Criminal Police Department ('the Division') is responsible for the investigation of computer-related crimes, in particular crimes set out in Chapter XXXV of the Criminal Code. Three investigators deal specifically with cybercrime cases.

According to Georgia's law, most investigations are carried out by the agencies of the Ministry of Interior. Other authorities are involved, including the Investigative Division of the Ministry of Finance (e.g. for fraud offences; intellectual property) and the Prosecution Service (offences relating to illegal income). The latter one also supervises most investigations in Georgia.

The Operative Technical Department (OTD) is the forensic expertise centre of the Ministry of Interior. It provides technical assistance to investigators and validates specific measures (e.g. covert online investigations). Its forensic unit is composed of 4 staffs. No specific standards are applied in processing digital evidence, although a guide prepared by the OTD is to be endorsed soon by the Ministry. The creation of a unit within the 3rd Division to be responsible for the collection and analysis of digital evidence is underway.

A memorandum of cooperation between LEA and ISPs was concluded in 2010. It defines the principles of cooperation and specifies the rights and responsibilities of the parties to the memorandum. Ten ISPs and the representative of Ministry of Interior signed it.

[11] Available on the website of the T-CY: www.coe.int/t/dghl/cooperation/economiccrime/cybercrime/T-CY/

### 4.3.2 Assessment and summary of progress made

Georgia participated actively in training activities on cybercrime issues in the recent years. Investigators of the 3rd Division attended several training events – held with the assistance of the CoE and other partners – and several study visits to relevant agencies of European partners (e.g. Estonia). Still, Georgia's LEA would certainly benefit from additional training on investigative and forensics measures in cybercrime cases.

Efforts have been made in the field of procedural measures, especially search and seizure, based on best practices from the US and the EU. Forthcoming amendments of the Criminal Procedure Code should modify the law accordingly, together with a new legal framework on digital evidence.

In order to deal with the OTD's heavy workload, the strategy for 2013 emphasises that a digital forensics facility should be established. Regarding the computer forensics equipment used by LEA in Georgia, the Data Exchange Agency of the Ministry of Justice plans to purchase specialized software.

The intention is furthermore to have specialised prosecutors. Due to insufficient resources for a specialised unit, the focus is now on enhancing specialisation of prosecutors through training.

## 4.4 International cooperation

### 4.4.1 The situation

Mutual assistance is regulated by Georgia's Law on "International Cooperation in Criminal Matters". At the stage of criminal intelligence gathering, the General Prosecutor's Office is capable to send and receive mutual assistance requests. The Ministry of Justice is the main authority involved in sending and receiving requests at the trial stage.

According to the information received no incoming requests for cooperation were received or sent. Direct cooperation with other national police bodies is possible and it happens. No 24/7 contact point had been established prior to the project.

The Situation Report mentioned several cases where outgoing requests were successful, although Georgia lacks sufficient practice on the issue. International cooperation remains a challenging issue. Several obstacles are mentioned in the reply to the T-CY Questionnaire:

- Absence of replies from certain countries and ISPs.
- Difficulty to identify the foreign competent authority.
- Time required to receive replies in certain cases.
- Time needed to translate requests.
- Technical shortcomings of Georgian ISPS (esp. limited data storage).

Georgia recommended that incoming requests be sent in English or French, via fax or e-mail preferably – with formal requests to be sent in parallel.

Georgia did not provide statistics on the number of requests, type of data sought, or offences concerned. Such information is required to make a proper assessment of Georgia's international cooperation regime, as well as its needs in terms of assistance and capacity-building.

### 4.4.2 Assessment and summary of progress made

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

The Law on "International Cooperation in Criminal Matters" (amended in October 2013) is to address the requirements of the Budapest Convention, including Article 29. A 24/7 contact point has now been established within the specialised cybercrime unit.

In October 2013, the National Assembly of Georgia approved a law on international police cooperation that provides for the possibility of cooperation specifically pursuant to the Budapest Convention. It addresses police-to-police cooperation and allows LEA of Georgia to undertake enforcement operations with foreign LEAs or international institutions – even in the absence of formal agreement. The Law permits the exchange of information with foreign authorities (data on wanted persons; offenders' connections; modus operandi; registration of firearms; criminal intelligence; etc.). Joint investigation teams and hot pursuits are also under consideration.

Spontaneous information can be sent and received pursuant to Georgian law, and have been shared on occasions.

## 4.5 Law enforcement training

### 4.5.1 The situation

The Police Academy of the Ministry of Interior is responsible for the training of law enforcement officers in Georgia. It does not deliver training on cybercrime matters or electronic evidence. There is no training strategy or any other relevant document adopted in these fields. No professional or academic qualifications seem to be available for LEA staff on these matters.

Cybercrime investigators as well as digital forensic specialists would require training, workshops and other relevant initiatives giving an opportunity to gain experience and knowledge on cybercrime issues. The Situation Report identified several training areas to be considered, including a course on the use of the Internet for open-source research or covert investigative activity. Joint training for investigators, prosecutors and judges would be useful (see below).

Arrangements with academic institutes or industry bodies would also provide precious assistance with the development and/or delivery of specialised training.

As regards resources available, the Academy is in need of advance training material, technical support and qualified trainers to conduct training on cybercrime investigation.

The Situation Report recommended that future training plans should follow a formalised and systematic approach.

### 4.5.2 Assessment and summary of progress made

Specialised training for police officers investigating cybercrime started in 2011. It covers areas including specific cybercrime offences, crime scene management and digital forensics. A joint training has been organised for the IT unit and police officers involved in cybercrime investigations. The setting-up of the courses benefited from the assistance of the Council of Europe and the International Law Enforcement Academy.

The training course for new recruits and in-service training addresses national and international legal issues and different stages of investigation: initiation of an investigation, crime identification, crime scene management, as well as the handling and transmission of evidence to the IT unit.

The Data Exchange Agency conducts first responder training for the Police Academy, to be incorporated later on in the training for new recruits and in-service training. Plans to develop further modules of cybercrime training are in preparation.

A guide is being developed for first responders, forensic processes and investigations. It will build on the input of the Council of Europe's event in Oslo, with some adjustments to national needs.

## 4.6 Judicial training

### 4.6.1 The situation

The High School of Justice is responsible for the initial and continuous training of judges. The Training Centre of the Ministry of Justice (hereinafter "Training Centre") is in charge of training of prosecutors.

There is no documented training strategy for judges and prosecutors on cybercrime and digital evidence. A prosecutor of the Prosecutor General's Office supervises cybercrime training. Judges are trained in these fields during their initial training at the High School of Justice – with one day devoted to legal aspects, and another day to technical aspects. Training on cybercrime and digital evidence are also included in the in-service training, again mostly in two-day training sessions.

While initial training of judges on cybercrime and digital evidence seems to be sufficiently organised, in-service training would need more consistency.

The High School of Justice supports networking and sharing of experiences for judges in general. Judges could benefit from in-service training on cybercrime jointly organised with others criminal justice stakeholders in Georgia. Arrangements with academic institutes, industry bodies or specialist law enforcement cybercrime units would also be beneficial for the setting-up of training.

### 4.6.2 Assessment and summary of progress made

According to the cybercrime unit, judges and prosecutors lack specialised knowledge on cybercrime issues — and in some cases, even simple notions of IT technologies (e.g. IP address). These shortcomings affect directly the ability to conduct investigations.

The cooperation between judges, prosecutors and law enforcement academies is considered to be satisfactory. Prosecutors and staffs of the Ministry of Justice attended certain training at the Police Academy. More training programmes should be developed for judges and prosecutors.

The prosecutors benefited from a one-week training with the US Department of Justice. A training curriculum for prosecutors still needs to be prepared.

The authorities indicated that the assistance of the Council of Europe would be welcomed to develop the curriculum for prosecutors. In addition, the courses developed under the CyberCrime@IPA project would be valuable for the development of interns' and in-service courses.

## 4.7 LEA/ISP cooperation

### 4.7.1 The situation

Currently, 185 ISPs are registered in Georgia. Internet services most typically provided are Wi-Fi (64 ISPs), DSL and optical networks (31-32), as well as dial-up line (18).

No regulations have been adopted to require ISPs to retain data for a given period of time. It is assumed that the development stage of Internet businesses is not at a sufficient level to allow so technically.

The operative and investigative phases allow for requests regarding the allocation of IP address without a court order. Once a criminal case has been initiated, a court order is required to obtain traffic, subscriber as well as content data from ISPs, pursuant to the Criminal Procedural Code and the Law on Operative-Investigative Activities. Real-time interception of traffic data is only allowed in exigent circumstances, with the issuance of an order within 24 hours. Authorized public agencies are entitled to use hidden telephone recording or eavesdropping; they may also collect information from transmission lines and computer systems by using dedicated software devices.

According to the Situation Report of 2011, no specific problems are encountered in the cooperation between law enforcement and ISPs in the investigation of cybercrime. The Ministry of Interior indicates that the LEA/ISP cooperation is satisfactory, despite the absence of legal obligation for ISPs to retain data.

### 4.7.2 Assessment and summary of progress made

Significant progress was made under the umbrella of the Cybercrime@EAP project in Georgia and the earlier Project on Cybercrime in Georgia (2009-10). In particular, a Memorandum of Understanding for LEA/ISP cooperation has been adopted. The Memorandum aims at the effective cooperation of LEA and ISPs in the investigation of cybercrime, while at the same time protecting the right to privacy. It sets out basic rights and responsibilities of both stakeholders, including the obligation of LEAs to provide as much information as possible about the investigation without prejudice to the interests at stake confidentiality, etc.

The Cybercrime@EAP project also permitted the organisation of several workshops where both LEA and ISPs were present. Such joint events are still to be developed at the domestic level.

## 4.8 Financial investigations

### 4.8.1 The situation

The main types of fraud involving crime proceeds are credit card fraud, phishing, as well as the money laundering of illegal income involving the Internet.

The prevention of these offences is mainly hindered by the lack of awareness and the insufficient training of professionals. It seems particularly difficult to identify offenders and determine the origin of criminal money flows.

Different entities are responsible in the field of financial investigations. The first to be mentioned is the Department of the Procedural Supervision of Investigation in the Ministry of Finance and the Ministry of Environment and Natural Resources of Georgia and for Prosecution of Illegal Incomes of the Chief Prosecutor's Office of Georgia ("the Department"). Its main functions are to support and supervise operative-investigative activities of the relevant agency within the Ministry of Finance; respond and in case of necessity, conduct full preliminary investigation of economic and financial crimes. It is also responsible for the prosecution of cases and the representation at court.

The Investigation Service of the Ministry of Finance ("Investigation Service") was established in 2009 by the Law on Investigative Service of the Ministry of Finance. It is a special investigative body, responsible for the prevention, suppression and investigation of financial and economic crimes. The Service is entitled to conduct investigative-operative activities, carry out investigations, and obtain necessary information and other activities provided by the legislation.

The agency investigating a particular case is competent to search, seize and confiscate proceeds from crime on the Internet. There is no separate special body that would perform this task. Investigations are carried out with the assistance of the computer forensic labs of the Ministry of Justice and of the Ministry of Finance.

The Law of Georgia on Prevention of Illicit Income Legalization defines monitoring entities (*see* the Situation Report of 2011 for a complete list). Such entities are responsible for the identification of parties to a transaction, registration and systemization of information on the transaction and submission of such information to the Financial Monitoring Service (FMS), an administrative type of FIU. The supervision of these monitoring entities is carried out by the National Bank of Georgia, the Ministry of Finance, and the Ministry of Justice.

The FMS receives and analyses information sent by monitoring entities and in a case of grounded suspicion, forwards appropriate materials to the relevant authority of the Prosecutor's Office and the Ministry of Interior. The Service is entitled to apply to the court for the purpose of sealing the property (bank account) or suspending a financial transaction. It can also cooperate domestically or internationally on AML/FT issues.

### 4.8.2 Assessment and summary of progress made

A restructuration of the FIU was decided in 2004 to establish a financial police. A further re-organisation took place in 2008 and created the Investigation Service. In its Report on the Fourth Assessment Visit to Georgia (3 July 2012), the MONEYVAL Committee indicated that the Georgian AML/CFT regime has significantly improved since the last assessment in 2007.

Yet, the MONEYVAL Report identified several threats and vulnerabilities to be addressed urgently, including i) customers that are, or are owned by, offshore companies for which the identity of their beneficial owners is unknown or where the identity has not been verified; ii) a rapid and ongoing increase of non-resident deposits; iii) the development of private banking activities, including a clientele of foreign politically-exposed persons; iv) the rapid growth of the casino business and rising number of non-face–to-face transactions; v) the existence of large Georgian-led criminal organizations abroad which exposes the risk of proceeds of crime being transferred back to Georgia; and vi) domestic statistics showing the existence of major proceeds-generating crimes.

Lack of sufficient human resources and specialised expertise seem to give cause for concern. As the MONEYVAL Report of 2012 stressed, a combination of technical deficiencies, poor implementation, and limited resources undermine the effectiveness of the FIU and AML/CFT supervision. The modest number of legal persons investigated or prosecuted for ML raises further concerns, since the authorities indicated the widespread use of companies in ML schemes.

Inter-agency seems to operate adequately. Where a criminal case is started, every investigator and prosecutor has access to information regarding the progress of the case, and can indicate possible shortcomings. Task forces can be established comprising staffs of the FIU, the Ministry of Interior, and the Prosecutor General's Office. Judges can also examine the case and issue warrants and judicial orders.

The supervisory bodies should collaborate with each other and with foreign counterparts and international organizations through the exchange of information and experience. The Situation Report of 2011 specified that the FMS has already concluded a Memorandum of Understanding with all Georgian supervisory bodies and LEAs, such as the Ministry of Justice (including Prosecutor's Office), the Ministry of Finance, the National Bank of Georgia and the Ministry of Interior. Joint training between the Ministry of Interior and the Ministry of Justice are also organised, although no information was provided on their frequency or topic.

At the international level, Georgia has urged for a more effective cooperation on financial crimes, especially among European countries.

## 4.9 Progress Made Against Previous Recommendations

| Cybercrime Situation Report March 2011 | Progress reported |
|---|---|
| The development of the unit for the collection and analysis of digital evidence, identified in the situation report, should be considered a priority; the unit should be adequately resourced with equipment and suitably trained staff. | Completed |
| Consideration of the observations made in the situation report on criminal law and criminal procedural law in view of possible amendments. | Completed |
| Consideration of the formation of specific prosecution unit to combat cybercrime in accordance with the needs of the country. As a minimum requirement, it is necessary for a selected number of prosecutors to become specialised in cybercrime prosecutions. | Completed, although improvement in the knowledge levels of the appointed prosecutors is needed |
| Development of a cybercrime training strategy incorporating the requirements of cybercrime investigators, digital forensics examiners and mainstream law enforcement staff relating to their role specific functions. This should include the development of individual training, education and continuous professional development programmes for the specialist cybercrime investigators. | Partially Completed. Formalisation of training is needed |
| Development of a cybercrime training strategy for judges and prosecutors that will include training at the initial and in service levels and specific advanced training for selected individuals and roles within the Criminal Justice System. Utilise the concept paper developed by the Council of Europe and the Lisbon Network on training for judges and prosecutors. | Partially Completed. Formalisation of training is needed |
| Consideration should be given to incorporating good practice in the handling of electronic evidence in criminal investigations; examining existing guides such as those developed by Interpol and Europol. | Completed |
| Engage with regional partners in an analysis of the issues adversely affecting international cooperation in cybercrime investigations and make recommendations for improvements, including methods for improving direct contact between law enforcement investigators | Partially Completed. |

## 4.10 New Recommendations

1. Continuing ongoing advances in international cooperation by examining the practices of other countries.

2. Developing first responder, investigator and advanced forensics training courses for the Ministry of Interior cybercrime division, the Ministry of Interior OTD and the Prosecutor General's office.

3. Organising workshops, study visits, and experience exchanges of staff to improve their knowledge.

4. Initiating a plan to upgrade the equipment of the cybercrime unit (on the basis of a study visit to another country to assess Georgia's specific needs).

5. Consolidating the training structure for both law enforcement and the judiciary.

6. Considering the combination of the 2 digital forensics capabilities within the Ministry of Interior to improve performance and cost effectiveness.

# 5 Republic of Moldova

## 5.1 The threat of cybercrime

### 5.1.1 The situation

As in other countries of the Cybercrime@EAP Project, Republic of Moldova's public institutions and private actors are increasingly dependent on information and communications technologies. In recent years, Republic of Moldova has been facing numerous cyberattacks of large scale (e.g. spyware sent via emails to staff of public institutions; use of botnets for DDoS attacks against websites of public authorities).

The analysis of the situation in Republic of Moldova demonstrated the need to create a national Cybercrime Centre to set common standards for LEA and judicial authorities and enhance cooperation between relevant points of contacts. At the initiative of the Supreme Security Council, an inter-agency workgroup has been created to assess the situation and suggest appropriate solutions. It is currently considering the elaboration of an advanced information protection system.

### 5.1.2 Assessment and summary of progress made

In the period 2010-2012, a constant number of approx. 45 cases were initiated each year by the prosecution with a significant increase compared to 2009, due to legislative amendments. As the Situation Report indicates, the number of cybercrime acts remains very much unchanged; yet, the acts committed appear to be increasingly sophisticated. Data available may underestimate the level of cybercrime, due to a low level of cases actually reported.

Considerable progress has been made in the implementation of measures recommended by the Situation Report, as is illustrated by the creation with the support of the project of a Cybercrime Centre within the Ministry of Interior. Republic of Moldova has also taken positive measures in the field of financial investigations and cooperation between LEA and ISPs.

Further initiatives should focus on the enhancement of inter-agency cooperation in the fight against cybercrime, as well as the increase of staff with relevant expertise within public bodies.

In September 2013, an Action Plan on cybercrime for 2014/15 was adopted.

## 5.2 Legislation

### 5.2.1 The situation

Moldova signed the Budapest Convention on 23 November 2001 and ratified it on 5 May 2009. The Additional Protocol was signed on 25 April 2003, but has not been ratified yet. The Convention on the Protection of Children against Sexual Exploitation and Sexual Abuse (CETS No. 201) was signed on 25 October 2009 and was ratified on 12 March 2012. Moldova ratified the second Additional Protocol to the MLA Convention (CETS No. 182) on 8 August 2013.

The Law on preventing and combating cybercrime of 3 February 2009 implemented the definitions as well as many substantive and procedural provisions of the Budapest Convention. A mechanism of data retention – as defined under the EU-Directive 2002/58/ECA – is in force. As a general principle, the Prosecutor General is responsible for the coordination, handling and execution of criminal proceedings pursuant to the Code of Criminal Procedure. A Law of 5 April 2012 amending the Criminal Procedure Code entered into force on 27 October 2012.

The Situation Report made a number of recomendations with regard to substantive law. Considering some contradictions or inadequate implementation of the Cybercrime Convention special attention should be paid to Articles 259, $260^2$, $260^4$ and $208^1$.

With regard to procedural law a review was recommended on the basis of the observations and suggestions made. Some interference appeared between the system of Criminal Procedural Law and the provisions of the Law on Preventing and Combating Cybercrime of 2010. The way the power of Article 16 has been implemented needs additional clarifications e.g. the time involved before action can be taken. Implementation of Article 18 needs to be more clearly defined.

Article 19 is not implemented with regard to specific powers. The concept of seizure may not be applicable.

### 5.2.2 Assessment and summary of progress made

In addition to the Situation Report recommendations for further clarifications or amendments, e.g. regarding illegal access, illegal interception and nationality-based jurisdiction, the cybercrime unit has also called for the adoption of a clear legal provision on bankcard fraud.
As regard conditions and safeguards, the Cybercrime@EAP discussion paper on Article 15 highly recommends the adoption of appropriate provisions on search and seizure (Article 19) and real-time collection of traffic data (Article 20).

Additional legislative reforms are currently under consideration, including on the interception of e-communications in cybercrime investigations. In this respect, legal advice is provided for by the Department of IT and Cybercrime investigations of the Prosecutor General. Procedural changes are also being discussed to remove the financial threshold (loss of Lei 50,000) to start an investigation and to broaden the possibility to obtain data from ISPs at the pre-investigative stage.

Following the adoption of the Action Plan on Cybercrime (2014/15) in September 2013, an inter-agency group was established. This group is expected to draft legislative amendments to address the issues identified above.

## 5.3 Specialised institutions

### 5.3.1 The situation

It was decided in 2010 to create an IT and cybercrime investigation section within the General Prosecutor's Office, directly subordinated to the General Prosecutor. It has competence for the investigation of many computer- and telecom-related offences (e.g. illegal access; copyright violation; child pornography). Recent action focused on the identification of areas vulnerable to cybercrime, the conduct of investigations thereof, the representation of the prosecution, capacity-building of the section and its interaction with other LEAs, and other tasks.

The Fraud Investigation Directorate of the Police Department (Ministry of Interior) also has a cybercrime section.

A cyber-lab has been created within the Technical Criminalist Directorate of the Ministry of Interior, where technical experts carry out information data analysis, collection, processing, etc. Their work is framed by the Criminal Code, Criminal Procedure Code, and methodological materials, etc. At the moment the lab is at the initial stage of furnishing and integration of equipment and specialized software. The following software is used: FTK Imager, Forensic Assistant, etc.

Staff levels are as follows:

- GPO's IT and Cybercrime Investigation Section: 4 staff (1 chief prosecutor; 2 prosecutors; 1 specialist);
- Cybercrime combating section: 7 staff (1 section head; 1 section deputy head; 5 operating investigators).

All staff working within the GPO's IT and cybercrime investigation section, as well as within the Ministry of Interior' Cybercrime Combating Section, have a legal qualification (min. Law Licence). One staff of the GPO's IT and cybercrime section is qualified in information technologies.

Informal cooperation exists with the private sector (including ISPs, phone companies, banks, credit card industries).

### 5.3.2 Assessment and summary of progress made[12]

Moldova has considerably changed the structure of LEA having competence for cybercrime investigations. A Cybercrime Centre has been created with the support of the Ministry of Interior, and is partly inspired by practices in Romania and Ukraine. Moldova is counting on new facilities and the hiring of new staffs for this purpose.

In 2010, Moldova's centre on human trafficking created a specialised unit for online child pornography. Activities of the unit are currently being developed.

The project provided an expert opinion including recommendations regarding the concept on the establishment of the National Centre of Cybercrime Investigations of the General Prosecutors' Office. Upon the requests from the Ministry of Internal Affairs and the General Prosecutors' Office of the Republic of Moldova, under the project a visit to Chisinau was organised to discuss the capabilities against cybercrime in the Republic of Moldova. The objectives of the expert visit were achieved through:

- Collection of the necessary information regarding the existing capabilities, responsibilities, resources and legal framework in the cooperation against cybercrime in the Republic of Moldova were collected during the meetings;
- Providing advice and assistance on a feasible organizational, legal structure as well as on roles and responsibilities to strengthen the capabilities against cybercrime in the Republic of Moldova.

Subsequently, a report was made available for the Moldovan authorities both in Romanian and English version. The study made recommendations concerning the following issues:

- Further improvement of the legal framework;
- The establishment of clear policies for critical national infrastructure protection;
- Institutional development, including in particular the strengthening of capacities for preventing and combating cybercrime within both the GPO and the MIA respectively, and the creation of a task-force involving GPO, MIA and other organisations;
- The strengthening of interagency cooperation;
- Enhancing public-private partnerships.

Several study visits and internships have been organised to Germany, Romania and Ukraine for members of the cybercrime unit. Similarly, the child pornography unit has benefited from the assistance of UNODC and Interpol as well as the United States – including training with the FBI. Future activities will include a study visit to the United Kingdom on online covert activities.

[12] As regards the structure of LEAs, this paragraph should be read in conjunction with the CoE study "Review of proposals to establish a Cybercrime Centre in the Republic of Moldova (CyberCrime@EAP Activity 2.2).

As for now, the cybercrime unit does not have a forensic centre. The General Prosecutor's Office is providing electronic evidence expertise when necessary. The new Cybercrime Centre of the Ministry of Interior will provide expertise in the future.

According to the high-tech crime unit, the following challenges still need to be addressed:

- Inefficient training of LEA officers on cybercrime issues and specific IT areas
- Insufficient hardware and software in cybercrime investigation
- Innovative nature of cybercrimes in criminal prosecution and court practice
- Gaps in criminal procedure law on cybercrime investigation
- Lack of (specific-) IT specialists.

## 5.4 International cooperation

### 5.4.1 The situation

International cooperation is possible either pursuant to applicable international agreements, or on the basis of reciprocity. The relevant pieces of legislation are the Law of 3 February 2009 on the levels of cooperation with foreign authorities and the Law of 26 January 2010 on Preventing and Combating Cybercrime.

Incoming requests related to criminal prosecution should be addressed to the General Prosecutor, and those made during trial or execution of sentence, to the Ministry of Justice. The request shall be sent by the General Prosecutor Office to the criminal investigation body or, where appropriate, by the Ministry of Justice to the court of the place where the action required is to be undertaken. Incoming requests need to be translated in Moldovan, although English translations are tolerated.

Outgoing requests shall be submitted by the criminal prosecution body to the General Prosecutor, and by the court to the Minister of Justice for submission.

The 24/7 contact point is not allowed to send or receive requests for judicial cooperation.

Moldovan law (article $540^2$ CPC) allows for the setting-up of joint investigation teams, on the basis of inter-state agreements.

The Situation Report of 2011 indicates that three MLA requests were executed in the first quarter of 2011, and nine requests were submitted through Interpol and SECI/GUM.

### 5.4.2 Assessment and summary of progress made

According to Moldova's replies to the T-CY Questionnaire on mutual assistance, incoming and outgoing requests relate to a wide range of data (subscriber data, computer traffic data) regarding various offences (copyright infringement, child pornography, illegal access, illegal interception, etc.).

Moldova's replies to the T-CY Questionnaire identified several challenges:

- Discrepancies between legal systems.
- Difficult cooperation with foreign authorities (i.e. absence of/delay in replies).
- Excessive formalism of international letters rogatory.
- Financial burden and time required for translating requests.
- Time issues (duration of the procedure; tight deadlines to handle evidence).

To enhance its international cooperation capacities, Moldova would benefit from the continuous sharing of best practices and experiences, including by participating in additional conferences,

workshops and training held on this topic under the auspices of the Council of Europe and other international institutions. Such efforts could be made in the wider context of the strengthening of the new Cybercrime Centre, mentioned by Moldova as a priority task.

## 5.5 Law enforcement training

### 5.5.1 The situation

The Police Academy is responsible for law enforcement training, including cybercrime training in the Republic of Moldova.

An Order of 20 December 2010 approved the Joint Action Plan in preventing and combating cybercrime. It recommended training for the law enforcement staff in the detection, investigation, criminal prosecution and adjudication of cybercrime, as well as in the connection between cybercrime and other types of crime.

Pursuant to the Order, the following organisations are involved in the development and delivery of cybercrime training:

- National Institute of Justice.
- General Prosecutor's Office.
- Ministry of Interior.
- Centre for Combating Economic Crimes and Corruption.
- Information and Security Service.
- State Company "special Telecommunication Centre", in cooperation with other institutions, authorities and organizations.
- In cooperation with other central public authorities, public institutions and civil society.

Staff of the Ministry of Interior's cyber lab have taken part in specialised courses, training and seminars. They perform IT forensics under a specific judicial permit.

However, training for new recruits in how to recognise and deal with electronic evidence is considered insufficient. There are no arrangements with academic institutes or industry bodies to assist with the development and/or delivery of specialised cybercrime or digital forensics training.

The following priority areas for training have been identified:

- Legal aspects of information security of individuals and legal entities, including public entities).
- Analysis of IT and telecom crimes.
- Analysis of means of reaction to acts of cybercrime.
- Protection of intellectual property, copyright and related rights.
- Organizational measures in the field of information security.
- Analysis of the risk at administration of information resources.

### 5.5.2 Assessment and summary of progress made

The creation of the new Cybercrime Centre appears to have provided a more systematic approach to training schemes.

Cybercrime units undertake their basic training together, and seem to cooperate closely. Joint training with other criminal justice stakeholders would also be highly beneficial to exchange experience, unify criminal prosecution and judiciary practice, and enhance inter-agency cooperation. Joint courses have already been organised by the Police Academy and the National Centre for the Fight against Corruption.

The General Inspectorate of Police is expected to take responsibility to train first responders on all types of crimes, including those involving electronic evidence. A Ministerial Order addressed the training for first responders delivered by the Forensic Centre. This training on how to handle electronic evidence is planned to target the Inspectorate of the National Police Patrol, as their officers are first responders.

The organisation of further events with foreign counterparts would allow cybercrime investigators and digital forensic specialists to network and share experiences. Such events could take the form of practical seminars, training, conferences, or even a direct participation in investigations of foreign LEAs.

## 5.6 Judicial training

### 5.6.1 The situation

The National Institute of Justice (NIJ) is responsible for the training of judges and prosecutors, including on cybercrime issues.

The presentation of the Order of 20 December 2010 made above is applicable here (*see* Law enforcement training). It should be noted that pursuant to the Order, the organisations involved in cybercrime training include the General Prosecutor's Office and the National Institute of Justice.

Courses on the professional application of IT and on cybercrime are included in the initial 18-month training program. An in-service training course (one-day long) is also delivered.

Similarly to the law enforcement needs, the organisation of events with foreign counterparts would allow judges and prosecutors to network and share experiences. Such events could include practical seminars, training and conferences. Furthermore, joint training with other criminal justice stakeholders would be highly beneficial to exchange experience, unify criminal prosecution and judiciary practice, and enhance inter-agency cooperation.

The priority areas for the training for judges and prosecutors are the same as those identified for law enforcement staffs (See above, para. 6.5.1).

### 5.6.2 Assessment and summary of progress made

Training plans are expected to be finalised, although the absence of information-sharing between agencies precludes any conclusion in this matter.

Overall, the training is considered to be insufficient. In particular, human resources seem to be lacking: only one staff delivers all training within the Prosecutor General's Office. Efforts to identify other trainers have failed so far. The current trainer would also need to gain additional knowledge, in order to adapt to the evolution of ITCs and cybercrime acts.

Trainers would benefit from the development of training-of-trainers programmes, including technical training on the investigation of specific types of crime, as well as on digital forensics and electronic evidence.

Some other ongoing projects are expected to provide also training on cybercrime matters for judges and prosecutors. The Ministry of Interior is also considering the development of training for judges on this issue.

## 5.7 LEA/ISP cooperation

### 5.7.1 The situation

434 ISPs are registered in the Republic of Moldova. The Telecommunication Agency is the state agency controlling ISPs and their activities. It receives complaints from customers.

The Situation Report of 2011 identified several problems regarding LEA/ISP cooperation:

- The majority of ISPs do not retain information traffic data in contradiction with domestic legislation (Law No. 20);
- Certain ISPs delay the disclosure of the requested information;
- Problems of information leakage within some ISPs, leading to the intentional destruction of evidence.

The Republic of Moldova's legislation requires the preservation of data by ISPs for 120 days. Amendments are under consideration to reduce the period to 90 days. The Criminal Procedure Code (special part) provides the legal framework for law enforcement in the obtaining of traffic, subscriber or content data from ISPs.

### 5.7.2 Assessment and summary of progress made

Informal arrangements have been set up for the cooperation between the law enforcement and ISPs. There are no joint training programmes in place.

The Ministry of Interior plans to adopt a Memorandum of Understanding with ISPs. It may take inspiration from the similar arrangement adopted successfully in Georgia. LEAs have already been discussing this issue with ISP associations in Moldova. Given the different considerations of each ISP, it appears that individual Memorandums with specific providers may be more suitable.

The blocking of access to child pornography websites is one of the priority polices to be implemented, with the assistance of the Ministry of communications. ISPs are encouraged to establish preliminary identification (personal ID address, phone number, etc.) when they assign dynamic IP addresses. The Ministry of Interior is also preparing guides for ISPs on child pornography and on online fraud. Among other reforms being considered, ISPs may soon be obliged to inform the law enforcement on offences reported by their customers.

## 5.8 Financial investigations

### 5.8.1 The situation

The authority responsible for financial investigations is the Office for Preventing and Combating Money Laundering (OPFML) within the structure of the Centre for Combating Economic Crimes and Corruption (CCECC). It acts as Moldova's FIU. Its main task is to receive and analyse suspicious transaction reports (STR) and details of cash transactions sent by reporting entities — mainly banks, insurance companies, loan companies and professional participants on financial markets. It is required to disseminate information on STR to criminal investigation authorities and other competent authorities, when there are reasonable suspicions of ML/FT and other proceeds-generating crimes. The authority that is mainly responsible for receiving disseminations by the OPFML is the Criminal Investigation Directorate (CID) within the CCECC.

In the course of an ML/FT investigation, the LEA may exercise all the investigative powers set out under the Criminal Procedure Code, including the interrogation of suspects, conduct of on-site investigations, searches and seizing objects and documents in order to collect evidence and trace criminal assets. Nevertheless, as mentioned in the MONEYVAL Third Mutual Evaluation Report

(2007), the range of techniques available is fairly limited and the use of such techniques is restricted to serious crimes, especially serious crimes and exceptionally serious crimes.

There are 17 staff at the Anti-corruption Centre with analytic responsibilities, financial investigation, IT expert, international cooperation. Resources available seem to raise concerns. The FIU uses different types of software to carry out its activities as well a database dedicated to STRs.

### 5.8.2 Assessment and summary of progress made

In September 2010, Moldova's authorities adopted a national strategy for the prevention and combating of money laundering and financing of terrorism for 2010-2012. The AML/CFT Law has been modified following a Constitutional Court decision of 2010, the main adjustment being related to the reporting regime and the organisation of the OPFML within the CCECC. It was stressed that the CCECC will no longer be responsible for money laundering matters; the Fraud Department of the Ministry of Interior should take over this competence.

In May 2012, the National Bank of Moldova initiated a Law on Electronic Payment Systems, which entered into force in May 2013. It is monitored by the National Bank and covers all electronic activities. All players have to be licensed with minimum standards of structure and activity.

Additional legislative reforms should be adopted in September 2013 to combat illegal money flows. A new Law on Payment Services and Electronic (virtual) Money will include rules on online payment services and the information to be kept about clients. This will involve controls on real collection of virtual money from PayPal accounts and other services.

Twice a year, the OPFML reports to Parliament on the progress of the AML/FT mechanisms. Results are shared with all stakeholders, including international bodies such as FATF, Egmont, Council of Europe, and Moneyval. Each institution has its own obligation under the current third strategy (2013-2018). A first examination of the strategy was carried out in July 2013.

The FIU has good relationships with the reporting bodies and associations. Workshops and meetings are organised, either in the consultation process for new legislations, or at the implementation stage.

Moldova reported that the action of the FIU has led to successful actions against international criminal activities in the past. An important scheme, identified through STRs in Moldova, led in 2010 to the sentencing of several offenders from Moldova; it involved persons in the United States, United Kingdom, Ukraine, Romania and Slovenia, for a value of $70m in total.

The Ministry of Interior already adopted a Memorandum of Understanding with the National Bank and banking association on the reporting of suspicious transactions and offences committed against their customers. The banks now also have internal training for their staff to improve the quality of STRs. In practice, STRs are to a very large extent reported by banks. The MONEYVAL's Report on Fourth Assessment Visit (4 December 2012) considered this as an indication of a serious lack of awareness by some of the reporting entities, especially in the designated non-financial businesses and professions.

According to the same MONEYVAL Report, the CID's level of knowledge related to the financial aspect of investigations, asset identification and tracing does not appear to be very comprehensive. Additionally, in spite of the number of steps taken (MoUs signed, joint working groups, etc.) there appears to be a lack of co-operation and co-ordination between the various law enforcement authorities in order to properly pursue and investigate ML/FT cases. On a practical level, the OPFML cooperates with law enforcement authorities, especially the CID, on a daily basis. In the course of an ML/FT investigation the CID and the Anti-corruption Prosecutor Office co-

operate closely with the OPFML. However, such close cooperation does not appear to exist between the OPFML and other LEAs that receive disseminations from the OPFML.

The judiciary stage still presents a bottleneck in the system with numerous cases pending before the courts. In their 2012 report, MONEYVAL's evaluators considered that the implementation was still far from being perfect and thus needs to be addressed by a firm prosecution policy and creation of jurisprudence, particularly on the evidentiary requirements.

## 5.9 Progress Made Against Previous Recommendations

| Cybercrime Situation Report March 2011 | Progress reported |
|---|---|
| • Consideration of the observations made in the situation report on criminal law and criminal procedural law in view of possible amendments. Some parts of the Budapest Convention have not been implemented yet. | Mainly completed. New proposals prepared for approval |
| • Even though digital evidence is recognised as being covered by the criminal code, it is recommended to include good practice in the handling of electronic evidence in criminal investigations; examining existing guides such as those developed by Interpol and Europol. | Some training is provided but not within a planned strategy |
| • Development of a cybercrime training strategy incorporating the requirements of cybercrime investigators, digital forensics examiners and mainstream law enforcement staff relating to their role specific functions. This should include the development of individual training, education and continuous professional development programmes for the specialist cybercrime investigators. | Elements of a strategy are incorporated in the training programme. |
| • Development of a cybercrime training strategy for judges and prosecutors that will include training at the initial and in service levels and specific advanced training for selected individuals and roles within the Criminal Justice System. Utilise the concept paper developed by the Council of Europe and the Lisbon Network on training for judges and prosecutors. | Some training is provided but not within a planned strategy |
| • Develop a framework for improved cooperation between law enforcement and Internet Service Providers using as a model, the "Guidelines for Cooperation between Law Enforcement and Internet Service Providers against Cybercrime" developed by the Council of Europe under its Project on Cybercrime. | Some Progress made. MoU's are under discussion. |
| • Improve capability to combat illegal money flows on the Internet by adoption of the relevant findings of the Council of Europe study "Criminal money flows on the Internet: methods, trends and multi-stakeholder counteraction" | Completed |
| • Engage with regional partners in an analysis of the issues adversely affecting international cooperation in cybercrime investigations and make recommendations for improvements, including methods for improving direct contact between law enforcement investigators. | Some progress made. |

## 5.10 New recommendations

1. Finalising the legislative amendments recommended.

2. Improving international cooperation mechanisms in cybercrime investigation, including on card fraud.

3. Establishing mechanisms for the gathering and analysing cybercrime information, with the assistance of relevant institutions (e.g. creation of a database; gathering and analysis of operative and other information).

4. Developing a coherent training strategy for cybercrime and electronic evidence.

5. Developing training on several issues (computer forensics, analysis of concrete cases), as well as regional seminars for specific units (esp. FIUs) and regional working groups on specific issues.

6. Improving the internal exchange of information on financial investigations.

7. Considering the placing of the Bank of Moldova as the supervisory body for online cybercrime fraud of the banks.

8. Building capacities on child protection issues (e.g. location of offenders), with the assistance of the Council of Europe.

# 6 Ukraine

## 6.1 The threat of cybercrime

### 6.1.1 The situation

Ukraine has been facing recently an expansion of cybercrime acts, partly due to the lack of appropriate devices to protect computer systems and computer data. Cyberthreats mentioned include spoofing, DDoS attacks (including via web services) or SQL-Injection. The Situation Report also refers to the following categories:

- Creation and distribution of viruses, Trojan horses; botnets
- Creation and distribution of pornographic content, including those depicting minors
- Offences related to payment systems and business activities (skimming, phishing, etc.)
- Money-laundering via electronic payment systems; e-commerce crimes
- GSM fraud; breaches of telecom regulations, including illegal broadcasting.

### 6.1.2 Assessment and summary of progress made

The number of cases recorded increased by more than four times when the new Criminal Procedure Code entered into force in November 2012.

The importance of cybercriminality within the country is directly linked to the demography and the extent of network infrastructures. According to statistics for 2009-2012, the most common forms of offences registered are the following:

- Illegal access to computer systems (83 cases in 2012);
- "Unauthorized actions with data stored in a computer system by persons having authorized access" (44 cases).

As the Situation Report shows, the creation and dissemination of malware and the unauthorised distribution of personal databases have been declining recently. Conversely, DDoS attacks have been increasing, especially those in the form of botnet attacks against public infrastructures.

Most offences (85%) are dealt with by the Ministry of Interior, while the Security Service tackles offences related to national security; other competent bodies include the Tax Police and the forthcoming State Bureau of Investigations. The newly adopted Criminal Procedure Code of 2012 modified the jurisdiction of LEA over criminal investigations.

## 6.2 Legislation

### 6.2.1 The situation

Ukraine was one of the first countries of this region that signed the Budapest Convention (10 March 2006). The Law no. 2824-IV on ratification entered into force on 1 July 2006. Ukraine signed the Additional Protocol to the Budapest Convention on 8 April 2005 and ratified it on 21 December 2006. On 21 September 2010, a number of amendments were made to the Law of Ukraine no. 2532-VI (2532-17) according to which the Ministry of Interior of Ukraine is responsible for setting up and managing a 24/7 cybercrime reporting network. Ukraine ratified the Lanzarote Convention on the Protection of Children (CETS 201) on 27 August 2012.

Most definitions and provisions of substantive law are found in the Criminal Code. The Telecommunication Act may also be relevant.

The Situation Report identifies several gaps (e.g. corporate liability[13]). With regards to criminal substantive law no effective implementation has been assessed of Articles 2, 3, 5, 6 of the Convention. It was recommended to review the provisions referred to on the basis of the questions, observations and suggestions made, in particular concerning the implementation of Articles 7, 8 and 9. Attention was requested for definitions and applicability to the offences of the criminal code. With regards to procedural law Articles 16, 18 and 19 Budapest Convention do not seem to have corresponding provisions in domestic law.

### 6.2.2 Assessment and summary of progress made

A new Criminal Procedure Code came into effect on 19 November 2012. Ukrainian authorities stressed that the process of adapting the criminal procedure legislation is still ongoing, with direct impact on cybercrime investigations and proceedings. Electronic evidence is already admissible under general procedural law on evidence. Investigators may undertake any action as specified by the Criminal Procedure Code, unless an order of the court or the prosecutor is required. In practice, though, virtually every primary action such as IP address lookup requires a court order. Moreover, a cybercrime investigator may not even apply for a warrant.

Many definitions are provided in the Telecommunication Act, and to a lesser extent in the Criminal Code. Discussions with Ukrainian authorities facilitated the practical understanding of many concepts established in domestic legislation, especially the telecommunication law. Definitions pursuant to Article 1 of the Convention should be expanded by the legal reforms under consideration. On the specific issue of child pornography, the establishment in 2013 of the Interagency Commission on sexual abuse of children is a welcome development.

,
The entry into force of the new Criminal Procedure Code in 2012 is a welcome development. However, some of the specific powers of Articles 16-19 Budapest Convention are not foreseen in the new CPC. This may hinder investigations but also raises questions regarding conditions and safeguards as stated in the Cybercrime@EAP discussion paper on Article 15[14]. The Assessment Report of the Council of Europe's Cybercrime Convention Committee (T-CY) on expedited preservation[15] also recommends the adoption of specific provisions to implement Articles 16 and 17.

## 6.3 Specialised institutions

### 6.3.1 The situation

Cybercrime units have been established within the Ministry of Interior of Ukraine. In early 2012, a separate Cybercrime Department was established within the Ministry of Interior. The human trafficking branch was integrated into the Criminal Investigation Department. Cybercrime units have also been established within the State Security Service. Their competence depends on the type of offence involved, based on the distinction between private interests of legal and natural persons and national security interests. So far, no pre-trial investigation division has been established. No specialised investigative unit seems to exist within the prosecution.

The existence of a unit on Tax Crime Detection in the Sphere of Innovative Technologies (State Tax Service) is also worth mentioning.

[13] Ongoing parliamentary debates on the criminal liability of legal persons are encouraging.

[14] http://www.coe.int/t/dghl/cooperation/economiccrime/cybercrime/cy_Project_EaP/2523_Article15_EAP_v3_public.pdf

[15] http://www.coe.int/t/dghl/cooperation/economiccrime/Source/Cybercrime/TCY/TCY2012/T-CY(2012)10_Assess_report_v31_public.pdf

When digital evidence needs to be collected and analysed, the Cybercrime Department engages experts of the MoI's Forensic Science Centre. Where necessary, other agencies and units can also invite experts of the Centre to participate to forensics activities.

Around 30 staff are involved in the fight against cybercrime, including 25 officers and 2 senior specialists in the cybercrime unit of the Cybercrime Department. Local cybercrime units have been established in the regions of Ukraine. In total, there are 33 staff working at the Department and 236 staff working at regional units.

Staff of the Forensic Science Centre have technical university degrees and receive targeted training in specialised training centres. The personnel of the cybercrime unit within the Cybercrime Department all have legal qualifications. Staffs of the computer intelligence unit have technical degrees. Training courses are held regularly, as well as events in Ukraine and abroad to exchange best practices.

The Cybercrime Department has well-established relations with actors of the private sector (ISPs, telecom companies, banks, and other).

The Situation Report of December 2011 identified two main challenges encountered by the cybercrime unit within the Ministry of the Interior:

- The lack of technological means, and
- The need to develop distant e-learning courses to upgrade staff qualification.

### 6.3.2 Assessment and summary of progress made

Computer-related offences and other offences are not distinguished in national statistics, hence preventing any statistical analysis at the present time. A registration system for cybercrime offences is under development.

The cybercrime unit has already made efforts in providing training to its staff and to the personnel of regional units and investigators. It also takes part in training organized by other Ukrainian institutions and NGOs. In close cooperation with the FBI, the Ministry of Interior plans to create a Cyberthreat and Analysis Centre to strengthen expertise in the analysis of hardware and mobile phone devices.

Furthermore, the Ministry has had successful cooperation with several educational institutions in Ukraine, illustrated by the creation of a group of students on the fight against economic crime within the Kiev National Academy of Internal Affairs.

## 6.4 International cooperation

### 6.4.1 The situation

The General Prosecutor's Office and the Ministry of Justice are responsible for the handling of extradition and mutual assistance requests. A 24/7 contact centre unit has been set up within the Cybercrime Department of the Ministry of Interior. The unit employs 9 persons responsible for the general oversight and performance of MLA requests. The contact point has no competence to send or receive requests, but can request the preservation of data and share operative information with foreign bodies.

Pursuant to the new Criminal Procedure Code (Chapter IX), the General Prosecutor's Office is the only state body deciding upon the execution of MLA requests. The General Prosecutor's Office also

examines requests of foreign States with whom no MLA agreement exists (e.g. Japan in 2012). Upon approval, the request is executed within one month by the competent body.

A Ukrainian investigator seeking foreign assistance needs to send a request to the competent central body (i.e. the General Prosecutor's Office), following prior approval of the prosecutor. The GPO then sends the request to the competent foreign authority within 10 days, either directly of via diplomatic channels. According to the Ministry of Interior, requests are usually made via e-mail and diplomatic channels. On the other hand, the Security Service mentions only mail.

Data obtained by Ukrainian LEAs outside the framework of an MLA request is unlikely to qualify as acceptable evidence in court proceedings. As regards non-MLA incoming requests, the Security Service can only provide information that does not contain personal data.

Spontaneous exchanges of information are possible, provided that Ukraine's law on data protection, privacy, and State secrecy are respected. Joint investigation teams can be set up under the supervision of the General Prosecutor's Office.

The Situation Report of December 2011 concludes with regard to international cooperation that Ukraine is in principle capable of rendering MLA. However, not much experience has been obtained yet.

### 6.4.2 Assessment and summary of progress made

An overview of domestic legislation and statistics provided in the T-CY Questionnaire on international cooperation can lead to the conclusion that Ukraine is able to carry out cooperation activities. Yet, more information is needed to make an appropriate assessment in this field.

The Security Service reported that 94 mutual assistance requests related to cybercrime have been received since Ukraine's ratification of the Cybercrime Convention in 2006. The numbers have varied widely in the period 2006-2013 (2-3 requests in 2007 and 2008, approx. 20 in 2009 and 2010, 11 in 2011, 28 in 2012 and 11 in 2013 so far). Referring specifically to requests that have been 'executed', the Ministry of Interior has reported 4 requests. All other relevant data are only available from the Security Service.

Subscriber data, log-files and copies of servers are among the information most commonly sought. Many requests deal with by the Ministry of Interior concern DDoS-attacks, unauthorized access to governmental servers and data, illegal access to local secured networks (e.g. France's recent request for cooperation). Outgoing requests of the Ministry of Interior cover all offences set out in the new Criminal Procedure Code, while requests of the Security Service focus on the involvement of Ukrainians in hacking teams, development of malware, intrusion and other. It needs to be pointed out that data-keeping on hacking teams involved in malware development, network hacking, etc. falls within the scope of the Ministry of Interior as opposed to the Security Service. The Ministry of Interior only makes requests that are related to criminal cases covered by the Cybercrime Convention.

Latest statistics available indicate that the 24/7 contact point is rather active: In 2012 and the beginning of 2013, approx. 400 incoming and 230 outgoing requests were processed by the unit.

The Security Service frequently receives requests for ad-hoc reporting, mostly in relation to fraud cases which also fall outside the scope of the Security Service. 40-70 requests are sent each year to foreign LEAs. The Ministry of Interior and the Security Service of Ukraine both encourage such practice, especially regarding data relevant to a criminal case, statistical data, and more generally illegal activities linked to Ukraine.

According to the authorities of Ukraine, the following challenges hinder international cooperation:

- Discrepancies between legal systems;
- Difficulties raised by specialised translation;
- Short period of time to execute a request (1 month, with a possible extension). The Convention does not specify the time limits for executing requests. Some of the Convention signatories use that loophole to ignore requests altogether;
- Difficulty to disclose data obtained by domestic LEAs by acceding to a computer system without the permission of its owner.

## 6.5 Law enforcement training

### 6.5.1 The situation

Twelve establishments are responsible for the general education of police officers in Ukraine. They receive about 30,000 new police recruits each year. The Situation Report of 2011 specified that training structures on cybercrime are under development. In particular, the National Academy of Interior is expected to become a cybercrime training centre.

No national training strategy seems to be in place at the moment. A training scheme on cybercrime is being developed, following an initiative of the "K" unit, Cybercrime Department of the Ministry of Interior. The Department already holds weekly training for its own staff and training for regional offices. Apparently, individual training plans still need to be finalised. The training plans and syllabi are in place. However, a special training platform must be implemented to allow trained specialists to train several hundreds of staff from multiple regions.

The structure of specialised training courses is at its initial stage of development. Due to the ongoing re-organisation of regional offices, no unified education/training programmes are currently implemented. Training offered for investigators include a general course on the use of the Internet for open-source research and other investigative activities.

Private IT companies frequently organize workshops to which the specialised staff of the Ministry of Interior is invited. It may be desirable for the Ministry to set up permanent arrangements with relevant actors of the private sector so as to develop the latter's contribution to this matter. The work is constantly in progress.

### 6.5.2 Assessment and summary of progress made

The National Academy of Interior initiated an in-service training course in 2011. A project to create an introductory video course for new staffs and other personnel requiring cybercrime knowledge is also under consideration.

The Division regularly participates in conferences, seminars, and training in Ukraine and abroad, with the support of international institutions (e.g. CoE, EU, OSCE, Hanns Seidel Foundation, etc.). It has had numerous activities in the recent years. Significant examples are given below.

With the support of the OSCE, the Division conducted in 2012-2013 a two-course training for their regional units. Serbian cybercrime specialists conducted the training for 25 persons. One course was organised in November 2012 on basic-level online cybercrime investigations. The second course took place in mid-May 2013; it addressed TOR-systems, encryption, the investigation of online attacks and other issues. Training skills development was part of the training.

The Division also initiated a 3-days training for its own staff by the State Financial Monitoring Service of Ukraine. The training addressed cooperation between investigators and operative

agents in the investigation of intrusions into distant management systems of bank accounts. Both operative agents and investigators participated to the training.

The Division has developed tests to assess the knowledge in cybercrime areas. These tests are used by the Division's regional staff and in specialized courses at university. Other welcomed initiatives have been taken, including the setting-up of an e-library containing video files from previous training, to be used in future training. While the training materials are indeed available, there are currently no knowledge exchange platforms in place.

In April 2013, 10 officers of the Division obtained CMI (Certified Malware Investigator) international certificates from a British company (7Safe). This project is considered as valuable for the new Cybercrime Centre. It was developed thanks to the FBI's funding and regular assistance.

## 6.6 Judicial training

### 6.6.1 The situation

No information was provided by Ukraine in the Situation Report (December 2011). If there were a training platform in place as mentioned above, staff, trainees, investigators, prosecutors and judges could be trained accordingly.

### 6.6.2 Assessment and summary of progress made

No information was provided by Ukraine in the Assessment Report.

## 6.7 LEA/ISP cooperation

### 6.7.1 The situation at the outset

Approx. 2,000 telecom operators and providers were registered in Ukraine in 2011, although the accurate number may be around 6,500. Other entities active on the telecom market have not been officially counted. All providers operate upon official registration and tax compliance. However, under the existing law, ISPs may not be held liable for failure to register which explains why only 2,000 of those 6,500 are officially registered. There is nothing the Ministry of Interior can do about the issue, though. Licensing is only a prerequisite for telecom operators. Such licensing is said to be outdated; upgrades regarding cyberthreats and the transmission of data to the law enforcement would be desirable.

The Internet Association of Ukraine (IAU) represents the interests of the telecom market players. It brings together about 100 of the largest ISPs and is a major platform for discussion between the state and telecom sector, including cooperation with the law enforcement.

Telecom entities are requested by the law to retain information about telecom services provided to their customers for a period of 3 years. In practice, this information is kept for 2-6 months, and up to 1 year or more in specific cases. Given the absence of accountability mechanisms and the regulation gaps in the telecom sector, many service providers do not keep information at all. Although the Law on Telecommunications says that data must be kept for a limited period it does specify neither the type of data to be kept nor the liability for failure to keep it.

Traffic data may be obtained through a court order in the case of an investigation of a grave or especially grave crime. The ISP then has a maximum of 30 days to comply with the order. Although the data retrieval procedure is cumbersome and as such, not conducive to prompt investigation, the Criminal Procedure Code provides no alternative to the existing procedure even in emergency cases so as to not violate the requirements for evidence admissibility during pre-trial investigation and court trial. Promptness is paramount in cybercrime response and international

assistance and is the fundamental operating principle of international 24/7 cybercrime response networks. It is especially important considering that, unlike other types of criminal offenses, cybercrimes share the following characteristics:

- cybercrimes are swift;
- trace evidence is very unstable, i.e. has very short life and can be easily destroyed, particularly remotely;
- in most cases, cybercrimes are transnational and highly anonymous;
- little to no information can be found about cybercrimes committed after the event;
- time and place of cybercrime are difficult to establish.

No special hotlines or other self-regulation mechanisms have been set up by telecom providers. The Ministry of State Security performs a limited monitoring of public Internet resources. ISPs can only be held liable for illegal content where their knowledge can be proved.

### 6.7.2 Assessment and summary of progress made

The adoption of the new Code of Criminal Procedure in 2012 has had a significant effect on LEA/ISP cooperation. While the former legislation allowed for requests to be made at the pre-investigative stage, the new Code limits most procedures and interactions to the investigative level. The procedure is also burdened by new requirement of a court order to implement search, seizure and production orders, as well as to collect traffic data and intercept content data. Such amendments have also impacted on the ability of Ukrainian authorities to execute expeditiously requests of foreign countries. No legislative reform is expected on this issue in the short term. On the other hand, the requirement of a court order to be complied with in 30 days seems to ensure a higher rate of compliance with law enforcement requests.

In practice, effective cooperation seems to greatly depend on the dimensions and the territorial extent of the ISP, with larger ISPs showing more motivation and responsiveness to requests of the law enforcement. To some extent, the telecom legislation also seems to hamper cooperation, as it fails to allocate interception costs and raises doubts about the range of providers it regulates (e.g. closed network). Cooperation is said to be difficult with certain foreign ISPs, particularly Yahoo and Microsoft as well as Facebook and Google who require the sending of a mutual assistance request.

The lack or inaccuracy of information on ISPs and their subscribers raise further concerns. The amendments suggested in this field will only be discussed following the ongoing general review of the entire criminal justice system.

The cybercrime division has been developing a Memorandum of Understanding with ISPs. The Memorandum was expected to lay out the framework for prompt recording and retrieval of technical information about cybercrimes. However, the new Criminal Procedure Code has rendered the Memorandum illegal. The future of the Memorandum depends on whether any further amendments are made to the Criminal Procedure Code. It should be signed with the Internet Association of Ukraine (IAU), as well as with ISPs not belonging to this association. More generally, the IAU is expected to play an increasing role in facilitating cooperation between the law enforcement and ISPs. This is illustrated by initiatives of the Association such as the One Window project, which aims at the creation of hubs providing all necessary information (esp. subscriber and traffic data) through a unique safe channel. Such initiatives represent an encouraging development, and may help in overcoming the current absence of contact points between LEA and ISPs. The Memorandum could also pave the way for the establishment of such channels. A project in this field was already initiated at the formation of the cybercrime division, and is now covered by amendments to the law on data protection.

There are no joint training programmes for law enforcement and ISPs.

## 6.8 Financial investigations

### 6.8.1 The situation

The following crime types were identified: GSM network fraud, Internet-auction fraud, payment card fraud and the use of compromised bank account details or accounts in electronic payment systems. Social networks and social engineering are often used as well. One of the most frequent fraud activities is international financial fraud (esp. 'financial pyramids').

The prevention and control of criminal money flows on the Internet is hampered by gaps in the regulation of e-payment system operation in Ukraine. The control and registration of money flows to off-shore jurisdictions and back to Ukraine is at a low level, due to the lack of effective mechanisms of cooperation with international AML bodies and insufficient legislation in Ukraine.

The State Committee for Financial Monitoring (SCFM), the Ukrainian FIU, is the lead agency responsible for AML/CFT issues. It was granted the status of central agency of executive power and has legal personality; its activities are directed and coordinated by the Cabinet of Ministers. The SCFM has an efficient structure and access to data from more than 20 public databases.

In 2012, 179 cases of unauthorized attempts to access bank accounts involving € 15 million were dealt with, of which 159 associated with unauthorized access to accounts of the residents and 20 to accounts of non-residents.

The institutions responsible for financial investigations are:

- the Ministry of Interior;
- the State Service for Countering Economic Crime;
- the units for countering organized crime;
- the Cybercrime Department of the Ministry of Interior and its three regional branches subordinate to the Ministry of Interior;
- the State Tax Administration – Tax Police;
- the Security Service of Ukraine;
- the Prosecutor's Office of Ukraine.

The institutions responsible for following and searching proceeds of crime on the Internet or computer systems are the Cybercrime Department (Ministry of Interior); the State service to counter economic crime (Ministry of Interior); units in charge with countering organized crime in LEA of Ukraine; and the Security Service of Ukraine. Seizure of criminal proceeds and confiscation thereof are a competency of investigative agencies, with the final decision on confiscation is to be made by the court in its judgement.

### 6.8.2 Assessment and summary of progress made

A new AML/CFT Law of Ukraine was adopted on 18 May 2010, based on the FATF 40 recommendations. It is considered that it sufficiently regulates the activities of the FIU. The same law introduced amendments to the Criminal Code and other laws. The same year, the National Bank of Ukraine suggested legislative amendments, including a new provision on electronic payment systems.

Since the Situation Report of 2012, the Division for Combating Cybercrime of the Ministry of Interior signed an agreement with the Banking Association of Ukraine on credit cards. It enables the Division to be informed of credit card fraud operations by the BAU, and to take actions to identify and apprehend perpetrators. The Division signed similar agreements with the SCFM, to receive operative data on intrusion in bank accounts' distant management services. Intrusions

have already been identified and investigated, resulting in the return of UAH 87 million. The agreement is considered to be very effective.

A working group has been established between the SCFM, the law enforcement and the National Bank of Ukraine. It meets every 4 months. The SCFM reports that they cooperation with the LEAs, especially the Ministry of Interior, is excellent.

The SCFM advises banks on how to react to suspicious transactions, and is working on a risk reduction strategy with the banks, including by establishing a better mechanism for identifying individuals. There is also a project to limit cash operations in Ukraine by named individuals. Banks are known to be very active in the fight against financial crimes, and participate to training (e.g. training for bank employees on current cases, typologies and tools).

The SCFM cooperates with the Egmont group and with foreign FIUs. Successful interactions have been reported, including a reply from the United States within 3 days, which enabled Ukraine to restrain funds in a bank account.

According to MONEYVAL's Third Round Assessment Report[16] (19 March 2009), the number of yearly initiated criminal money laundering cases sent to court has been slightly decreasing since 2004, while the number of ML convictions has slightly increased. However, the updated statistics presented in the last Progress Report (6 December 2012) are positively assessed, as they show that the total number of ML convictions is continuously increasing (approx. 210 convictions in 2008 and 2009, 250 in 2010, 266 in 2011).

With the entry into force of the new Criminal Procedure Code in 2012, the authorities consider that prosecutions shall be possible without the need to ascertain the predicate offence at the moment of taking a decision to initiate an investigation. The Progress Report of 2012 welcomed this development, as it appears to be illustrative of changes in the investigative approach of the ML offence; there are cases now of successful autonomous prosecutions of ML offences.

## 6.9 Progress Made Against Previous Recommendations

| **Cybercrime situation report April 2012** | **Progress reported** |
|---|---|
| Keeping specific statistics about technology related crime that provides an insight into the seriousness of cybercrime in the national territory. However, these are general stats that do not add to the analysis or investigation of cybercrime. In other words, the stats can be broken down by applicable legal provisions but not by types of crime. Such statistics could e.g. concern the number of victims, the number of cases reported to the police, the number of cases prosecuted and the relevant criminal provisions. Such statistics could also provide information about the modus operandi applied in those cases for internal police use only. | Statistics are available regarding all cybercrime types |
| Consideration of the observations made in the situation report on criminal law and criminal procedural law in view of possible amendments. Also could be considered the enactment of specific offences concerning aggravating circumstances or the protection of specific interests. Some parts of the Budapest Convention have not been implemented yet. | Partially completed. See report for work still to be done in this respect |
| Consider the formation of a specific prosecution unit or, at least, providing prosecutors with sufficient specialized knowledge and skills to combat cybercrime in accordance with the needs of the country. | No information was provided for the assessment report |

[16] MONEYVAL reports are available at: http://www.coe.int/t/dghl/monitoring/moneyval/

| | |
|---|---|
| Incorporate the work currently being undertaken in Ukraine, into a cybercrime training strategy incorporating the requirements of cybercrime investigators, digital forensics examiners and mainstream law enforcement staff relating to their role specific functions. This should include the development of individual and group training and advanced training courses for cybercrime investigators. Build upon the existing programmes offered by the Police Academy. | Excellent progress has been made to create a structured training programme that may be of value to others in the region |
| In the absence of any information provided in the responses to the questionnaire, it is recommended that work be undertaken to develop cybercrime training strategies for judges and prosecutors that will include training at the initial and in service levels and specific advanced training for selected individuals and roles within the Criminal Justice System. Utilise the concept paper developed by the Council of Europe and the Lisbon Network on training for judges and prosecutors. | No information was provided for the assessment report |
| Continue to develop a framework for improved cooperation between law enforcement and Internet Service Providers using as a model, the "Recommendations for Cooperation between Law Enforcement and Internet Service Providers against Cybercrime" developed by the Council of Europe under its Project on Cybercrime. | Partially completed. MOU being developed. CPC changes needed |
| Improve capability to combat illegal money flows on the Internet by adoption of the relevant findings of the Council of Europe project "Criminal money flows on the Internet: methods, trends and multi-stakeholder counteraction". | Excellent progress is reported in the efficiency of the authorities in Ukraine |
| Incorporate good practice in the handling of electronic evidence in criminal investigations; examining existing guides such as those developed by Interpol and Europol. | Covered by CPC, no specific standards in place |
| Engage with regional partners in an analysis of the issues adversely affecting international cooperation in cybercrime investigations and make improvement recommendations, particularly for direct contacts between investigators. | 24/7 functioning. MLA request information not provided |

## 6.10 New Recommendations

1. Continuing the ongoing harmonisation of substantive legislation with the Cybercrime Convention, and reviewing the way by which the definitions are implemented in domestic law.

2. Adopting provisions on corporate liability in substantive criminal law.

3. Considering amendments to criminal procedural law, including its international cooperation aspects, on the basis of the recommendations provided.

4. Strengthening the 24/7 Contact Point, with the assistance of the Council of Europe.

5. Organizing further events and projects to further the training of the law enforcement.

6. Finalising the project of Memorandum of Understanding between LEAs and ISPs.

7. Developing events and exchanges of best practices on electronic money for the FIU.

# 7 Overall assessment and conclusions

## 7.1 Perception of CyberCrime@EAP by participants

The CyberCrime@EAP project only had a limited budget at its disposal[17] but is nevertheless perceived as beneficial. For example:

- Representatives from Armenia consider that CyberCrime@EAP helped create a cybercrime department in the Office of the Prosecutor General. It also supported the reform of the legislation, in particular through the study visit to Portugal.

- Representatives from Belarus consider, among other things, that CyberCrime@EAP allowed them to benefit from the experience of neighbouring countries, to share experience and to create networks.

- Representatives from Georgia appreciate the networking opportunities but also the specific training and tools, such as the 1st responder's course in Oslo that can now be applied in Georgia. The project furthermore helped maintain the momentum that led to the establishment of the Cybercrime Unit.

- Representatives from Moldova believe that the networks created but also the experience shared on law enforcement/ISP cooperation were particularly useful.

- Representatives from Ukraine state to have a better understanding on how to apply legislation on cybercrime in practice, to benefit from the networks established with neighbouring countries, and to be able to strengthen the 24/7 point of contact. The CoE report on criminal money flows on the Internet is considered to have provided significant inputs; based on that report the financial intelligence unit established criteria for suspicious transaction reporting and reporting entities are better able to identify criminal cases.

The assessment suggests that significant progress has been made in project areas in most of the fields covered by the project.

With the assistance from the project, meeting the challenge of cybercrime is becoming a priority in the region. The need for cybercrime strategies – aimed at crime prevention and criminal justice – was discussed in order to ensure a comprehensive response to cybercrime and other offences involving electronic evidence. There is now a better understanding of the need to take measures against cybercrime in the region and to provide a framework for a range of different measures, including the participation of multiple public and private sector stakeholders.

Policy- and decision-makers participated in activities organised under the project. This resulted in a stronger involvement and support of decision-makers to the project as well as a greater awareness about cybercrime as a threat against society.

The activities carried out under the project fostered the identification of needs at national and regional levels and of strategic priorities reflected in the declaration on the strategic priorities regarding cybercrime for Eastern Partnership countries.

[17] EUR 724,000 over 30 months (compared, for example, to EUR 2.77 million for the sister project in South-eastern Europe CyberCrime@IPA).

## 7.2 Legislation

The project addressed the state of cybercrime legislation in each project area as it is recognised that without criminalisation of such conduct, countries cannot investigate and prosecute cybercrime and, importantly, cannot request for assistance of another country. The main instrument to be applied is the Budapest Convention (CETS 185).

The Situation Report drafted in the beginning of the project evaluated to what extent project areas had implemented the Convention. Apart from the content of the Convention and its Protocol on Xenophobia and Racism, the report considered other regulations and instruments of the European Union and the Council of Europe.

All project countries have been strongly encouraged to implement Article 15 on conditions and safeguards in relation to investigative powers. An international conference on Article 15 – organised in Baku in November 2012 in conjunction with the Internet Governance Forum under CyberCrime@EAP and its sister project CyberCrime@IPA – allowed to review how the conditions and safeguards of the Budapest Convention are implemented in Eastern and South-eastern Europe, as well as the conditions to be established in order to meet rule of law and human rights requirements when investigating cybercrime and securing electronic evidence. A follow up roundtable was organised on 7 December in Strasbourg for EAP countries. Based on these activities, the project prepared a report on the implementation of Article 15 (Conditions and Safeguards) of the Budapest Convention in the Eastern Partnership region.[18]

With the assistance of CyberCrime@EAP, participating countries are now aware of the need to:

- Continue to strengthen legislation on cybercrime and based upon the recommendations made under the project. It is important to close the gaps identified in legislation that prevent effective investigation of cybercrime, including money flows on the Internet, cooperation with Internet service providers and international cooperation.

- Ensure that procedural law powers are foreseen in specific provisions and applied with respect to human rule of law and human rights. The project has also made available a study on safeguards and conditions (Article 15 of the Budapest Convention on Cybercrime).

Overall, substantive criminal law provisions are in line with the Budapest Convention. It is anticipated that gaps, unclear wordings and other shortcomings will be resolved in time by practice, court decisions, legal interpretations or further reforms if necessary.

The main problem in the region appears to be that specific procedural powers – as foreseen in the Budapest Convention – have not been fully implemented under domestic laws in some of the countries. This may carry risks regarding conditions and safeguards to protect the rights of individuals (Article 15 Budapest Convention).

In the course of CyberCrime@EAP, several countries have begun to prepare amendments to their Criminal Code and Criminal Procedure Code that will see additional improvements.

Progress made in the region regarding legislation is thus satisfactory. Further support may be required in the near future to maintain this momentum.

18 http://www.coe.int/t/dghl/cooperation/economiccrime/cybercrime/cy_Project_EaP/2523_Article15_EAP_v3_public.pdf

## 7.3 Specialised institutions

All countries (Armenia, Azerbaijan, Belarus, Georgia, Moldova, Ukraine) have undertaken important reforms regarding specialised cybercrime units at law enforcement and/or prosecution levels.

Some of them also adopted training schemes, and some reached out to other donors and organisations for additional support.

Good progress has thus been made in the region. CyberCrime@EAP supported institutional reform, such as the establishment of specialised high-tech crime units in Armenia, Georgia and the Republic of Moldova. With the advice of the project a specialised cybercrime department was established under the General Prosecutors' Office of the Republic of Armenia. In January 2013, a specialised cybercrime division was established within the Ministry of Internal Affairs of the Republic of Georgia, including a 24/7 point of contact as part of the specialised cybercrime division. The project submitted a feasibility report on the initiative of the Moldovan authorities to establish a cybercrime centre. In addition, it reinforced inter-agency cooperation among national authorities (cybercrime units of police, prosecution services, state security services etc.) and provided information about the Cybercrime Centres of Excellence initiative of the European Union in view of establishing such national centres of excellence in some of the project countries.

Further needs have been identified regarding the training of staff, the creation of forensic centres within or separate from specialised units and additional technical equipment and software.

Where specialised institutions responsible for investigations on cybercrime and electronic evidence have been established within state security services, concerns may arise regarding rule of law and human rights principles, and additional safeguards may need to be considered.

## 7.4 International cooperation

The project increased the level of participation in international fora against cybercrime facilitating the participation of representatives from project countries in the following events:

- Octopus Conference (6-8 June 2012, Strasbourg, France) and Cybercrime Convention Committee Meeting (T-CY) (4-5 June 2012, Strasbourg, France);
- Internet Governance Forum (5-8 November 2012);
- Cybercrime Convention Committee Plenary Meeting (5-6 December 2012).

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

The project continued to create synergies with another joint project of the Council of Europe and European Union on cooperation against cybercrime in South-eastern Europe (CyberCrime@IPA), which is funded under the Instrument of Pre-Accession (IPA)[19]. This allowed to exchange experience in the fight against cybercrime between two regions in a cost-effective manner.

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

Furthermore, this project continued to build upon the achievements of the joint EU/COE Project on cybercrime in Georgia when establishing a cybercrime unit in that country. In June 2012, Georgia deposited the instrument of ratification of the Cybercrime Convention, thus becoming a Party to this treaty.

The opportunity for networking and experience exchange created by CyberCrime@EAP enhanced police and judicial cooperation between countries of the region, but also with countries from South-eastern Europe and others that participated in project activities.

The role of the 24/7 points of contact for urgent international cooperation was strengthened during the project. The project succeeded to clarify and network these contact points in the region as well as to increase their efficiency.

Project areas were encouraged to make best use of existing channels of communication (24/7 Network, Interpol, EUROJUST, GPEN, SECI, etc.) and to ensure where possible that the contact point responsible for cooperation against crime under different initiatives were the same in order to avoid a proliferation of contact points and networks.

Nevertheless, several countries reported difficulties in their cooperation with third countries or with multi-national service providers and often obtain no replies to their requests.

Proposals have been made to further simplify the procedures for mutual legal assistance, for example, by sharing subscriber information without the need for MLA. Some of these proposals will be discussed by the Cybercrime Convention Committee (T-CY).

It seems, nevertheless, that further networking and confidence building between participating countries and third countries as well as private sector stakeholders will be required.

## 7.5 Law enforcement training

The project supported the participation of the EAP countries in the International Workshop on Electronic Evidence organised under CyberCrime@IPA project. The Electronic Evidence Guide has been developed under CyberCrime@IPA to provide countries with guidance in the process of collecting and handling electronic evidence. The Guide was disseminated among the project countries of both the CyberCrime@IPA and the CyberCrime@EAP to enhance the cooperation against cybercrime but also to assist the countries with developing training strategies and materials.

A training course - Training of Trainers and LEA 1st responders course - was held at the Norwegian Police University College in Oslo from 25th February to 1 March 2013. It has been developed as an output of the European Union/Council of Europe Joint Project on Regional Cooperation on Cybercrime in the IPA region. This particular course was held for the trainers who will deliver the course in their own countries as part of their national training programme. The project countries of the CyberCrime@IPA and CyberCrime@EAP projects have varying levels of cybercrime training incorporated within their national training programmes. This course for trainers was necessary in order to enable a standardised course to be delivered in the region and to provide additional skills for the trainers to be able to deliver the underlying course in their own countries. The course provided procedural as well as practical information about the subject matters and concentrated on how these issues impact on the day-to-day work of the delegates. In addition, this course provided delegates with skills to enable them to prepare and deliver presentations on the subject for their peers.

Training is an area where capabilities vary considerably in the region. All countries deliver training to some extent, and this ranges from seminars to ad hoc event and structured training courses that form part of a programme. Initial and in-service training on cybercrime and digital evidence is

available, for example, in Armenia on the handling of digital devices that may contain evidence, in Belarus on online child abuse or in Ukraine where in-service training was initiated in 2011.

Further training courses are under development in most countries. Some project areas have published manuals and developed training courses, notably using the training materials from the Council of Europe Oslo training course for 1st responders. In Armenia, a guide on search and seizure is being developed, in Azerbaijan a training course on child pornography is in preparation, in Georgia a guide for 1st responders and forensic procedures and in Moldova further training for new recruits on electronic evidence are being prepared.

However, in all six countries a strategy or systematic approach to training of law enforcement staff on cybercrime and electronic evidence is yet missing. In some countries there is also an absence of an authority responsible for such training.

Law enforcement training will thus remain a priority in the future. International organisations but also the private sector may be able to provide support.

## 7.6 Judicial training

Judicial training is a field where further work is necessary. Some initiatives are underway, such as a guide for prosecutors in Armenia, several conferences that are planned in Belarus in 2013/14, or training in Georgia with the support of the US Department of Justice. However, such training appears to be ad hoc and not sustainable. Systematic training strategies are still missing in most countries.

The training materials made available under the CyberCrime@EAP project should be useful and may help incorporate training on cybercrime and e-evidence into domestic training curricula:

- Training manual for the introductory (basic) training course for judges and prosecutors as well as the training materials (e.g. teaching materials, including presentations, practical exercises and assessment material).

- Training manual for the advanced training course for judges and prosecutors as well as the training materials (e.g. teaching materials, including presentations, practical exercises and assessment material).

Judicial training should become a priority in all six countries in the future.

## 7.7 Law enforcement/ISP cooperation

The project reviewed the current state of cooperation between LEA and ISP in the EAP countries and identified the measures and specific steps to be taken in each project country to strengthen such cooperation. Good practices and relevant initiatives were presented by industry and law enforcement authorities, including methods for obtaining and analysing computer data from service providers e.g. production order, search and seizure, preservation of content and traffic data.

Overall, good progress has been noted with regard to law enforcement/Internet service provider cooperation. The following guidelines and good practices served participating countries for inspiration:

- The Council of Europe Guidelines for cooperation between law enforcement and Internet service providers (2008) developed under the Global Project on Cybercrime.[20]

- The Memorandum of Understanding between law enforcement and ISPs concluded in Georgia in 2010 (prepared with the assistance of the EU/COE joint Project on Cybercrime in Georgia).

The Memorandum of Understanding developed in Georgia is in demand by others in the region and will help improve levels of cooperation in countries where the relationships are currently coercive and where cooperation can bring benefits in terms of information exchange and a better understanding of the issues faced by various parties.

Similar MoUs are under consideration in Moldova and Ukraine. In Armenia and Azerbaijan practical working arrangements have been established between LEA and ISPs.
Cooperation between law enforcement and Internet service provider will remain a challenge, in particular in countries where procedural powers on access to data are not precisely defined. Cooperation agreements thus need to contain safeguards to ensure that rule of law and human rights (including data protection) requirements are met.

## 7.8 Financial investigations[21]

CyberCrime@EAP helped link up anti-cybercrime organisations and anti-money laundering/financial investigation bodies. A primary tool has been the typology study on criminal money flows prepared by the Council of Europe and to which the CyberCrime@EAP project also provided inputs.[22]

The project supported activities for raising awareness to confiscate proceeds from crime on the internet, strengthening interagency and public-private cooperation in this area and identifying countermeasures and good practices. The EAP countries participated in the International workshop on Public Private Cooperation against cybercrime and Criminal Money on the Internet (Istanbul, Turkey, 26-28 November 2012) organised under the CyberCrime@IPA project. Representatives of the EAP region were invited with the purpose to continue the intra-regional approach concerning criminal money flows on the Internet. Moreover, tools and guidance on public/private information sharing against cybercrime are provided for the project countries.

CyberCrime@EAP encouraged stronger interagency cooperation in some countries (Armenia, Georgia and Ukraine) while such cooperation needs to be further enhanced in others. In Ukraine, the project and the typology report led to the development of additional criteria for suspicious transaction reporting.

Given that most cybercrime is profit-driven, financial investigations on the Internet will gain in importance in the future.

[20] http://www.coe.int/t/dghl/cooperation/economiccrime/cybercrime/Documents/Reports-Presentations/567_prov-d-guidelines_provisional2_3April2008_en.pdf

[21] For detailed reports on the anti-money laundering systems, see the MONEYVAL reports at: http://www.coe.int/t/dghl/monitoring/moneyval/

[22] http://www.coe.int/t/dghl/monitoring/moneyval/Typologies/MONEYVAL(2013)6_Reptyp_flows_en.pdf

## 7.9 Future support to capacity building on cybercrime and electronic evidence

The present assessment report suggests that good progress has been made in the countries participating in CyberCrime@EAP in spite of limited resources. The progress to date may be considered a foundation for further action.

The themes covered by this project should remain strategic priorities in the coming years:

1. Cybercrime policies and strategies;
2. Complete and effective legislation;
3. Specialised cybercrime units;
4. Law enforcement training;
5. Judicial training;
6. Financial investigations and the prevention and control of fraud and money laundering
7. Cooperation between law enforcement and Internet service providers;
8. Efficient regional and international cooperation.

The public authorities of these countries will have the primary responsibility for the implementation of effective measures against cybercrime. The private sector and the international community may provide support.

The Council of Europe may support further capacity building with respect to:

- Engagement of decision-makers;
- Strengthening of legislation, in particular procedural powers and safeguards and conditions (Article 15 Budapest Convention and data protection);
- Skill for judges and prosecutors on cybercrime and electronic evidence;
- Law enforcement training strategies;
- International cooperation;
- Public reporting systems on cybercrime.

# 8 Appendices

## 8.1 Assessment Teams

| Team members | Email | Project area assessed |
|---|---|---|
| Giorgi Tielidze (Georgia)<br>Nigel Jones (UK) | g.tielidze@mia.gov.ge<br>nigel.p.jones@gmail.com | Armenia |
| Gergo Nemeth (Council of Europe)<br>Nigel Jones (UK) | Gergo.nemeth@coe.int<br>nigel.p.jones@gmail.com | Belarus |
| Vahagn Harutyunyan<br>Nigel Jones (UK) | vahar@police.am<br>nigel.p.jones@gmail.com | Georgia |
| Vahagn Harutyunyan (Armenia)<br>Nigel Jones (UK) | vahar@police.am<br>nigel.p.jones@gmail.com | Moldova |
| Giorgi Jokhadze (Georgia)<br>Veaceslav Soltan (Moldova)<br>Nigel Jones (UK) | GJokhadze@dea.gov.ge<br>v.soltan@procuratura.md<br>nigel.p.jones@gmail.com | Ukraine |

## 8.2 Strategic Priorities for the Cooperation against Cybercrime in the Eastern Partnership Region

Adopted at the Conference on Strategic Priorities under the CyberCrime@EAP project Kyiv, Ukraine, 31 October 2013

### Declaration on Strategic Priorities for Cooperation against Cybercrime

We, representatives of Ministries of Interior and Security, Ministries of Justice and Offices of Prosecutor's General of States participating in the CyberCrime@EAP project of the Eastern Partnership Facility

- Meeting at this regional Conference on Strategic Priorities on Cybercrime held in Kyiv, from 30 to 31 October 2013, in cooperation with the Council of Europe and the European Union;

- Taking note of the Joint Declaration on Eastern Partnership Justice and Home Affairs adopted by Ministers responsible for justice and home affairs of European Union Member States and States participating in the Eastern Partnership (Luxembourg, 8 October 2013) which stresses, *inter alia*, the importance of enhancing cooperation against cybercrime through effective application of the standards of the Budapest Convention on Cybercrime;

- Conscious of the benefits of information and communication technologies that are transforming our societies;

- Concerned by the risk of cybercrime that adversely affects confidence and trust in information technologies as well as the rights and safety of individuals, including in particular children;

- Recognising the positive obligation of governments to protect individuals against cybercrime;

- Mindful of the need to respect fundamental rights and freedoms, including the protection of individuals with regarding to the processing of personal data, when protecting society against crime;

- Considering the need for cooperation between public and private sectors for the prevention and control of cybercrime and the protection of computer systems;

- Believing that effective measures against cybercrime require efficient regional and international cooperation;

- Underlining the value of the Budapest Convention on Cybercrime as a guideline for domestic legislation and a framework for international cooperation;

- Noting with appreciation the increasing importance paid by the European Union to cybersecurity and action against cybercrime;

- Considering, in particular, that partnerships should be sought between the European Cybercrime Centre (EC3) at Europol and our law enforcement authorities;

- Grateful for the support provided by the European Union and the Council of Europe through the CyberCrime@EAP regional project;

- Building on the progress made and on the action on cybercrime already taken in the States of the region, while noting that further efforts are required;

We endorse

the strategic priorities for cooperation against cybercrime

presented at this conference

and

we are committed to

- Pursue cybercrime strategies to ensure an effective criminal justice response to offences against and by means of computers as well as to any offence involving electronic evidence;

- Adopt complete and effective legislation on cybercrime that meets human rights and rule of law requirements;

- Strengthen specialised law enforcement units and the specialisation of prosecution services with respect to cybercrime and electronic evidence;

- Implement sustainable law enforcement training strategies;

- Support the training of judges and prosecutors on cybercrime and electronic evidence;

- Pursue comprehensive strategies to protect children against online sexual exploitation and sexual abuse in line with the Lanzarote Convention;

- Promote financial investigations and the prevention and control of fraud and money laundering on the Internet;

- Strengthen cooperation with the private sector, in particular between law enforcement authorities and Internet service providers;

- Engage in efficient regional and international cooperation;

- Share our experience with other regions of the world to support capacity building against cybercrime;

- Promote adherence to the Budapest Convention on Cybercrime at the global level.

Declaration adopted by acclamation in

Kyiv, Ukraine, 31 October 2013

# Appendix: Strategic priorities for cooperation against cybercrime

## 1 - Strategic priority: Cybercrime policies and strategies

As societies are transformed by information and communication technology, the security of ICT has become a policy priority of many governments. This is reflected in adoption of cybersecurity strategies by many governments with a primary focus on the protection of critical information infrastructure. However, governments also have the positive obligation to protect people and their rights against cybercrime and to bring offenders to justice.

Governments may therefore consider the preparation of specific cybercrime strategies or to enhance cybercrime components within cybersecurity strategies or policies.

Relevant authorities may consider the following actions:

- **Pursue cybercrime policies or strategies** with the objective of ensuring an effective criminal justice response to offences against and by means of computers as well as to any offence involving electronic evidence. Consider as elements of such policies or strategies preventive measures, legislation, specialised law enforcement units and prosecution services, interagency cooperation, law enforcement and judicial training, public/private cooperation, effective international cooperation, financial investigations and the prevention of fraud and money laundering, and the protection of children against sexual violence.

- Ensure that human rights and rule of law requirements are met when taking measures against cybercrime.

- **Establish online platforms for public reporting on cybercrime.** This should provide a better understanding of cybercrime threats and trends and facilitate criminal justice action. Such platforms may also be used for public information and threat alerts.

- Create awareness and promote preventive measures at all levels.

- **Engage in public/private cooperation**, including in particular in the cooperation between law enforcement authorities and Internet Service Providers.

- **Engage in international cooperation to the widest extent possible.** This includes making full use of the existing bi- and multilateral and regional agreements, in particular the Budapest Convention on Cybercrime. Measures and training to accelerate mutual legal assistance should be implemented. Governments (Parties and Observers to the Convention) should actively participate in the work of the Cybercrime Convention Committee (T-CY) and should engage in cooperation with the European Cybercrime Centre (EC3) and other initiatives of the European Union.

- **Evaluate on a regular basis the effectiveness of the criminal justice response to cybercrime and maintain statistics**. Such analyses would help determine and improve the performance of criminal justice action and allocate resources in an efficient manner.

## 2 - Strategic priority: A complete and effective legal basis for criminal justice action

Adequate legislation is the basis for criminal justice measures on cybercrime and the use of electronic evidence in criminal proceedings. States participating in the CyberCrime@EAP project have made much progress in bringing their legislation in line with the Budapest Convention as well as related Council of Europe and European Union standards on data protection, on the protection of children against sexual violence or on crime proceeds and money laundering.[23] However, further strengthening is required and often legislation has yet to stand the test of practice. This is particularly true for specific procedural law powers.

The adoption of complete and effective legislation that meets human rights and rule of law requirements should be a strategic priority.

Relevant authorities should consider the following actions:

- **Further improve procedural law provisions to secure electronic evidence by law enforcement.** This should include laws and implementing regulations on the use of the expedited preservation provisions of the Budapest Convention (follow up to assessment by Cybercrime Convention Committee), but also other rules on access to data held by private sector entities.

- **Evaluate the effectiveness of legislation.** The application in practice of legislation and regulations should be evaluated on a regular basis. Statistical data on cases investigated, prosecuted and adjudicated should be maintained and the procedures applied should be documented.

- **Ensure that law enforcement powers are subject to conditions and safeguards in line with Article 15 Budapest Convention.** This should include judicial oversight of intrusive powers but also respect of principles of proportionality and necessity.

- **Strengthen data protection legislation in line with international and European standards.** Governments are encouraged to ensure that their national data protection legislation complies with the principles of the Council of Europe's data protection convention ETS 108 and to participate in the Convention's current modernisation process. The same applies to the future data protection standards of the European Union. This will facilitate the transborder sharing of data also for law enforcement purposes.

- **Complete legislation and take preventive and protective measures on the protection of children against online sexual violence**. While many provisions of the Lanzarote Convention have been implemented, in some States or areas issues such as "possession of child pornography", "knowingly obtaining access" and "grooming" still need to be addressed.

- Adapt legislation on financial investigation, the confiscation of crime proceeds and on money laundering and the financing of terrorism to the online environment. Rules and regulations should in particular allow for swift domestic and international information exchange.

[23] See for example Council of Europe Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data (ETS 108), the "Lanzarote Convention" on the Sexual Exploitation and Sexual Abuse of Children (CETS 201), Convention on the Laundering, Search, Seizure and Confiscation of Proceeds from Crime and the Financing of Terrorism (CETS 198).

## 3 - Strategic priority: Specialised cybercrime units

Cybercrime and electronic evidence require a specialised response by criminal justice authorities. Law enforcement authorities and prosecution services need to be able to investigate and prosecute offences against computer data and systems, offences by means of computers as well as electronic evidence in relation to any crime. In all States participating in the CyberCrime@EAP project, the creation or strengthening of police-type cybercrime units is in progress and the specialisation of prosecutors is under consideration in some. This process should be pursued. It is essential to understand that technology changes day by day and that the workload of cybercrime and forensic units is increasing constantly. The resourcing (staff, equipment, software) and maintenance of specialised skills and the adaptation of such units to emerging requirements is a continued challenge.

The continued strengthening of specialised cybercrime units should be strategic priority.

Relevant authorities should consider the following actions:

- **Establish – where this has not yet been done – specialised cybercrime units within the criminal police.** The exact set up and functions should be the result of a careful analysis of needs and be based on law.

- **Enhance the specialisation of prosecutors.** Consider the establishment of specialised prosecution units or, alternatively, of a group of specialised prosecutors to guide or assist other prosecutors in cases involving cybercrime and electronic evidence.

- **Review the functions and resourcing of specialised units on a regular basis.** This should allow to adjustments and thus to meet new challenges and increasing demands.

- Facilitate cooperation and exchange of good practices between specialised units at regional and international levels.

- **Improve procedures for cybercrime investigations and the handling of electronic evidence.** Examine and consider implementation of national and international standards and good practices in this respect. Consider making use of the Guide on Electronic Evidence developed under the CyberCrime@IPA project in cooperation with experts of the Eastern Partnership region.

## 4 - Strategic priority: Law enforcement training

Law enforcement authorities need to be able not only to investigate offences against and by means of computer systems but also deal with electronic evidence in relation to any type of crime. With the exponential growth in the use of information technologies by society, law enforcement challenges have increased equally. All law enforcement officers – from first responders to highly specialised computer forensic investigators – need to be enabled to deal with cybercrime and electronic evidence at their respective levels. Elements of law enforcement training strategies have been identified, but consistent training strategies have not yet been adopted.

The preparation and implementation of sustainable training strategies to train law enforcement officers at the appropriate level should be a strategic priority.

Relevant authorities should consider the following actions:

- **Implementation of a domestic law enforcement training strategy.** The objective should be to ensure that law enforcement agencies have the skills and competencies necessary to investigate cybercrime, secure electronic evidence, carry out computer forensic analysis for criminal proceedings, assist other agencies and contribute to network security. Investment in such training is justified given the reliance of society on information technologies and associated risks.

- **Include rules and protocols on the handling of electronic evidence in all levels of national training.** It is important to recognise that electronic evidence impacts on all criminal activities and training in recognising and dealing with electronic evidence is needed by all law enforcement operatives and not only those in specialised units. This training could be based on the Guide on Electronic Evidence developed under the CyberCrime@IPA project.

- **Consider the introduction of individual training plans for specialist investigators.** The changes in technology and the manner in which criminal abuse that technology mean that there is a need for an appropriate number of highly trained personnel that are competent and able to conduct investigations and or digital evidence examinations at the highest level. It will also enhance their status within the criminal justice system.

- **Consider the implementation of procedures to ensure best value for the investment in cybercrime training.** Cybercrime and computer forensics training is very expensive. In order to ensure that an adequate return is received for the investment, States should ensure that staff are appointed to and remain in posts that reflect the level of knowledge and skills they have. To this end, training and human resource strategies need to be complimentary.

# 5 - Strategic priority: Judicial training

As – in addition to offences against and by means of computers – an increasing number of other types of offences involve evidence on computer systems or other storage devices, eventually all judges and prosecutors need to be prepared to deal with electronic evidence. A clear need for systematic and sustainable training for judges and prosecutors has been identified in all States participating in the CyberCrime@EAP project.

Enabling all judges and prosecutors to prosecute and adjudicate cybercrime and make use of electronic evidence in criminal proceedings should remain a strategic priority.

Relevant authorities should consider the following actions:

- **Adapt existing training materials and train trainers**. Training concepts and materials have already been developed by the Council of Europe and could be adapted to the needs of domestic training institutions. Trainers should be trained in the delivery of the materials.

- **Mainstream judicial training on cybercrime and electronic evidence.** Domestic institutions for the training of judges and prosecutors should integrate basic and advanced training modules on cybercrime and electronic evidence in their regular training curricula for initial and in-service training.

- **Introduce measures to ensure that judicial training on cybercrime and electronic evidence is compulsory.** It has been apparent during the project that training for judges and prosecutors is voluntary in most project areas. This led to many instances where participants only attended training for very short periods of courses and did not benefit fully from the training that was delivered.

- **Introduce training records for individual judges and prosecutors.** In order to ensure that best use is made of the training delivered to judges and prosecutors, it is advisable that a record is kept of all training received by individuals so as to inform requirements for further specialised training and to ensure the right people are trained and their skills utilised appropriately.

## 6 - Strategic priority: Financial investigations and prevention and control of fraud and money laundering on the Internet

Most crime involving the Internet and other information technologies is aimed at generating economic profit through different types of fraud and other forms of economic and serious crime. Large amounts of crime proceeds are thus generated and are circulating on the Internet.

Therefore, financial investigations targeting the search, seizure and confiscation of crime proceeds and measures for the prevention of fraud and for the prevention and control of money laundering on the Internet should become a strategic priority.

Governments should consider the following actions:

- **Establish an online platform for public reporting on fraud on the Internet and on cybercrime in general.** The use of standardised reporting templates will allow for a better analysis of threats and trends, of criminal operations and organisations, and of patterns of money flows and money laundering. This will facilitate measures by criminal justice authorities and financial intelligence units to prosecute offenders and to seize and confiscate crime proceeds. The platform should also serve preventive functions (public awareness and education, threat alerts, tools and advice). The more domestic platforms are harmonised with those of other States, the easier it will facilitate regional and international analyses and action.

- **Promote pro-active parallel financial investigations** when investigating cybercrime or offences involving information technologies/the Internet. This requires increased interagency cooperation between authorities responsible for cybercrime and for financial investigations as well as financial intelligence units. Joint training may facilitate such interagency cooperation.

- **Create trusted fora** (domestic and regional) for public/private information sharing on cyber threats regarding the financial sector. Domestic fora should be available to key stakeholders (such as financial sector representatives, Internet service providers, cybercrime units, financial intelligence units, Computer Security Incident Response Teams). Their purpose is to identify threats, trends, tools and solutions to protect the financial sector against cybercrime. The regional forum should consist of the fora established at domestic levels.

- **Establish the legal framework for the seizure and confiscation of crime proceeds** and digital assets as well as for the prevention of money laundering on the Internet. This should include digital assets, such as e-money and virtual currencies. Rules, regulations and procedures for anti-money laundering should also apply to Internet-based payment systems.

- **Exploit opportunities for more efficient international cooperation.** Linking anti-money laundering measures and financial investigations with cybercrime investigations and computer forensics offers added possibilities for international cooperation. Governments should make use of the opportunities available under the Budapest Convention on Cybercrime, the Convention on the Laundering, Search, Seizure and Confiscation of Proceeds from Crime and the Financing of Terrorism (CETS 198) of the Council of Europe and the revised 40 Recommendations of the Financial Action Task Force (FATF). Consideration should furthermore be given to the findings of the MONEYVAL typology study on criminal money flows on the Internet of March 2012.[24]

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

# 7 - Strategic priority: Cooperation between law enforcement and Internet service providers

Cooperation between law enforcement agencies and Internet service providers (ISPs) and other private sector entities is essential for protecting the rights of Internet users and for protecting them against crime. Effective investigations of cybercrime are often not possible without the cooperation of ISPs. However, such cooperation needs to take into account the different roles of law enforcement and of ISPs as well as the privacy rights of users.

Enhanced law enforcement/ISP cooperation and public/private sharing of information in line with data protection regulations should become a strategic priority.

Governments should consider the following actions:

- **Establish clear rules and procedures at the domestic level for law enforcement access to data** held by ISPs and other private sector entities in line with data protection regulations. A clear legal basis in line with the procedural law provisions and the safeguards and conditions of the Budapest Convention on Cybercrime will help meet human rights and rule of law requirements. Guidelines[25] adopted at the Octopus Conference of the Council of Europe in 2008 may help law enforcement and ISPs organise and structure their cooperation. Governments should facilitate the use of the expedited preservation provisions (Articles 16, 17, 29 and 30) of the Budapest Convention taking into account the results of the assessments by the Cybercrime Convention Committee.[26]

- **Foster a culture of cooperation between law enforcement and ISPs.** Memoranda of understanding between law enforcement and Internet Service Providers are a fundamental tool in this respect. Regional coordination of such MOUs would facilitate the ability of law enforcement authorities to conduct investigations across regional borders, with the knowledge that comparable standards have been adopted in other States. MOUs combined with clear rules and procedures may also facilitate the cooperation with multi-national ISPs and other private sector entities including in the disclosure of data stored in foreign jurisdiction or on cloud servers that are managed by these ISPs.

- **Facilitate private/public information sharing across borders.** Private sector entities hold large amounts of data on cybersecurity incidents. The transborder sharing of such data would help improve the security of the information infrastructure as well as investigate offenders. Governments should consider legislation and the conclusion of agreements allowing for private/public information sharing and encourage the development of guidelines to facilitate the sharing of information intra- and transborder, including procedural, technical, legal and data protection safeguards.

[25] http://www.coe.int/t/dghl/cooperation/economiccrime/cybercrime/Documents/LEA_ISP/default_en.asp.
[26] Assessment report adopted by the T-CY in December 2012 http://www.coe.int/t/DGHL/cooperation/economiccrime/cybercrime/TCY2013/TCYreports/TCY_2012_10_Assess_report_v30_public.pdf

## 8 - Strategic priority: More efficient regional and international cooperation

Cybercrime and electronic evidence are transnational by nature, thus requiring efficient international cooperation. Immediate action is required to secure electronic evidence in foreign jurisdictions and to obtain the disclosure of such evidence. However, the inefficiency of international cooperation, in particular of mutual legal assistance, is still considered among the main obstacles preventing effective action against cybercrime.

Rendering international cooperation on cybercrime and electronic evidence more efficient should be a strategic priority.

Governments should consider the following actions:

- **Exploit the possibilities of the Budapest Convention on Cybercrime and other bilateral, regional and international agreements on cooperation in criminal matters**. This includes making full use of Articles 23 to 35 of the Budapest Convention in relation to police-to-police and judicial cooperation, including legislative adjustments and improved procedures. Governments (parties and observers to the Convention) should fully participate in the 2013 assessment of the international cooperation provisions of the Budapest Convention that is being undertaken by the Cybercrime Convention Committee (T-CY) and any follow up resulting from this assessment. They should follow up to the T-CY assessment of 2012 and promote the use of Articles 29 and 30 of the Budapest Convention regarding international preservation requests.

- **Provide for training and sharing of good practices.** Authorities for police and judicial cooperation should engage in domestic, regional and international training and the sharing of good practices. This should facilitate cooperation based on trust.

- **Evaluate the effectiveness of international cooperation.** Ministries of Justice and of Interior and Prosecution Services should collect statistical data on international cooperation requests regarding cybercrime and electronic evidence, including the type of assistance requests, the timeliness of responses and the procedures used. This should help identify good practices and remove obstacles to cooperation. They may engage with regional partners in an analysis of the issues adversely affecting international cooperation.

- **Strengthen the effectiveness of 24/7 points of contact.** Such contact points have been established in all States in line with Article 35 Budapest Convention, but their role needs to be enhanced and they may need to become more pro-active and fully functional.

- **Compile statistics on and review the effectiveness of 24/7 contact points** and other forms of international cooperation on a regular basis.