CyberCrime@IPA

EU/COE Joint Project on Regional Cooperation against Cybercrime

Assessment report

Criminal justice capacities on cybercrime and electronic evidence in South-eastern Europe

Results of the peer-to-peer assessments under the CyberCrime@IPA project

Strasbourg, 18 June 2013

Data Protection and Cybercrime Division, Council of Europe, Strasbourg

www.coe.int/cybercrime

Funded by the European Union and the Council of Europe

EUROPEAN UNION

COUNCIL OF EUROPE CONSEIL DE L'EUROPE

Implemented by the Council of Europe

CONTACT

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

Executive summary

Through the CyberCrime@IPA[1] joint project – launched in November 2010 and completed in April 2013[2] – the European Union and the Council of Europe, in cooperation with other partners, provided support to the Western Balkans and Turkey in their efforts to tackle cybercrime. The areas covered by the project were Albania, Bosnia and Herzegovina, Croatia, Montenegro, Serbia, "The former Yugoslav Republic of Macedonia", Turkey and Kosovo*.[3]

During the inception phase of CyberCrime@IPA, a detailed situation report was prepared for each of the eight project areas.[4]

Under Result 8 of CyberCrime@IPA peer-to-peer assessment visits were then carried out between October and November 2012 to determine progress made since the launch of the project. The present report reflects the outcome of these assessments. It includes an update reflecting activities carried out in the remaining months of the project, that is, between December 2012 and April 2013. The report was discussed in detail at the Regional Conference on Strategic Priorities (Dubrovnik, Croatia, February 2013) and the Closing Conference of CyberCrime@IPA (Budva, Montenegro, April 2013). Moreover, written comments have been received and incorporated. The report is now considered adopted.

The aim of the Assessment Report is to provide officials of project areas with information about progress made in respect of the eight expected results of the project. The report draws conclusions and makes recommendations for further action needed to ensure sustainability. In respect of each area, the report compares the situation reported at the beginning of the project and assesses progress made until the assessment visits. It is intended to supplement the previous reports drafted under the project and provide an updated assessment of each area's capabilities to counter cybercrime underlying problematic areas and making recommendations for action.

There is clear evidence that a great deal of progress has been made in the project areas in the implementation of mechanisms to counter cybercrime. The project engaged the authorities in all project areas in a broad process of reform towards a concerted and consistent approach to cybercrime. This process is based on a better understanding of cybercrime as a threat against society, as well as of the complex set of measures to be taken at national, regional and international levels to meet this challenge. It can rely on greater awareness of decision-makers and the involvement of a wide range of key institutions from each of the eight project areas.

With the contribution of the project, cybercrime is now considered a priority concern in the region by decision-makers, parliaments and governments. The need for cybercrime strategies – aimed at crime prevention and criminal justice – was tackled in many activities implemented by the project in order to ensure a comprehensive response to cybercrime and other offences involving electronic evidence. The launching conference of the project (February 2011) included a special session for policy- and decision-makers, and the project's approach was to involve decision-makers in almost all activities. This led to a greater awareness of cybercrime at the decision-maker level. The commitment of Ministers and senior officials was reaffirmed by the Declaration on strategic priorities regarding cybercrime adopted at the high-level Conference held in Dubrovnik on 15 February 2013.

The key achievements of this project have been in raising awareness, including through training activities, establishing networks, improving regional cooperation and bringing about legal reforms.

---

[1] Joint Project Regional Cooperation in Criminal Justice: Strengthening capacities in the fight against cybercrime

[2] While project activities ended on 30 April 2013, CyberCrime@IPA was extended to 30 June 2013 to allow for the completion of the MSC course at University College Dublin.

[3] *This designation is without prejudice to positions on status, and is in line with UNSC 1244 and the ICJ Opinion on the Kosovo* Declaration of Independence.

[4] Finalised March 2011.

All project areas are now aware and able to deal with a range of cybercrime and electronic evidence. They have mounted cybercrime prosecutions and had positive verdicts returned.

Elements of institutional capabilities required to engage cyber criminality are in place throughout all criminal justice systems within the region.

Practical achievements include:

- Legislation on cybercrime and electronic evidence is stronger and more in line with the Budapest Convention and rule of law and human rights principles
- Specialisation and specialised units in police and prosecution services has increased
- Law enforcement training has become more of a priority
- Judicial training has been or is on the way to being mainstreamed into judicial training curricular
- The ground has been prepared to ensure that in the future criminal money on the Internet can be seized and confiscated
- A culture of cooperation between public and private sector is emerging
- Countries and areas now do engage in regional and international cooperation against cybercrime and the securing of electronic evidence.
- A number of practical tools are available, ranging from good practice study on specialised cybercrime units, to a blueprint for law enforcement training strategies, judicial training materials or the electronic evidence guide.

This approach led to better cooperation in the region and an increasing number of successful investigations. Informal cooperation with neighbouring police and other law enforcement authorities is now extensive as a direct result of the networking opportunities provided by the trainings and activities organised under CyberCrime@IPA project.

International cooperation has increased through better use of existing bi- and multilateral and regional agreements, in particular the Budapest Convention on Cybercrime and other Council of Europe and European Union instruments, as well as channels of communications. Governments are actively participating in the work of the Cybercrime Convention Committee (T-CY) and they are advised to engage in cooperation with the newly created European Cybercrime Centre (EC3).

The project increased also the cooperation between Western Balkans and Turkey and countries of the Eastern Partnership region by organising joint activities with the joint European Union/Council of Europe CyberCrime@EAP project[5]. Furthermore, the project provided opportunities for project areas to establish contacts with countries from other regions of the world during the Octopus Conferences in 2011 and 2012 and the Internet Governance Forum (Baku, Azerbaijan, 6-8 November 2012).

Legislation throughout the region is harmonised to a great extent with relevant Council of Europe and European Union standards, in particular the Budapest Convention on Cybercrime. The project advised project areas in strengthening cybercrime legislation and prepared specific legal opinions and recommendations for Bosnia and Herzegovina, Montenegro, Serbia and "The Former Yugoslav Republic of Macedonia". Furthermore, Bosnia and Herzegovina (14 Nov 2012), Croatia (21 Sep 2011), Montenegro (25 Nov 2010), "The former Yugoslav Republic of Macedonia" (11 June 2012) and Turkey (7 Dec 2011) ratified the Convention on Protection of Children against Sexual Exploitation and Sexual Abuse (Lanzarote Convention). Serbia and Albania had already ratified this treaty.

The strengthening of specialised cybercrime or high-tech crime units was strongly promoted under the project. A "Good practice study on specialised cybercrime units" was developed jointly with the

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

European Union Cybercrime Task Force (EUCTF). This study was made available to the project areas to guide them in the establishment of such units. During the implementation of the project a Cybercrime Unit was established in August 2011 in Kosovo*, which is responsible for the investigation of offences committed against computer systems and data, as well as those committed by means of computer systems. A High-tech Crime Department was established also in Croatia in June 2012. The Department is located within the Service for Economic Crime and Corruption, National Police Office for Suppression of Corruption and Organized Crime. Furthermore, a new Cybercrime Department was created within the Turkish National Police. It has been stated that the recommendations from the good practice study developed under the project were considered when setting-up theses specialised units.

"The former Yugoslav Republic of Macedonia" made considerable progress in building its capability against cybercrime and exploring the opportunities to further improve the situation through activities such as creation of the specialised prosecution department and development of a centre of excellence. The work of the Cybercrime Unit has been formally recognised by receiving two awards from SELEC for their role in detecting and disrupting two regional criminal enterprises engaged in credit card and e-commerce fraud.

The facilities of the National Cybercrime Department of Turkey (Ankara) are probably the strongest in the region and probably amongst the best in the world. The forensic technicians are trained to a high standard, have excellent facilities and are well equipped. All police officers and police superiors learn general information about digital evidence including how to collect it. Turkey is unique in the region in terms of population, geographical situation, reliance on technology and their existing and continuing capability to deal with cybercrime and electronic evidence. They have established practices and procedures that are in accordance with international standards. There is a comprehensive Training Strategy document, which details an extensive programme of training activity for a variety of roles for new and existing officers. Other project areas could benefit from the experience of Turkey.

During the activities organised under the project, an important concern became obvious, namely, the difficulty for judges and prosecutors to deal with electronic evidence in court. Good practices from European Union Member States and other countries have been presented and discussed in different events. However, the project specifically followed up on this issue by developing a Guide on Electronic Evidence.

In order to respond to the need for judicial training on cybercrime and electronic evidence, identified during the inception phase, under the project:

- A training pack for basic judicial training was developed. The training material was designed to provide judges and prosecutors with an introductory level of knowledge on cybercrime and electronic evidence.
- 15 trainers from all project areas were trained in delivering judicial training on cybercrime and electronic evidence in their own country/area.
- Some 140 judges and prosecutors attended the basic in-country trainings on cybercrime and electronic evidence, which were delivered based on the training pack developed and by the trainers trained under the project (with assistance from international trainers).
- Over 100 judges and prosecutors that participated in basic course attended the advanced training developed and delivered by the project.

The judges and prosecutors trained are now aware of European Union and Council of Europe instruments, as well as the threat of cybercrime to the society. They are now in the position to disseminate this knowledge to their peers. Furthermore, consistent training has been provided for judges and prosecutors from the project areas to ensure that law enforcement powers are subject to conditions and safeguards. These brought the countries of the region closer to the human rights

standards of the European Union and the Council of Europe when investigating, prosecuting or adjudicating cybercrime or offences involving electronic evidence.

As a result, cybercrime training appears to have gained greater importance. It is reported that cybercrime training is now introduced or under consideration to be included in the initial training programme for all judges and prosecutors, which was not the case at the beginning of the project. In Albania, a training strategy was implemented and training to all police officers on handling electronic evidence was introduced.

The majority of the training institutions reported to have already included these modules in the curricula. However this training is still considered as specialized training and in most cases it is organized as part of the continuous training curricula, which is organized for judges and prosecutors that are already holding these posts. The judicial training institutions from Albania, Montenegro, Serbia, "The Former Yugoslav Republic of Macedonia" and Kosovo* reported that the training materials developed under the project are being introduced as training material for the initial and in-service training. Turkey reported that the material developed under the project was used to improve the course on cybercrime that was part of the initial training. Cybercrime training is considered very important; however, at this point it is very difficult to predict when the module will be included in the in-service training.

A Regional Pilot Centre for Judicial Training was established in Zagreb, Croatia. The national judicial training institutions from the region will interact with the Regional Pilot Centre for Judicial Training in view of updating training materials, documenting and disseminating good practices and providing regional training.

Serbia has wide ranging and extensive experience in dealing with cybercrime and has developed appropriate responses by both police and prosecutorial departments. During the period of the project it has improved its networking with other countries. Considerable progress has been made by Serbia in terms of judicial training in that there is now a training strategy in place, and training is scheduled for delivery as part of their programme in 2013. Serbia also intends to make use of the Guide on Electronic Evidence in its training programme and has delivered training at the international level through a number of projects.

All project areas had resources committed to financial intelligence and investigations. Coordination between these two elements appears to be challenging. The majority reported examples of asset confiscation. An important achievement in Serbia's fight against organised crime is the seizure and confiscation of illegally gained assets. Prosecution of offenders coupled with confiscation of assets has proved to be the most effective method for disrupting criminal enterprise. The financial regulatory services have enjoyed considerable success and have so far confiscated in excess of €100 Million from criminal activity. Such achievements are highly commendable. However, tracing money flows on the Internet is not possible by the majority. Those with the most sophisticated capabilities reported varying degrees of success. Access to databases and analytical software varied considerably. Many areas reported that investigation of this type of crime is obstructed by the need for legal proceedings to have been initiated before information may be obtained from financial institutions.

The project pursued a regional approach and generated dynamics of cooperation while bringing in other European and international expertise. In all events organised under the project, good practices were presented by partner countries (France, Italy, Slovenia and Romania), European Union Member States (e.g. Estonia, Germany, Ireland, Spain, Portugal, the Netherlands and United Kingdom), as well as from the private sector (Microsoft, German Internet Service Provider Association ECO). Synergies were created with a broad range of initiatives and organisations, in particular developed at the European Union level (e.g. Europol, European Cybercrime Training Education Group (ECTEG), Cybercrime Centres of Excellence for Training, Research and Education

(2CENTRE), the European Cybercrime Task Force (EUCTF), the Organization for Security and Co-operation in Europe (OSCE), and others).

The project areas began the project at different stages of their development and, therefore, also end the project with different capabilities. The level of networking between areas should be harnessed in the post project phase to enable best practice developed in one area to be spread across the region.

Overall, project areas should be congratulated on the progress that has been made and encouraged to ensure that these gains are not lost in the post-project period.

1 Introduction

CyberCrime@IPA comprised eight expected results. Result 8 required:

> Regional assessments carried out to determine progress made in terms of legislation, the strengthening institutional capacities for the investigation, prosecution and adjudication of cybercrime and international cooperation.

The present report reflects the results of the assessments implemented between October-November 2012[6] and is closely related to Result 1 on cybercrime policies and strategies. The rational in this respect was the following:

1. A situation report was prepared between November 2010 and February 2011 under CyberCrime@IPA assessing the situation in each project area with regard to legislation, specialised institutions and international cooperation, law enforcement training, judicial training, financial investigations and law enforcement/Internet service provider cooperation. That report thus established the baseline. It also made recommendations for reform.
2. CyberCrime@IPA supported activities related to the above-mentioned topics. These activities provided additional information and led to additional recommendations.
3. Peer-to-peer assessment visits were carried out to each project area to further complete the information of the situation report, review implementation of the recommendations made under the project (situation report and project activities). This resulted in the present Assessment Report for each project area that contains:
   - consolidated and accurate information on each of the themes covered
   - an analysis of the state of implementation of recommendations
   - specific recommendations for further action.
4. The draft Assessment Report was discussed in the Regional Conference on strategic priorities (Dubrovnik, Croatia 13-15 February 2013).
5. The report is to help project areas develop their cybercrime policies and strategies and when seeking further support through technical cooperation projects. The findings of the report are reflected in the Declaration on Strategic Priorities in the Cooperation against Cybercrime adopted by Ministers and senior officials in Dubrovnik on 15 February 2013.

The Assessment Report is based on and should be considered in connection with the following reports drafted under the project:

- Situation Report assessing the existent capabilities in the beginning of the project
- 1st Progress Report covering the period 1 March – 30 September 2011
- 2nd Progress Report covering the period 1 November 2011 – 31 May 2012
- 3rd Progress Report covering the period 1 June – 31 December 2012

The assessment process involved conducting interviews with the 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, the following institutions were visited:

- Ministry of Justice
- Prosecution Service Representatives
- High-tech Crime Units (including 24/7 point of contact)
- Financial Intelligence and/or Investigation Units

[6] An earlier version of the present Assessment Report was discussed in detail during a regional conference in Dubrovnik, Croatia, 13 – 15 February 2013, and again at the closing conference in Budva, Montenegro, 29 – 30 April 2013 . The present version reflects additional information received and activities carried out between January and April 2013.

- Judicial Training Institutions
- Police and Law Enforcement Training Institutions.

The Report covers the same topics that were subject of the Situation Report and that are being addressed by CyberCrime@IPA:

- Legislation (result 2)
- Specialised institutions and international cooperation (result 3)
- Law enforcement training (result 4)
- Judicial training (result 5)
- Financial investigations (result 6)
- Law enforcement – Internet service provider cooperation (result 7).

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

Legislation

The project addressed the state of cybercrime legislation recognising that without adequate criminalisation of this conduct a State cannot investigate and prosecute cybercrimes and, moreover, it cannot request for assistance of another State. The main instruments to be applied and the leading instrument in this area are the Budapest Convention (CETS 185) and its Additional Protocol on Xenophobia and Racism (CETS 189).

The Situation Report drafted in the beginning of the project evaluated to what extent project areas have implemented the Convention with a focus on certain aspects in view of possibly common progress. Apart from the content of the Convention and its Protocol, the report considered other regulations and instruments of the European Union and the Council of Europe to support the Budapest Convention. In addition, for the purpose of result 2 of the project legislative profiles of project areas were updated during the inception phase and are available online[7].

With the assistance from the project, areas are now aware of the need to:

- Strengthen legislation on cybercrime and draft amendments that consider the recommendations for improvement from the Situation Report. In this context, it is essential 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 implemented and applied with respect of human rule of law and human rights. The project made available a study on safeguards and conditions (Article 15 of the Budapest Convention on Cybercrime) to provide guidance to project areas and included Croatia as good practice[8].

Overall, the relevant laws in the project areas implement the Budapest Convention. Some project areas applied the minimum level required by the Budapest Convention, others went beyond. Some provisions of the Budapest Convention are not yet fully implemented while some unclear wordings provided by different laws, which were identified as being problematic in the Situation Report, might be in time solved by practice, court decisions or legal interpretations.

Considering the complex recent criminal law reforms that have been undertaken in the region, it became more necessary to assess the effectiveness of legislation than to pursue additional

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

[8] See: http://www.coe.int/t/DGHL/cooperation/economiccrime/cybercrime/Documents/Reports-Presentations/2467_SafeguardsRep_v18_29mar12.pdf

amendments in all project areas. The project therefore discussed at regional level practical cases and court decisions to obtain information about the effectiveness of legislation adopted. Where amendments were still feasible, specific activities were organised and legal advice was provided i.e. in Serbia, Bosnia and Herzegovina and Montenegro.

The implementation of the project coincided with the efforts undertaken by the Cybercrime Convention Committee (T-CY) to assess the implementation by Parties of Articles 16, 17, 29 and 30 on expedited preservation of stored computer data and disclosure of traffic data at domestic and international levels. This was an excellent opportunity to coordinate the efforts made by the T-CY Committee with the needs identified in the region. Adequate participation in the T-CY meetings was ensured from project countries (with the exception of Kosovo* all are Parties or signatory (Turkey)) to provide clarifications and guidance on the implementation of these important provisions. The recommendations made by the T-CY in its Assessment Report[9] should be considered by the Parties in future amendments.

A detailed analysis of the implementation of the Lanzarote Convention was provided through a discussion paper on the measures taken in 45 countries to criminalise conduct related to the sexual exploitation and abuse of children[10]. The standards of reference are the relevant provisions of the Convention on Cybercrime (Article 9 on child pornography) and the substantive law provisions of the Convention on the Protection of Children against Sexual Exploitation and Sexual Abuse. With the exception of Kosovo* all countries are covered by the paper. Project areas should consider the gasp identified in this report.

Specialised institutions & international legal cooperation

As previously mentioned, several project areas have undertaken reforms to establish such units and the project provided further assistance. Furthermore, on the occasion of depositing the instrument of ratification of the Budapest Convention, a Party has to indicate the 24/7 contact point responsible to assist in cybercrime investigations on expedited basis. The project succeeded to establish, clarify and network these contact points in the region as well as to increase their efficiency. Thus, several activities under the project provided training for the 24/7 contact points.

Project areas were advised to make best use of the existing channels of communication (24/7 Network, Interpol, EUROJUST, GPEN, SECI etc.) and where possible the contact point responsible for cooperation against crime to be the same for the other channels and avoid overlapping and proliferation of networks.

In order to network and exchange information and experience not only among countries covered by the project but between all Parties to the Budapest Convention, project areas (with the exception of Kosovo*) were encouraged to contribute to the discussions taking place in the Cybercrime Convention Committee meetings in 2011 and 2012.

The workshop on international cooperation (Istanbul, 10-12 April 2013) identified as the core problem the inefficiency of mutual assistance and the fact that the competent central authorities for MLA are too overburdened to give priority to "Article 31" requests for electronic evidence. The possible solutions discussed in the workshop will be dealt by the Cybercrime Convention Committee (T-CY).

---

[9] Available at:
http://www.coe.int/t/dghl/cooperation/economiccrime/cybercrime/TCY2013/TCYreports/TCY_2012_10_Assess_report_v30_public.pdf

[10] Available at:
http://www.coe.int/t/DGHL/cooperation/economiccrime/cybercrime/Documents/Reports-Presentations/2571_Child_benchmark_study_V32_pub_4_Dec12.pdf

During the implementation of the CyberCrime@IPA project all Parties covered by the project established 24/7 points of contact. The project has involved the points of contact in several activities to support their networking. In addition, the project supported the participation of 24/7 points of contact in several trainings (e.g. G8 3rd Training Conference of the 24/7 points of Contact, 8-10 November 2011).

Law enforcement training

Training is delivered throughout the region to varying levels. The training can range from seminars to ad hoc events, training courses and structured academically accredited courses. In addition, some project areas have published manuals of guidance. Full implementation of the national cybercrime training strategies developed under the project, role requirements and individual training plans would improve this situation.

The project:

- Drafted a strategy for law enforcement training with a regional component and specific strategies for each project area
- Ensured participation of one representative from each area in the Master of Sciences (MSc) programme in Forensic Computing and Cybercrime Investigation offered by University College Dublin (UCD)
- Investigators and other officials were trained on the need to ensure the rule of law and human rights principles (Article 15 of the Convention on Cybercrime - Safeguards and conditions)
- 24/7 contact points were funded to participate in a G8 training (Rome, Italy, 8-10 November 2011) and other trainings
- Law enforcement and prosecution services participated in the training on lawful interception of traffic and content data for law enforcement purposes, including legal, procedural and technical considerations and based on good practices
- Advised project areas to apply for European Cybercrime Training and Education Group (ECTEG) training materials developed with EU funding and managed by ECTEG and University College Dublin
- Advised areas to apply for membership in ECTEG and funded participation in the ECTEG meetings
- Organised a 1st responder training course (Oslo, 25 February – 1 March 2013) and prepared a 1st responders training package.

Further assistance for law enforcement is foreseen in the remaining months of the project (e.g. training material and training course for first responders as well as a train the trainers course).

Judicial training

There was a clear need to provide project areas with training materials. Thus the project has prepared:

- 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).

The materials developed were translated into local languages. Several activities are aimed at ensuring their integration into the curricula of the training institutions from the region.

The Judicial Pilot Centre was established - with the support of the project – within the Judicial Academy of Croatia and is aimed at disseminating good practice, carrying out researches and developing guidelines, training the trainers and facilitating exchanging of different experiences. It is necessary to identify lessons learned from other countries.

A meeting of the Heads of Judicial Training Institutions was organised on 25 March 2013 in Zagreb aimed at discussing the functioning and sustainability of the regional Judicial Pilot Centre. The priorities agreed on this occasion were the followings:

- Training on Electronic evidence
- E-learning
- Exchange of trainers
- Establishing a calendar of events
- Provision of Training of Trainers courses
- Development of materials

A Memorandum of Understanding will be signed by the Heads of the Judicial Training Institutions from the region to serve as the basis for the cooperation in the future.

Law enforcement/Internet service provider cooperation and financial investigations

Under this result, the project supported joint training courses carried out for cybercrime investigators, financial investigators and financial intelligence units, and helped establish regional and domestic trusted fora for regular information exchange between public and private sector stakeholders. Thus, it raised awareness of the need to confiscate proceeds from crime on the Internet and strengthened interagency and public-private cooperation against criminal money on the Internet.

In order to address this challenge, the projected made use of:

- The Council of Europe Guidelines for cooperation between law enforcement and Internet service providers cooperation (2008) developed under the Global Project on Cybercrime
- Typology study on criminal money flows on the Internet (2012) developed in cooperation with MONEYVAL and finalised with contributions from the project
- Octopus conferences (www.coe.int/octopus).

A number of activities organised under the project discussed this topic:

- Regional workshop on criminal money flows (Serbia, March 2011)
- Regional workshop on LEA/ISP cooperation (Albania, June 2011)
- Workshop on criminal money flows (Ukraine, February 2012)
- Octopus workshop on private/public information sharing (Strasbourg, June 2012)
- International workshop on public/private cooperation against cybercrime and criminal money on the internet (26-28 November 2012, Istanbul, Turkey)

Under the project several project areas concluded MOUs between LEA and ISPs.

Regional Law Enforcement Centre of Excellence

The establishment of a Centre of Excellence for Law Enforcement is recommended. Such a facility could extract tacit knowledge and expertise from practitioners, which would be distilled into operating manuals and training materials for the benefit of the whole region. This would promote self-sufficiency and reduce dependency on international experts. Such a facility might also have a lead role in developing new techniques and identifying technical and systemic vulnerabilities. Another advantage of this approach is that such a Centre may be able to take advantage of

existing centres of excellence that have been created in some 10 EU countries, by developing on-going relationships with them.

Internet Usage in Europe in 2010[11]					
EUROPE	**Population (2010 Est.)**	**Internet Users, Latest Data**	**Penetration (% Population)**	**User Growth (2000-2010)**	**% Users Europe**
Albania	2,986,952	1,300,000	43.5 %	51,900.0 %	0.3 %
Bosnia-Herzegovina	4,621,598	1,441,000	31.2 %	20,485.7 %	0.3 %
Croatia	4,486,881	2,244,400	50.0 %	1,022.2 %	0.5 %
Kosovo*	2,200,000[12]	700,000	37.35[13] %	0.0 %	0.1 %
"The former Yugoslav Republic of Macedonia"	2,072,086	1,057,400	51.0 %	3,424.7 %	0.2 %
Montenegro	666,730	294,000	44.1 %	0.0 %	0.1 %
Serbia	7,344,847	4,107,000	55.9 %	926.8 %	0.9 %
Turkey	77,804,122	35,000,000	45.0 %	1,650.0 %	7.4 %
TOTAL Europe	**813,319,511**	**475,069,448**	**58.4 %**	**352.0 %**	**100.0 %**

Internet Usage in Europe in 2012					
EUROPE	**Population (2012 Est.)**	**Internet Users, Latest Data**	**Penetration (% Population)**	**% Users Europe**	**Facebook Sept 2012**
Albania	3,002,859	1,470,000	49.0 %	0.3 %	1,084,880
Bosnia-Herzegovina	3,879,296	2,327,578	60.0 %	0.4 %	1,310,900
Croatia	4,480,043	3,167,838	70.7 %	0.6 %	1,573,340
Kosovo*	1,836,529	377,000	20.5 %	0.1 %	n/a
"The former Yugoslav Republic of Macedonia"	2,082,370	1,180,704	56.7 %	0.2 %	941,240
Montenegro	657,934	328,375	50.0 %	0.1 %	306,480
Serbia	7,276,604	4,107,000	56.4 %	0.8 %	3,513,820
Turkey	79,749,461	36,455,000	45.7 %	7.0 %	31,483,300
TOTAL Europe	**820,918,446**	**518,512,109**	**63.2 %**		

[2] http://www.internetworldstats.com/
[12] ≈ 2,200,000 is population in total, estimation by Statistical Office of Kosovo* - http://esk.rks-gov.net//
[13] 37.35% is % of households with internet (an average household has more than 7 members)

2 Albania

2.1 Cybercrime and the criminal justice system

2.1.1 The situation at the outset

Albania reported the following types of cybercrime occurring most frequently:

- Internet fraud, including the setting up and use of fraudulent websites in order to illegally obtain personal and financial data
- Credit card and banking card fraud. Use of forged or stolen credit cards
- Use of counterfeit banking cards obtained by methods like skimming (most of the time concerning foreign banking accounts). Selling stolen credit card data on the Internet
- Computer-related forgery. Most of the time in relation to social networks and concerning illegal access, impersonation of other person for the purpose of obtaining illicit financial profits. A special subcategory is added offering of illegally reproduced software
- Illegal access. Directed against websites of public and private entities in order to disrupt their functioning or cause harm to their societal image. Directed against computer system of private users and for the purpose of illegal obtaining of personal and financial data
- Offering and transmitting of child pornography material over the Internet.

2.1.2 Assessment and summary of progress made

The Cybercrime Department records indicated the following number of cases:

- In 2010, there were a total of 60 Cases
- In 2011, there were a total of 82 Cases
- Between Jan and Sept 2012 there were 78 Cases.

The Department continued to encounter all cybercrime acts identified in the Situation Report with increases in email hacking and web page defacements that have recently been experienced, including attacks on Government web pages. E-mail hacking, identity thefts, betting scams and attacks on, "on line" bank accounts are also increasing.

Statistics from the Tirana Joint Investigation Unit (JIU) for the first 9 months of 2012 indicate that 12 cybercrime cases were investigated with 3 cases pending, 7 cases sent to court and 5 cases sentenced. These cases relate to financial crimes, corruption, and abuse of official duty, tax crime and money laundering. Some child pornography cases have also been investigated but difficulties are experienced as the act of simple possession is not criminalised under Albanian criminal law.

Because the number of offences is relatively small, the development of expertise has not been as rapid as it might be in other countries. A number of needs were identified:

- Access to international IT and legal experts for advice
- Notifications regarding emerging crime trends
- Descriptions of associated "evidential" profiles and intervention opportunities.

2.2 Legislation

2.2.1 The situation at the outset

Albania ratified the Budapest Convention on 20 June 2002 and its Additional Protocol on Xenophobia and Racism on 26 November 2004. The Convention on the Protection of Children against Sexual Exploitation and Sexual Abuse was ratified on 14 April 2009.

The Criminal Code was adopted in 1995 (Law 7895 of 27 January 1995). In order to undertake the obligations required by the Budapest Convention, Albania enacted the Law 10023/27 November 2008 and amended the Law 9859/20 January 2008. The Criminal Procedural Code also adopted in 1995 (Law 7905/21 March 1995) was amended by Law 10054/29 December 2009). Additional laws were adopted that are relevant for these issues.

As indicated in the Situation Report, a number of provisions on substantive and procedural law provided by the Budapest Convention and its Additional Protocol have been implemented in Albania. The project identified and discussed possible gaps in the legislation that could prevent effective investigation of cybercrime, including money flows on the Internet, cooperation with Internet service providers and international cooperation.

2.2.2 Assessment and summary of progress made

Although the Situation Report had identified some gaps in the Albanian legislation, in general the existent provisions are largely in line with the Budapest Convention and its Protocol on Xenophobia and Racism. In addition, on the basis of article 5 of the Constitution all international treaties are part of national legislation, which means that definitions and other concepts should be understood in the same way as intended under Convention.

As legislation on cybercrime was adopted rather recently insufficient experience was gained in the prosecution of cybercrime. Thus, further amendments should be preceded by a comprehensive assessment of practice – including court decisions – in order to draw accurate conclusions on their efficiency. Both the project team and project management agreed during the implementation of the project that amending legislation at this point would have been premature.

Under the project, participation of Albania ensured in the assessment carried out by the Cybercrime Convention Committee (T-CY) on Articles 16-17 and 29-30 and legal advice was provided on the implementation of procedural safeguards and conditions (Article 15 of the Convention on Cybercrime), as well as on the relevant provisions criminalising sexual violence of children.

2.2.3 Recommendations

- Albania in the process of reviewing its criminal substantive and procedural law provisions to consider the recommendations made by the Situation Report
- Consider the recommendations made by the Assessment Report of the Cybercrime Convention Committee (T-CY) with regard to the implementation of the measures related to expedited preservation of computer data and disclosure of traffic data at domestic and international level (Articles 16-17 and 29-30 of the Budapest Convention).[14] It may be useful to organise additional training for law enforcement and service providers in the practical application the preservation provisions.

[14] Availabile at:
http://www.coe.int/t/DGHL/cooperation/economiccrime/cybercrime/TCY2013/TCYreports/TCY_2012_10_Assess_report_v30_public.pdf

- Consider addressing the gaps identified in the Discussion paper "Protecting children against sexual violence: The criminal law benchmarks of the Budapest and Lanzarote Conventions".[15]

2.3 Specialised institutions

2.3.1 The situation at the outset

There was no specialised high-tech crime unit established in the Albanian Prosecution Office. The existing special units against corruption and economic-financial crime have the competence to deal with cybercrime. These units are established in the main prosecution offices of the judicial districts. It was noted that in the future, due to the very special nature of cybercrime, there may be a need to set up specialised units. In the Albanian criminal justice system the prosecutor leads and controls the investigations conducted by the state police or other police structures with the authority to investigate.

Within the police, a Sector against Cybercrime had been created within the Directorate against Financial Crime, Department for Crime Investigation. This unit was responsible for applying police, scientific and procedural measures for the prevention, tracing, documentation and fight against cybercrime. A Computer Forensic Laboratory has also been established in the Institute of Scientific Police. It is responsible for the examination of computer devices and the documentation of computer related criminal offences.

There were 5 police officers in the central office of the Sector against Cybercrime (11 in the sections in the districts). The Sector of Digital Forensic had 6 experts, 4 of which were sworn officers and two civilian technical staff. This structure dealt with all types of cybercrime: computer frauds and forgeries, phishing, money theft through cloned credit cards, hacking and cracking, crime related to electronic trading, electronic procurement, child pornography on the Internet, illegal interception of computer data, skimming, and other crimes that can be committed on the Internet, covering the territory of Albania.

Obstacles identified in the investigation of cybercrimes were the lack of network, monitoring programmes and computer platforms to enable online investigations.

2.3.2 Assessment and summary of progress made

Albania has not created a specialised cybercrime unit in the prosecution office per se. However, there is a Joint Investigation Unit (JIU) that deals with economic crimes, money laundering, corruption and cybercrime. Four prosecutors tend to be allocated all cybercrime cases and are de facto, specialist cybercrime prosecutors.

Except Tirana, there are six JIU in the main prosecutor offices:

- Durres 4 Prosecutors
- Shkoder 4 Prosecutors
- Vlore 3 Prosecutors
- Fier 3 Prosecutors
- Korce 3 Prosecutors
- Gjirokaster 3 Prosecutors.

The Sector against Cybercrime in Tirana has seen a small increase in staff (5 investigators and 7 forensic analysts). There are 6 satellite units in the main conurbations, as well as another 7 forensic examiners. They belong to a committee which meets quarterly with the Albanian Banking

[15] http://www.coe.int/t/DGHL/cooperation/economiccrime/cybercrime/Documents/Reports-Presentations/2571_Child_benchmark_study_V32_pub_4_Dec12.pdf

Association to examine the problem of credit card fraud. The committee's agenda includes, inter alia, identification of: emerging criminal trends and tactics; crime series and systemic weaknesses being exploited; preventative measures and security issues designed to reduce cybercrime and criminal opportunities.

This unit serves as the 24/7 contact point, with the Interpol Desk taking out of hours calls. It is able to assist with intelligence and local knowledge of systems and procedures.

Cybercrime Response Teams have been established to assist first responders with the correct handling and processing of sources of digital evidence. These specialist officers can be deployed at short notice to assist at crime scenes. They have all received advanced investigative cybercrime training to enable them to fulfil this role.

A manual of guidance - "Investigation of Electronic Crime and Computer Evidence" - has been developed for police officers. This manual has the status of a police "General Order", which makes compliance with its content mandatory.

The Forensic Laboratory has sufficient equipment and software to enable them to carry out "computer" examinations. They have FRED machines and access to ENCASE, FTK and XRY for mobile phones.

The Cybercrime Unit would require in the future more specialist software, in particular to facilitate monitoring Internet activity and following money flows. It would also need more training and specialised staff.

2.4 International cooperation

2.4.1 The situation at the outset

Mutual Assistance is coordinated by the Central Authority (Ministry of Justice). Incoming MLA-requests are sent to the General Prosecution Officer that is in charge of their execution, if international instruments enable the granting of the request. Requests from district courts and prosecution officers are sent to the Central Authority and from there to foreign authorities. In urgent cases direct cooperation is possible while notifying the Ministry of Justice.

In 2010, one MLA request was received from Greece and Albania made five MLA request to Germany, Malaysia and Spain.

Access to and obtaining data located in US servers is done through Interpol, Contact Officers and other cooperation bodies, and of course by sending letters rogatory.

Albania has been involved in cases of direct exchange of information on cybercrime cases with the countries in the region in the form of joint meetings. This is only for exchanging of information as a letter rogatory is needed in order to obtain information in evidential form. Examples of cases include investigations concerning the use of blank plastic cards with magnetic stripes with banking information that were used to withdraw money from ATMs in Albania.

The 24/7 contact point was not established in the beginning of the project.

2.4.2 Assessment and summary of progress made

The law on International Legal Cooperation introduced strict time limits for dealing with requests from abroad. These time limits depend upon the nature of the request made.

In 2012 there were the following cybercrime MLA requests:

- 6 made to other countries (Nigeria, UK and Spain)
- 7 received from other countries.

The Sector against Cybercrime now serves as a 24/7 point of contact in line with Article 35 Budapest Convention. However, the number of requests remains small and this channel is so far mainly used for cooperation with European countries.

Within CyberCrime@IPA the 24/7 contact point participated in several international trainings (e.g. Octopus Conference, G8 training), as well as in several specific activities organised under project that targeted international cooperation and training for 24/7 contact points in the region. Furthermore, the project facilitated a large representation from each area in the Octopus Conference and the Cybercrime Convention Committee (T-CY) Plenary meetings. Among the themes discussed were transborder access to data and jurisdiction in the context of cloud computing, public-private information sharing, international cooperation, specialised units etc.

2.5 Law enforcement training

2.5.1 The situation at the outset

The institution responsible for law enforcement training in Albania is the Department for Police Training, the Centre for Police Training, Tirana. There was no documented cybercrime training strategy in place in Albania. The annual matrix of planned normal training activities was and is approved at the beginning of each year and its implementation is obligatory. It includes training activities on cybercrime that will be conducted by trainers in the General Police Directorate, as well as those to be conducted by partner police bodies, foundations, programmes, etc.

There was no structured programme of cybercrime training events in Albania and they relied very much on events being provided by external international bodies such as US Department of Justice (ICITAP) and the Police Assistance Mission of the European Community to Albania (PAMECA). Although new recruits were taught basic computer skills and how to use software, there was nothing in relation to the identification and handling of digital evidence, within their programme. Officers did not have individual training plans. The Department for Police Training offered training by lectures from the cybercrime units on topics such as: "The construction and functioning of the internet networks", "Identification of IPs", "types of Cybercrime and their investigation".

2.5.2 Assessment and summary of progress made

Under the project:

- Investigators and other officials were trained on the need to ensure rule of law and human rights principles (Article 15 of the Convention on cybercrime - Safeguards and conditions) when applying the measures foreseen under the Budapest Convention to investigative cybercrime.
- One law enforcement representative from Albania (Head of Sector against Cybercrimes, General Directorate of State Police) was funded to participate in the Master of Sciences (MSc) programme in Forensic Computing and Cybercrime Investigation offered by UCD.
- Law enforcement and prosecution services participated in several trainings (e.g. on interception of traffic and content data for law enforcement purposes), study visits and other activities that resulted in enhanced capabilities of law enforcement and judicial authorities to detect, investigate, prosecute and adjudicate cybercrime.

The police training plan for 2011 included 4 training events offered by the Hans Seidel Foundation in Germany. The topics were computer crimes, crimes in illegal interference on the Internet, theft by means of telephones and credit card frauds.

At the beginning of 2011, a 7-day training course was held on the topic "Basic Investigation of Computers and Electronic Crimes Program" in cooperation with International Criminal Investigative Training Assistance Programme organized by the US Department of Justice (ICITAP). The attendees at the training were cybercrime investigators, as well as prosecutors and judicial police officers.

Basic training is now given to all police recruits on electronic evidence, sources, preservation, search and seizure. Advanced training is given to specialist officers involved in this field. Cybercrime Response Teams have been established that can be deployed to crime scenes when requested to do so by first responders. The Cybercrime Unit are used to deliver this advanced training.

A training strategy has been drafted which details in service training needs and delivery methods up until the end of 2013. Furthermore, there is a training database capable of identifying individuals, trainings received against a profile of the training they need for their particular role.

There does not appear to be a corresponding HR strategy designed to preserve expertise and prevent unnecessary training effort from being delivered as a result of ephemeral deployments. It was felt that a tenure policy[16] for specialists might assist to build expertise and develop a corpus of knowledge in this field.

As previously reported, a number of training events sponsored by the international community are delivered within the Academy. They have forged good relationships with industry and have received training delivery support from Microsoft, the Albanian Telecommunications Industry and the Department of Technology and Information.

Commencing in 2013, training will be conducted in their regional training centres. Most of the expertise and knowledge has so far been developed in Tirana and it is recognised that this needs wider promulgation.

A Board has been established with a mandate to improve professional standards throughout all law enforcement agencies. Cybercrime capabilities feature high on this Board's agenda. As a result, The Police Academy now delivers more hours of cybercrime training than is delivered on drugs and terrorism.

The inclusion of cybercrime in the draft training strategy and the introduction of training to all police recruits in the handling of electronic evidence reflect important progress. Cybercrime training appears to have gained greater importance with the inclusion of such training at various levels within the police service.

2.6 Judicial training

2.6.1 The situation at the outset

The institution responsible for training of judges and prosecutors is the Magistrates School of the Republic of Albania. The School is a public institution, which enjoys administrative, academic and financial autonomy for the purposes of accomplishing its goals and responsibilities. The main duties of the School are the initial professional training of judges and prosecutors through a three-year programme, and the in-service training of judges and prosecutors. In conformity with the law or upon a request by interested institutions if there is enough capacity created by the initial training and continuous training of magistrates, the School may conduct professional training activities for court administration employees or other legal professions related to the justice system.

[16] A requirement to serve a minimum period within a particular post

There was no single strategy for training judges and prosecutors in the areas of cybercrime and digital evidence and no specific training was offered in the programmes of the School; however, the initial training programme was spread over three academic years and cybercrime was treated within different subjects during the first and second year. Activities related to this topic had also been included in the continuous training programme. In the framework of the three-year programme for the continuous training of in-service judges and prosecutors, a number of training events in the area of cybercrime had been organized.

Within the framework of the in-service training programme, the School of Magistrates had organised seminars on the topic of cybercrime, both for judges and prosecutors (since November 2009 four seminars had covered computer crime, computer related offences, computer fraud, insurance, subsidies and credit fraud).

It was considered that training for judges and prosecutors should be provided at the basic level. The prosecutors working in the task force covering the computer crime investigations should receive advanced training. There should be a complete training system according to a curriculum based on a model from one of the European Union countries.

2.6.2 Assessment and summary of progress made

A basic training course was delivered by the project in cooperation with in the School of Magistrates of Albania. However, not all 20 participants completed the course. A basic level of training on cybercrime and digital evidence is now included in initial training for all judges and prosecutors.

Two representatives from Albania (one public prosecutor and one prosecutor member of the Joint Investigation Units (JIU)) participated in the train the trainers course.

It is reported that cybercrime training is now included in the initial training programme for all judges and prosecutors, which was not the case at the beginning of the project.

From the on-going academic year (October 2012- June 2013), the School of Magistrates has started the new initial training program that includes cybercrime at basic level and is delivered by an investigator and an IT expert.

The School of Magistrates needs to consider the interest of prosecutors and judges in order to identify the nature and type of training they require. Thus the School has sent the program for the on duty training program for judges and prosecutors, in order to identify their interest and needs regarding cybercrime training. The number of participants and the necessary training required would determine the number of times and the type of training that will be delivered and inform the training strategy for 2013 to 2015. Three seminars are planned for 67 judges and prosecutors for the period 2013-2015.

Due to relatively limited exposure to this type of offences there is currently insufficient expertise and thus support from international experts is required to deliver future training activities.

2.7 LEA/ISP cooperation

2.7.1 The situation at the outset

There are about 80 ISPs operating in the territory of Albania, which are divided in two categories: main/primary ISPs and secondary ISPs. The main/primary ISPs have the greatest number of users and bigger capacities whereas the secondary ISPs are subcontracted by the main ISPs. The Authority of Electronic and Postal Communications issues licenses for ISPs. They are registered in the National Registration Centre as companies offering Internet service.

One of the main problems identified in dealing with ISP's and access to their data was the inability of the police to obtain preliminary information about the identity of Internet users/ISP subscribers, due to personal data and privacy protection policies of the ISPs. Information can only be obtained through the prosecutor and only if there has been a criminal investigation initiated jointly by the police and the respective prosecution office. In the cases of police investigations, the information from the ISPs is obtained through the Sector for the Interception of Telecommunications and relations with the Intelligence Services in the General Prosecution Office. As devices for the interception of traffic data are being installed both by the General Prosecutor and the ISPs, this is seen as a temporary issue. ISPs currently lack the facilities that enable the accurate identification of users.

In order to obtain traffic or content data the prosecution office makes a request to the respective court. If approved, the order is sent to the judicial police for execution. ISPs have the obligation to provide the required data. The State Police has not nominated specific contact points and no information was provided regarding any such contact points of ISPs.

Data retention is obligatory under Article 101 of the law on electronic communications in Albania. There were no agreements in place for law enforcement and ISPs to cooperate with each other, nor any training programmes for the parties.

Together with other jurisdictions they have experienced some difficulties with securing prompt cooperation from some ISPs.

There were also some procedural issues to be noted: preservation orders require a judge's order. Disclosure of an IP address requires an order from a prosecutor. However, data can only be obtained where there is a "case". This in general terms only exists when there is a reported crime.

2.7.2 Assessment and summary of progress made

AKEP[17] was established in order to regulate the operations of ISPs. They issue licences to companies when they are satisfied that they are able to comply with a number of legal requirements such as preservation and retention of data. This organisation has only recently been established and so its regulatory activity has been so far limited.

In practice in Albania there are not many cases of data collection, even if the changes in the Criminal Procedure Code of 2008 the country regulated the manner of collection of data. In order to obtain traffic or content data the prosecution office makes a request to the respective court. If approved, the order is sent to the judicial police for execution. ISPs have the obligation to provide the required data. On 7 February 2013 an agreement was concluded with 4 mobile operators to cooperate with law enforcement.

Data retention is obligatory in Albania under the law on electronic communications of 2008. Based on the law on electronic communication, the ISPs have to keep data for a maximum of 2 years. The minimum time for the data retention depends on several things, mainly on the type of data. The minimum can be 1 year in most cases however the data retention for the purpose of penal proceedings is maximum 2 years.

Under CyberCrime@IPA several activities organised in Belgrade, Kyiv and Istanbul targeted the cooperation with the private sector with the aim to develop a culture of cooperation.

[17] http://www.akep.al/

2.8 Financial investigations[18]

2.8.1 The situation at the outset

The main types of fraud affecting Albania included and still include on-line purchase of travel tickets using stolen credit card data, which have been successfully investigated, and online unlicensed gambling, which has been identified but not investigated.

This is a new area for the Albanian authorities and as such they have identified the following as shortcomings in their ability to be effective in the control and prevention of these activities:

- Lack of experience on the part of judges, prosecutors, judicial police officers and financial experts in the investigation of these crimes
- Although an improvement in the level of referrals is noted, the referral of suspicious activities on the Internet by those having an obligation to report remains low
- The Albanian Banks have little tradition and as a result their personnel do not have the necessary professional level required for the detection and referral of suspicious activities in the area of Internet money laundering
- The existence of the informal economy, use of cash transactions and financial activities happening outside the banking system.

Financial investigations are the responsibility of the following organisations:

- The State Police (Directorate against Financial Crimes), Ministry of Finance (General Directorate for the Prevention of Money Laundering) FIU (The Unit for the Supervision of Gambling), General Prosecution Office, High Inspectorate for the Declaration of Assets, High State Audit, State Intelligence Service, General Directorate of Customs and the General Tax Administration.

The institutions responsible to deal with the search and seize of proceeds of crime on the Internet are: Ministry of Finances (General Directorate for the Prevention of Money Laundering) (GDPML) - FIU (Unit for the Supervision of Gambling).

There has been cooperation between the State Police and the Unit for the Supervision of Gambling for the identification and discovery of illegal gambling organised through the Internet, which is an activity that involves crime (tax evasion). There has been cooperation with the FIU in relation to suspicious transactions performed on the Internet.

2.8.2 Assessment and summary of progress made

So far the authorities have not encountered any cases of money laundering on the Internet or criminal use of Internet banking.

There are 28 defined criminal acts, including cybercrime, with an associated asset confiscation liability. All prosecutors have a legal obligation in such cases to seek and confiscate criminal assets. Since 2010, approximately €7 Million worth of assets have been confiscated. It was not possible to identity what proportion was attributable to cybercrime or electronic evidence. The relevant law places the burden of proof upon the prosecution in the first instance to show suspicion that assets are the result of illegal activity. Thereafter the burden shifts to the defendant to prove the assets are legitimate. These matters fall under the competence of the civil court and thus it is possible to have an acquittal within the criminal system, which results in assets being confiscated within the civil system.

[18] For detailed reports on the functioning of the anti-money laundering systems see the MONEYVAL evaluation and progress reports at: http://www.coe.int/t/dghl/monitoring/moneyval/Countries/Albania_en.asp

During the implementation of the project Albania identified gaps in the legal framework aimed at the prevention of criminal money flows on the Internet (e.g. absence of simplified procedures to enable effective communication between institutions) to be considered as well as need for training of the staff.

2.9 Progress made against previous recommendations

Cybercrime situation report March 2011	**Progress reported**
Keeping statistics that provide an insight in the seriousness of cybercrime in the national territory. Such statistics could for example 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.	Not Completed
Keeping statistics on application of the specific powers in the criminal procedural code, including with information about application, technical details and cases concerned.	Not Completed
Review of national criminal law and criminal procedural law in the domain of cybercrime taking into account the observations made in the country report. In particular, attention is demanded of the legal concept of seizure of computer data and the possible need for expedited execution of investigative powers.	Completed
Review of MLA-procedures with a view to accelerate the handling of requests in cases where digital evidence is concerned.	Completed
Consideration of the formation of specific prosecution unit to combat cybercrime in accordance with the needs of the country.	Partially Completed
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
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
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 the global Project on Cybercrime.	Partially Completed
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"	Not Completed
Incorporate 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
2nd Progress report 1st November 2011 - 31 May 2012	**Progress Reported**
Increase the efficiency of the 24/7 contact point.	Partially Completed
Sign an agreement on cooperation with EUROJUST.	Work in Progress
Organising training courses on cybercrime, in particular for prosecutors, judges, Ministry of Justice personnel responsible with MLA requests.	Completed

Standardisation of MLA requests.	Completed
Develop training manuals, including a glossary of the terms the cybercrime field.	Completed
Consider electronic communications on MLA between Parties to the Conventions	Partially Completed (T-CY is also reviewing international cooperation provisions of the Cybercrime Convention)

2.10 New recommendations

1. Maintain statistics in order to assess the effectiveness of all aspects of the criminal justice process.

2. Review existing Human Resource Strategies to ensure they are appropriate. The authors of any such strategy should be encouraged to consider implementing a tenure policy for specified specialist posts.

3. Continue to develop the training strategy for judges and prosecutors and include continuous career development opportunities.

4. Continuous training and capability development by specialist cybercrime investigators based upon identified capability gaps.

5. Conclude a Memorandum of Understanding with AKEP to establish a forum and processes for dealing with ISP problems and issues.

3 Bosnia and Herzegovina

3.1 Cybercrime and the criminal justice system

3.1.1 The situation at the outset

State level: At the State level the Criminal Code did not contain cybercrime provisions. That is left to the criminal codes of the entities and district.[19] For that reason no criminal statistics about cybercrime were kept.

Federation: Examples of the types of crime reported are:

- DoS and DDoS attacks, mostly directed against web-sites of private companies for the purpose of extortion
- Internet fraud, where citizens of Bosnia Herzegovina were victims
- Unauthorised access to computer systems and networks thereby damaging legal entities in Bosnia and Herzegovina
- Credit cards scams – by means of skimming and phishing
- Wireless network abuse
- Child pornography on the Internet.

Statistics of Police Administration of the Federation, in particular the Department for Economic Crime, Anti-Corruption, Money Laundering and Computer Crime, together with the prosecutor's office filed 47 reports concerning 79 suspects of different cybercrimes.

Republika Srpska: The majority of the cases relate to child pornography on the Internet, unlawful access to databases and abuses of social networks. A lower number of crimes committed concerned misuse of credit cards and electronic fund transfer scams. Because of the recent enactment of cybercrime legislation no statistics were available.

Brčko District: The Brčko District did not avail of statistic cybercrime material. The number of criminal investigations to cybercrime investigations had been very limited. In the questionnaire it was referred to one case of data interference and some cases of Internet fraud and attempted Internet fraud.

Prosecutors reported challenges in prosecuting cases such as court demands for the physical presence of "the forged credit card". This is not always possible as there isn't a tangible credit card, only a virtual one.

Courts have also been requesting paper copies of evidence and transcripts of audio files. Printing the entire contents of a 1TB hard drive is not practical and indicates a level of basic technical misunderstanding. This may have its roots in legal tradition rather than a legal obligation.

3.1.2 Assessment and summary of progress made

Within BiH some prosecutors are dealing with cybercrime cases but this is not their exclusive responsibility and they are not well trained in cybercrime and electronic evidence. Prosecutions have been initiated for a wide range of cybercrimes. There have been successful prosecutions for cases of child pornography, credit card fraud, distribution of malware, abuse of stock market, using fake credit cards to fund terrorism. There were verdicts in some cases whilst others are on-going.

[19] Apart from criminal law on copyright, see under Article 10 (Offences related to infringements of copyright and related rights) Convention on Cybercrime

The Federation has instituted legal procedures in respect of credit card fraud, economic espionage, on line fraud, malware DDoS attacks, child pornography and terrorism.

The Brčko district, in the past 2 years, instituted legal procedures in respect of 4 cases, which were on-going for offences of child pornography and on line private abuse of data. A public awareness campaign to encourage the public to report cybercrimes was recently launched.

The Republika Srpska has instituted legal procedures in respect of credit card fraud, malware, child pornography, DDOS attacks and online fraud.

3.2 Legislation

3.2.1 The situation at the outset

Bosnia Herzegovina ratified the Budapest Convention and its Additional Protocol on Xenophobia and Racism on 19 May 2006.

These international instruments were used and implemented by the State and the entities as a model/guideline for the amendment of their internal criminal laws. In fact, in Bosnia Herzegovina four sets of criminal law/criminal procedural law apply. Although these laws are very similar, with regard to cybercrime some important divergences can be established. Accordingly, the legislation at the State and entities level has to be considered in order to obtain a complete overview of the present status of measures against cybercrime in Bosnia and Herzegovina. In some areas the state has exclusive legislative jurisdiction, as well as entities.

At the state level some definitions have been included in the Criminal Procedure Code, which are similar to Article 1 of the Convention. The competence for ensuring the specific legal framework for investigating and prosecuting cybercrimes belongs to the entities and district. A detailed analysis of the existent provision was provided in the Situation Report, which was prepared in the beginning of the project. The Report, as well as the regional workshop on legislation held in Sarajevo in on 24-25 May 2011, identified several gaps in the legislation of Bosnia and Herzegovina, Furthermore, it made recommendations for improvement, in particular to review the criminal procedural law at all levels e.g. expedited execution of investigative powers, collection of traffic data and the interception of electronic communications.

Among the entities, Republika Srpska enacted amendments to the Criminal Code concerning criminal offences against security of computer data (OJ 73/10, 30 July 2010) in force from 7 August 2010. This law amended the Criminal Code by inserting a specific chapter XXIVa comprising of seven new articles.

3.2.2 Assessment and summary of progress made

Bosnia and Herzegovina (State level, Republika Srpska, Federation of BiH and Brčko District) needs to reach a better harmonisation. The Ministry of Justice has a moderating team responsible for examining provisions that should be incorporated in BiH legislation and how to be implemented at the entities level (TEAM for tracking the implementation and harmonization of legislation in Bosnia and Herzegovina).

During the 2nd Steering Committee meeting (Budva, Montenegro, 12 September 2011), the delegation of Bosnia and Herzegovina reconfirmed the request for a country specific workshop on legislation. The specific Workshop on legislation was organised in Sarajevo on 26 March 2012 and it was aimed at providing further assistance on cybercrime legislation to the country.

The Workshop discussed the provisions that require further reform in order to fully implement the Budapest Convention and the European Union standards. It reviewed the gaps identified at state,

entities and district level and discussed possible amendments to the legislation. Subsequently, a document with specific recommendations was prepared by the project, translated and submitted for consideration to the TEAM for tracking the implementation and harmonization of legislation in Bosnia and Herzegovina.

Currently, the Ministry of Justice is drafting amendments to the Criminal Procedure Code at the state level with the assistance from the project.

During the implementation of the project, Bosnia and Herzegovina was included in the analysis provided by the Discussion paper "Protecting children against sexual violence: The criminal law benchmarks of the Budapest and Lanzarote Conventions". This report identified some gaps in the legislation concerning protection of children against sexual violence.

On 14 November 2012 (during the implementation of the CyberCrime@IPA project) Bosnia Herzegovina ratified the Convention on the Protection of Children against Sexual Exploitation and Sexual Abuse (Lanzarote Convention).

3.2.3 Recommendations

Additional measures and solutions need to be identified to fill the legislative gaps at the level of entities and district. Under the project, it resulted that closing the legislative gaps identified within different activities of the project is a matter of urgency. Thus the authorities in Bosnia and Herzegovina should:

- Amend current legislation in the light of the Situation Report (2011) and the Recommendations made in 2012
- Consider the recommendations made by the Assessment Report adopted by the Cybercrime Convention Committee (T-CY) with regard to the implementation of the measured related to expedited preservation of computer data and disclosure of traffic data at domestic and international level (Articles 16-17 and 29-30 of the Budapest Convention)
- Consider the gaps identified in the Discussion paper "Protecting children against sexual violence: The criminal law benchmarks of the Budapest and Lanzarote Conventions".[20]

3.3 Specialised institutions

3.3.1 The situation at the outset

Federation: There was no specialised unit exclusively established to deal with high tech crime in the Federation of BiH. Within the Federation Police Administration there is the Department for Economic Crime, Corruption, Money Laundering and Computer Crime, which is responsible for detection, investigation and providing evidence in relation to computer crimes identified by the Criminal Code of the Federation of BiH. The division of responsibilities between prosecutors and law enforcement units in BiH (police) is specified by the provisions of the Criminal Procedure Code of the Federation of BiH. There are 6 police investigators within Department for Economic Crime, Corruption, Money Laundering and Computer Crime.

A Forensic and Support Centre is operating within the Federation Police Administration. There was no position of an IT expert who could provide expertise on digital evidence.

The Federation had identified that the speed at which information is obtained through the Interpol and international legal assistance mechanisms is the main difficulty in performing its assigned

[20] http://www.coe.int/t/DGHL/cooperation/economiccrime/cybercrime/Documents/Reports-Presentations/2571_Child_benchmark_study_V32_pub_4_Dec12.pdf

tasks, especially in view of requesting information from companies such as Google and Yahoo, which are based in the USA.

Republika Srpska: A High Tech Crime Unit (the Special Investigation Unit) had been established within the Ministry of Interior, the Administration of Criminal Police. The Prosecutor's Office has no such specialised structure. The High Tech Crime Unit is competent to investigate offences committed against computer systems. The Unit has its own digital forensics laboratory, which meets its own needs and those of other organisational units in the Ministry of Interior. The Unit is in the process of preparing an official publication of procedures for seizure of digital evidence that are expected to enter into force in 2011. The Unit currently employs 9 members of staff; however an increase of staff and the setting up of a regional office were anticipated.

Brčko-District did not have its own digital forensics laboratory, or trained forensic investigators. The police, based on court's order if necessary, collect the evidence, which is then submitted upon the prosecutor's order to an authorised expert witness.

No high-tech crime unit had been established in the Police of Brčko District due to its specific territorial and subject matter jurisdiction. However, since 2008, three police officers of the Criminal Police Unit have been systematically trained (one of the Economic Crime and Corruption Department, one of the Organised Crime Department and one of the Criminal Intelligence Support and Anti-terrorism Department). It was recognised that the police were not competent to deal with offices against computer systems. Should such cases require investigation, the police would have enlisted the support of an IT expert.

3.3.2 Assessment and summary of progress made

At the State level, the Security Investigation and Protection Agency (SIPA) deals only with IPR crimes and do not have a cybercrime capability per se. At present they have very limited capabilities. Regulatory Communication Body has national competence under Ministry of Communication.

The Federation of BiH has no Cybercrime Unit but 4 investigators deal with cybercrime matters (not exclusively) and 2 deal with child pornography cases. There is no computer forensic capability and any examinations needed are outsourced to the Forensic Department of the Republika Srpska.

The Republika Srpska has a specialised Cybercrime Unit. It consists of 9 persons and includes a computer forensic capability. There are plans to separate the forensic capability from the investigative part.

The Brčko District does not have a Cybercrime Unit; however, 4 police officers within Organised Crime deal with cybercrime (not exclusively). There are plans to make them a specialised team. They can do some basic forensic searching using an old version of Encase but have no detailed forensic capability.

A law enforcement officer from the Federation of BiH is funded by CyberCrime@IPA to participate in the MSc in Forensic Computing and Cybercrime Investigation (University College Dublin).

As previously stated the project advised in setting up specialised units and representatives from Bosnia and Herzegovina participated in the development of this Good Practice Study. In almost all activities organised by the project, Bosnia and Herzegovina benefited from a larger representation than the other project areas on the consideration that participation at all levels (state, entities and district) needs to be ensured.

There is an action plan and strategy at the State Level to ensure the deployment of a CERT during 2013. The Republika Srpska has already a CERT.

There is a clear difference between the capabilities of the State, entities and Brčko district. There is collaboration between Republika Srpska and the Federation with the latter drawing on the formers digital forensics capability.

3.4 International cooperation

3.4.1 The situation at the outset

At the State level the procedure for providing mutual legal assistance in criminal matters follows the provisions of the European Convention on Mutual Legal Assistance in Criminal Matters and its Protocols to which Bosnia and Herzegovina is a Party, as well as the provisions of multilateral and bilateral agreements on legal assistance that are binding on Bosnia and Herzegovina.

The procedure for providing mutual legal assistance in criminal matters is regulated by the Law on Mutual Legal Assistance in Criminal Matters that entered into a force on 15 July 2009. The Ministry of Justice is the central authority for executing mutual assistance requests in criminal matters received from foreign authorities (including prosecutors, courts, police and the etc.). After that the competent authority in Bosnia and Herzegovina (courts, prosecutor's office, police bodies) directly acts upon the request of a foreign authority, and decides whether the request can be granted and in what way.

International police to police cooperation was provided through Interpol channels and is restricted to the exchange of information. No joint police teams were established.

In the Republika Srpska unilateral trans-border investigative actions are allowed under domestic law. Requests for MLA in criminal cases Brčko-District are issued by the courts or by the prosecution service. A request is submitted to the Judicial Committee of Brčko District and then forwarded to the competent Ministry of the State BIH. There were no experience obtained and no statistics concerning incoming and outgoing requests in the field of cybercrime.

The establishment of a 24/7 contact point was within the competence of the State of Bosnia Herzegovina and it resulted from the project activities that it was not functional.

3.4.2 Assessment and summary of progress made

The Ministry of Justice is the Central Authority for sending and receiving all requests for MLA and has a specialised department responsible. It is estimated that a request received from abroad takes between 3/5 days to 1 month to be executed depending on the complexity of the request.

The competent authorities are courts or prosecutors who are able to execute MLA requests.

So far 10 requests have been sent through the 24/7 contact point for assistance but no requests for assistance have been received.

There were examples of international cooperation and joint investigations with LEAs from abroad:

- A case investigated with the USA concerned stealing and altering data from a pharmacist website.
- Child Pornography
- Credit card fraud and terrorism.

Within the Republika Srpska the Cybercrime Department conducted dozens of investigations in cooperation with international partners through direct contacts:

- Child pornography cases: Initial information in several cases was obtained from international partners. In the local case "Skelic" 2.5 million pictures and 7.5 thousands videos were seized.
- Botnet investigations international case ("Bee Hive") took over full control of large Butterfly/Zeus/Yorik/Kraken botnet structure with infected 10 million PCs in 170 countries worldwide. Botnet was uninstalled by Court order of County prosecutor office Banja Luka (Republika Srpska);
- Credit card fraud international case "Cardshop" seized 505 265 credit card fully and took down global, regional and local part of criminal group. Visa International was included in case regarding processing bank info;
- Support to international LEA partners against cybercriminal worldwide: spamming case (arrested Pakistani citizen in London, UK etc.) and conducting worldwide cybercrime takedown operations ("Darkbot");
- Testify as expert witnesses (Slovenia, the USA);
- Reinforcing investigations conducted by police agencies in region.

To increase the cooperation at national level, the project supported the establishment of a subsystem of contact points in all police agencies in Bosnia and Herzegovina with a central Contact Point at the state level that will receive all requests and forward them to responsible police agencies. Thus a 24/7 contact point was established within Directorate for Coordination of BiH Police Bodies.

There are also subsidiary 24/7 contact points within Brčko District, the Federation of BiH and Republika Srpska, as well as within a number of other ministries.

The project advised on institutional set up, responsibilities and authority of 24/7 points of contact in line with article 35 of the Convention on Cybercrime and specific trainings were provided to increase their efficiency. However, the cooperation between different institutions in Bosnia and Herzegovina might remain a challenge to be addressed in the future.

3.5 Law enforcement training

3.5.1 The situation at the outset

State level: The Agency for Training and Advanced Professional Training of Personnel is the competent body for developing and delivering basic and specialised training courses to law enforcement agencies within the Ministry of Security. There was no documented training strategy at the state level covering the areas of cybercrime investigation and digital forensics. New recruits were not taught how to recognise and deal with electronic devices that may contain evidence.

Federation: Within the Federation Ministry of Interior there is the Police Academy located in Sarajevo. The Academy develops and delivers appropriate types of education of police officers. Training courses in computer crime are rare and are mostly organised in cooperation with the support of foreign governments and international organisations. There was no documented cybercrime training strategy within the Federation. During the initial training course for police investigators, the basics of security, identification and collection of evidence are taught, while specialist courses cover the basics of networks and search and seizure of digital evidence. New recruits were not taught how to recognise and deal with electronic evidence during their training; however they are provided with this training during workshop activities.

Republika Srpska: The institution responsible for law enforcement training in general is the Ministry of Interior, Administration for Police Training, through its two organisational units, the Police College (university level police education facility) and the Police Academy, located in Banja Luka. The Policing High School and the Police Academy did not have a documented training strategy for law enforcement officers and staff of the Ministry of Interior who deal with cybercrime

investigations and digital forensics. However, as part of the curriculum of the Policing High School, students of criminal studies were taught the subject of High Tech Crime.

Brčko-District: The Police Academies in Sarajevo and Banja Luka are identified as the principal institutions responsible for law enforcement training. Training on cybercrime in Brčko District was limited in 2010 to the potential for one lecture on computer crime given by professors of the police academy of the criminal science faculty. It was recognised that investigators need to attend cybercrime training courses to an identified standard, providing initial to advanced content.

3.5.2 Assessment and summary of progress made

There are two Police Academies, one in the Federation and another within Republika Srpska. In addition there is a Police College in Republika Srpska. This college delivers a cybercrime module during one semester.

The international community sponsors a number of other training events. A first responder manual was produced but there is a requirement for more training. BiH have requested assistance for specialised trainers from the region to assist with delivery of specialist training.

Training material obtained has been translated into the local language. It was believed that it would be beneficial to make this available to officers working within all 10 Cantons.

The Judicial Training Centres in Bosnia and Herzegovina organized several training sessions for judges and prosecutors in relation to electronic evidence. Based on the need that was identified in these trainings the High Judicial and Prosecutorial Council of Bosnia and Herzegovina decided that it would be useful to prepare a Guide on handling electronic evidence, which would be uniform and used in the entire country. The document has already been finalised and is distributed to prosecution offices and will be distributed as well to police officers who handle electronic evidence. The guide provides the definitions of electronic evidence, definitions of devices and a glossary of terms. In addition the guide provides graphic (photos) description of the devices which may contain electronic evidence. It explains the newest mediums for storing of data such as the cloud. The 2nd part of the Guide deals with the handling of evidence including a basic plan for the search for digital evidence, the investigators should be trained on how to recognize the items that may collect electronic evidence, the proper marking and handling of electronic evidence.

Under CyberCrime@IPA:

- Investigators and other officials were trained on the need to ensure the rule of law and human rights principles (Article 15 of the Convention on cybercrime - Safeguards and conditions)
- One representative from Bosnia and Herzegovina (Cyber Crime Investigator, Department for Combating Organized Crime, Federal Police Administration) was funded to participated in the Master of Sciences (MSc) programme in Forensic Computing and Cybercrime Investigation offered by UCD
- Law enforcement and prosecution services participated in the training on interception of traffic and content data for law enforcement purposes, including legal, procedural and technical considerations and based on good practices
- The project facilitated large representation in the Octopus Conference and the Cybercrime Convention Committee (T-CY) Plenary meetings.

3.6 Judicial training

3.6.1 The situation at the outset

State level: Judicial training is not conducted at the State level in Bosnia and Herzegovina. However State Level judges and prosecutors are trained by the two Centres for Training of Judges and prosecutors in the Federation of BiH and in Republika Srpska.

Federation: Judicial training and professional development of judges and prosecutors is carried out by the Public Institution – Centre for Education of Judges and Prosecutors in the Federation of Bosnia and Herzegovina.

The Centre did not have a cybercrime training strategy for judges and prosecutors; however, it included in its programme, cybercrime courses that are attended by both judges and prosecutors.

The Federation Centre did not provide cybercrime training in its initial training programme. Judges and prosecutors could apply to participate in the cybercrime aspects of the in-service training. The Centre works closely with the Federation Police Administration and the Forensic Institute of the Federation Ministry of Interior in planning and implementation of training activities.

Republika Srpska: The institution responsible for the training of judges and prosecutors is the Public Institution of the Centre for Education of Judges and Prosecutors (CEJP). CEJP included a joint training in Computer Crime for judges and prosecutors in the 2010 Professional Development Programme.

Brčko-District: Such training and professional development of judges and prosecutors is carried out by the Judicial Commission of Brčko District of BiH. It identified the need for some judges and prosecutors to have more advanced training and for joint international events to be held.

3.6.2 Assessment and summary of progress made

There are two educational centres, one in the Federation and the other in the Republika Srpska. Both cooperate with the Judicial Commission and assist with the training requirements of the Brčko District.

There are plans for ad hoc annual training for judges and prosecutors to be delivered in cooperation with the Police Academies and Forensic Centres. Police experts will assist with training. In addition, they also provide training on legislation relating to cybercrime.

In 2011, the Centre for Education of Judges and Prosecutors (CEJP) included a joint training in Cybercrime – High Tech Crime for judges and prosecutors (Professional Development Programme), which deals with collection of digital evidence.

The regional basic training event organised by CyberCrime@IPA in Banja Luka was conducted at the Public Institution Centre for Judicial and Prosecutorial Training of the Republika Srpska. Eleven participants attended the event.

Bosnia and Herzegovina participated in the train the trainer and subsequent in country training offered by the CyberCrime@IPA project. However, BiH took up only one of the two places available on the train the trainer course and the attendee now works for another organisation, leaving BiH with no cybercrime trainers. It is interesting to note that a seminar to be organised in December 2012 was oversubscribed. This should alert the authorities to the need to consider improving the current training offering.

CyberCrime@IPA will make available training materials that will be hopefully integrated into curricula of the training institutions.

3.7 LEA/ISP cooperation

3.7.1 The situation at the outset

State level: In Bosnia and Herzegovina there are 76 ISPs currently registered. The responsible institution for the registration of Internet Service Providers is the Communications Regulatory Agency of BiH[21]. The three leading ISPs are BiH Telecom, HT Eronet and Mobis.

Federation: The main problem identified by the Federation is that in Bosnia and Herzegovina law does not regulate the keeping of logs by ISPs.

The Federation Police Administration did not appoint a permanent contact point nor did the ISPs. However, there was a communication between them and the cooperation was at a satisfactory level. The Federation Police Administration held meetings with the BH Telecom as a major ISP in BiH in order to improve the cooperation. There were no joint training programmes, but the Federation emphasised that representatives of ISPs and law enforcement agencies had participated in training sessions covering computer crime issues, which were implemented by the Council of Europe in Bosnia and Herzegovina through its relevant projects.

Republika Srpska: The lack of an obligation for ISPs to retain data was identified as the main problem encountered in the engagement with ISPs. Data was obtained from ISPs under a court order and on the basis of Memorandum of Understanding, which identifies standard documentation and procedures. The MOU was treated as an official secret. Specific organisational units were nominated as points of contact for cooperation and the heads of units were the responsible individuals. There were no training initiatives for law enforcement and ISPs in this activity.

Brčko-District: The lack of data retention legislation was identified as an obstacle to effective investigation, along with the lack of information on prepaid service subscribers.

3.7.2 Assessment and summary of progress made

There are plans to amend the existing law on electronic communications. The Regulatory Authority appears only to be able to issue licences but control of ISPs appears to be ineffectual and in need of an overhaul. Fines levied against ISPs are small and are not considered a deterrent. In particular, registering SIM Card purchases is largely ignored. SIM Cards are bought and sold in large quantities on the internet and are therefore a readily interchangeable commodity. Getting responses from ISPs in urgent cases can take 6 months or there is no response. This lack of cooperation is hampering prosecutions.

A main obstacle to the criminal justice community has been the lack of legislation requiring data retention by ISPs. This does not prevent and should encourage the type of discussion and development of MOUs. Republika Srpska has MOUs with its ISPs and thus cooperation is considerably better. A decision was made by the Council of Ministers requiring data retention for 12 months. This Decision has the force of law but it has encountered some administrative difficulties.

Bosnia and Herzegovina identified the need to reduce time to get information from ISPs to organise obtaining data for investigations rather than all requests needing court orders.

[21] A detailed list of ISPs is available at: www.rak.ba.

As stated above a number of activities organised under the project, as well as international events in which representatives from Bosnia and Herzegovina participated with the support of the project, were aimed at improving public-private cooperation.

3.8 Financial investigations

3.8.1 The situation at the outset[22]

State level: At the state level, the State Investigation and Protection Agency (SIPA) is the responsible institution for financial investigations, within which the Financial and Intelligence Department is responsible for investigation of money laundering and financing terrorist activities operates.

There is a Task Force of the Institutions of BiH to prevent money laundering and financing terrorist activities, composed of representatives of the Ministry of Security of BiH, the Ministry of Justice of BiH, the Prosecutor's Office of BiH, the Intelligence and Security Agency of BiH, the Central Bank of BiH, the Ministry of Interior of the Federation of BiH and RS, the Indirect Taxation Agency of BiH, the Agency for Security of BiH, the Tax Administrations of FBiH and RS and Brčko District, the Banking Agency of FBiH and RS, the Securities Commission of RS and FBiH. The basis for the operation of this Task Force is to improve the inter-agency approach to the issue of money laundering. When it comes to seizure and confiscation of proceeds from crimes committed with the use of the Internet, they are regulated by the provisions of the BiH Criminal Procedure Code and are carried out in the same way as for other crimes.

Federation: The primary types of fraud and other offences using the Internet, identified by the Federation are criminal offences of computer fraud related to illegal use of credit cards and other non-cash payment cards for purchasing various goods on the Internet; the use of those cards for child pornography, and for on-line betting etc.

The public and private organisations involved in the prevention and detection of criminal money flows on the Internet are the above-mentioned law enforcement agencies, as well as all legal and physical persons provided by the Law on Prevention of Money Laundering and Financing Terrorist Activities of BiH as responsible to notify the Financial Intelligence Department on any suspicious transaction.

Republika Srpska: There were no statistics regarding criminal activity involving illegal money flows on the Internet and the main barrier was the inadequate cooperation with the banks. The Financial Investigation Department with support of the High Tech Crime Department of the Ministry of Interior are responsible for following criminal money flows, as well as search, seizure and confiscation of proceeds from this type of crime. There is a special law in RS, namely the Law on confiscation of illegally gained assets, which entered into force on 1 July 2010.

Brčko-District: The experience of Brčko District on this subject matter consisted of two investigations; one involving a victim report of a fraud relating to a vehicle purchased through the Internet and the other from a victim of an attempted fraud through the "Spanish Lottery".

3.8.2 Assessment and summary of progress made

The Financial Intelligence Unit operates with State-wide competence being part of SIPA and thus under the Ministry of Security. Their primary responsibilities include money laundering. The Unit has 5 analysts who are able to access a limited number of national databases such as Taxation Records, Registry for Identity and others. Specific Land Registry records can be accessed by way

[22] For detailed reports on the functioning of the anti-money laundering systems see the MONEYVAL evaluation and progress reports at: http://www.coe.int/t/dghl/monitoring/moneyval/Countries/BH_en.asp

of written request. Apart from I2 there was no analytical software to assist. Although data sources are searchable there were no tools allowing a consolidated view of data relating to a specific entity nor was any capability to conduct federated searches.

Suspicious financial transaction records are analysed against these data assets in order to identify potentially illegal money flows. Suspicious money movements are referred to the relevant Financial Investigation Unit for prosecutorial consideration of further investigation.

The Financial Intelligence Unit has direct access to central banks system. They are able to request account transaction details for up to 10 years and are empowered to instruct a bank to monitor an account and can freeze an account for up to 5 days. This period may be extended but only with a Court Order and Prosecutors consent.

There have been no incidents of attacks on Internet banking facilities or any incidents of on line money laundering. There were no statistics on assets confiscated. Many financial investigations were performed by Cybercrime Department of the Republika Srpska in cooperation with financial institutions and international partners (LEA and Visa). Cases were related to online fraud: tracking "automated vending carts", stock exchange fraud and market manipulation, using virtual payment and money transfer systems (Liberty Reserve, Webmoney, Bartercheque, Western Union, Moneygram), credit card fraud, criminal cash-out services, criminal re-shipping services and criminal pay per install services. Cybercrime department of Republika Srpska also successfully conducted several investigations related to attacks on Internet banking facilities and bank phishing cases mostly to German, the UK and banks in the USA. Banks have regular meetings with Cybercrime Department of RS. Banking officials have assisted in field operations and they are instructed how to monitor and alert about incidents.

It appears to be a structure and capability to deal with suspicious financial transactions and cooperation between financial institutes and LE in individual entities but not across them. Statistical information is not provided that may enable an assessment of the effectiveness of these arrangements.

3.9 Progress made against previous recommendations

Cybercrime situation report March 2011 – State level	Progress reported
1. The units in Bosnia and Herzegovina will be recommended hereafter to keep statistics of the volume and type of cybercrimes.	Some progress reported High Judicial and Prosecutorial Council maintains a database of the information on applications, investigations, indictments and convictions regarding entity criminal law and criminal law of the Brčko District of Bosnia and Herzegovina, which are defined as offenses related to cybercrimes.
2. It is also recommended to keep statistics about application of the specific powers in the criminal procedural code, including information about application, technical details and cases concerned, as well as taking a coordinating role by the State.	Not completed
3. Review of MLA-procedures with a view to accelerate the handling of requests in cases were digital evidence is concerned. In particular, attention is demanded of the legal concept of seizure of computer data and	Some progress reported

the possible need for expedited execution of investigative powers.	
4. Review criminal procedural law, in particular concerning the collection of traffic data and the interception of electronic communications.	Some progress reported (review under way at state level, as well as in the Republika Srpska)
5. 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.	Some progress reported Training strategies are considered at entity level. In Republika Srpska is underway.
6. 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.	Not completed
7. 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".	Not completed
8. Incorporate good practice in the handling of electronic evidence in criminal investigations; examining existing guides such as those developed by Interpol and Europol.	Some progress reported in the Republika Srpska
9. 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
Recommendations made by second progress report 1 Nov 2011 – 31 May 2012	
Enacting, adapting and harmonising the law in BiH (regarding, confiscation illegally acquired property) formation at all levels Agency for the Management of seized property	Some progress reported Republika Srpska adopted legislation and Federation has a draft law
Networking and access to databases of financial institutions and other relevant institutions in the private and public sector (electronic reporting and accessing)	Some Progress accessing databases
Strengthening of specialist training for prosecutors and investigators	Some progress
Amendments of the law on communications in BiH concerning the obligations of ISP and telecom operators regarding obligation to deliver data	Some progress Ministers Decision on retention
Sign an agreement on cooperation with EUROJUST.	Not completed
Consider the possibility of standardising the forms of requests	No progress report
Establish a web-portal ("Centre of excellence") which would provide an overview of international instruments, legal framework, current trends (newest forms) of cybercrime, information on the judicial and police authorities responsible for the provision of assistance in the investigation of cybercrimes.	Some progress reported Republika Srpska has its portal on this matter
Harmonisation of the legislation with the Budapest Convention on Cybercrime.	Some progress. Review underway
Define and provide continuous training for representatives of judicial and police bodies with the goal of increasing the efficiency of international cooperation.	Some progress

Cybercrime Situation Report March 2011 - Federation	Progress reported
1. Keeping statistics that 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.	Not completed
2. Keeping statistics on application of the specific powers in the criminal procedural code, including with information about application, technical details and cases concerned.	Not completed
3. Review of national criminal law and criminal procedural law in the domain of cybercrime taking into account the observations made in the country report. In particular, attention is demanded of the legal concept of seizure of computer data and the possible need for expedited execution of investigative powers.	Some progress. Legal review under way
4. Consultation with State authorities in view of improving and acceleration the handling of MLA-requests with regard to digital evidence.	Some progress
5. Consideration of the formation of specific police and prosecution units at the Federation level.	Some progress.
6. 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.	Not completed
7. 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.	Not completed
8. Develop a framework for improved cooperation internally in BiH and 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
9. Improve capability to combat illegal money flows on the Internet by all levels working on the adoption of the relevant findings of the Council of Europe study "Criminal money flows on the Internet: methods, trends and multi-stakeholder counteraction".	Not completed
10. Incorporate good practice in the handling of electronic evidence in criminal investigations; examining existing guides such as those developed by Interpol, Europol and Republika Srpska.	Some progress
11. Engage with national and 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
Recommendations Made by Second Progress Report 1/11/11 – 31/5/12	
None	

Cybercrime Situation Report March 2011 - Republika Srpska	**Progress reported**
1. Keeping statistics that 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. Contact with Europol on the matter could be useful.	Not completed
2. Keeping statistics on application of the specific powers in the criminal procedural code, including with information about application, technical details and cases concerned.	Not completed
3. Review of national criminal law and criminal procedural law in the domain of cybercrime taking into account the observations made in the country report. In particular, attention is demanded of the legal concept of seizure of computer data and the possible need for expedited execution of investigative powers.	Some progress Review underway
4. Consider the formation of a prosecution unit to combat cybercrime in accordance with the needs of Republic of Srpska.	Not completed.
5. Consultation with State authorities in view of improving and acceleration the handling of MLA-requests with regard to digital evidence.	Some progress
6. 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.	Some progress Republika Srpska (Ministry of Interior) is preparing a training strategy
7. 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.	Not completed
8. Develop a framework for improved cooperation internally in BiH and 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.	Complete. MOU's signed
9. Improve capability to combat illegal money flows on the Internet by all levels working on the adoption of the relevant findings of the Council of Europe study "Criminal money flows on the Internet: methods, trends and multi-stakeholder counteraction".	Not completed
10. Continue to develop the good practice in the handling of electronic evidence in criminal investigations; ensure compatibility with current international guides such as those developed by Interpol and Europol.	Some progress
11. Engage with national and 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
Recommendations Made by Second Progress Report 1/11/11 – 31/5/12	

None	
Cybercrime situation report March 2011 - Brčko-District	**Progress reported**
1. Keeping statistics that 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. Contact with Europol on the matter could be useful.	Not completed
2. Keeping statistics on application of the specific powers in the criminal procedural code, including with information about application, technical details and cases concerned.	Not completed
3. Review of national criminal law and criminal procedural law in the domain of cybercrime taking into account the observations made in the country report. In particular, attention is demanded of the legal concept of seizure of computer data and the possible need for expedited execution of investigative powers.	Some Progress Review underway
4. Consultation with State authorities in view of improving and acceleration the handling of MLA-requests with regard to digital evidence.	Some progress
5. Consider the formation of specific police and prosecution units within Brčko district.	There are 9 prosecutors in total so may not be practical.
6. Engage in the development of a cybercrime training strategy with those responsible for delivering training on behalf of Brčko District, 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.	Some Progress
7. Develop a framework for improved cooperation internally in BiH and 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
8. Improve capability to combat illegal money flows on the Internet by all levels working on the adoption of the relevant findings of the Council of Europe study "Criminal money flows on the Internet: methods, trends and multi-stakeholder counteraction".	Not complete
9. Incorporate good practice in the handling of electronic evidence in criminal investigations; examining existing guides such as those developed by Interpol, Europol and Republika Srpska.	Some progress
10. Engage with national and 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

3.10 New recommendations

1. Review the legal framework at state, entities and district levels to full implement international standards (see also the section on legislation)
2. Consider revision to Procedural Codes to allow the service of digital evidence in place of printed documents
3. Consider development/adoption of the national Strategy for combating cybercrime
4. Analyse existing competencies and overlapping competencies to establish protocols and operational policies in order to clarify roles and responsibilities.
5. Analyse legal best practices regarding confiscation of assets (on-going within IPA 2010 National Project on support to law enforcement in BiH)
6. Identify suitable computer forensic service capability
7. Federation to consider establishing a cybercrime unit
8. Improve collaboration between specialist assets offering common services.
9. Encourage establishment and use of 24/7 capability within Republika Srpska
10. Participate in more regional training and in train the trainers
11. Promote wider use of existing Manuals
12. Continue to develop law enforcement training strategy
13. Continue to develop judicial training strategy
14. Raising awareness within the judiciary
15. Amending Criminal Code to shift the burden of proof where criminal assets are suspected. There is a law on confiscation of assets deriving from crime only in Republika Srpska, which provides the burden of proof also on suspect
16. Refining the tactical coordination procedures between intelligence, investigations and prosecutors office
17. Continue to develop MOUs based on existing Guidelines on LEA-ISP Cooperation

4 Croatia

4.1 Cybercrime and the criminal justice system

4.1.1 The situation at the outset

Computer fraud was the most frequently occurring cybercrime. Other frequently occurring criminal activities were credit card fraud, prevention of credit card validations by blocking computer systems, deletion of historical credit data of banking organisations and other related crimes.

Further, a strong increase was noticed in phishing cases and identity theft, in particular in relation with social networks. The same was the case with hacking and (attempted) fraud by means of spam.

4.1.2 Assessment and summary of progress made

Of all economic crimes, computer fraud is the highest ranking crime. The State Attorney's Office has monthly and annual oversight of detailed statistics and this information is subject to regular performance review. The Office also monitors and reports on the number and type of "Special Enquiry Measures".

2011 Cybercrime Statistics:

- 137 computer related fraud
- 50 child pornography
- 6 Infringement of Secrecy, integrity and accessibility
- 7 Computer Forgery
- 20 Copyright infringements

- 200 cybercrime cases in total
- 140 indictments
- 122 convictions
- 35 sentenced to imprisonment

Statistics for 2012 will only become available in 2013.

In total, the country has 420 prosecutors dealing with criminal matters associated with economic crimes, including cybercrime, as well as those involved with child protection and child pornography.

There are no prosecutors dealing exclusively with cybercrime. However, 27 prosecutors deal with corruption and organised crime, including cybercrime.

4.2 Legislation

4.2.1 The situation at the outset

Croatia ratified the Budapest Convention on 17 October 2002 and its Additional Protocol on Xenophobia and Racism on 4 July 2008. During the implementation of the project, on 21 September 2011, Croatia also ratified the Convention on the Protection of Children against Sexual Exploitation and Sexual Abuse.

In preparation of the ratification of the Budapest Convention Croatia amended its Criminal Code in 2004 by introducing a number of new or modified criminal offences concerning child pornography,

infringement of confidentiality, integrity and availability of computer system, computer data and computer programs, computer forgery and computer fraud.

A reformed Criminal Procedural Act (1997) had entered into force on 1 July 2009 and only applied in cases of investigated and prosecuted by the Office concerning the Suppression of Corruption and Organised Crime (USKOK).

4.2.2 Assessment and summary of progress made

In June 2011, Croatia formally closed its negotiations with the European Union, and the accession treaty was signed on 9th December 2011. Following the positive referendum in Croatia in January 2012 and the ratification process in EU member states, Croatia is to become the 28th member of the EU by 1 July 2013. As noted in the last European Commission progress report, Croatia is showing significant improvements in the promotion and protection of human rights.

Starting from 1 September 2011 further reforms replaced the Criminal Procedural Act 1997. At the same time, a basic reform of the Criminal Code was undertaken to respond to obligations and standards arose from international instruments (such as UN, EU acquis, Council of Europe conventions, case law of ECHR, recommendations of GRECO and MONEYVAL, OLAF guidelines and reports of the European Committee for the Prevention of Torture (CPT).

The new Criminal Code entered into force in January 2013. Cybercrime offences are included in a distinct Chapter and this will give more legal clarity to these crimes. The legislation of Croatia is harmonised with both the Budapest and Lanzarote Conventions.

Croatian law is also harmonized with the EU acquis as regards rules regulating the collection and processing of data in the field of electronic communications. In that respect, it should be noted that provisions of Directive 2002/58/EC concerning the processing of personal data and the protection of privacy in the electronic communications sector[23] and Directive 2006/24/EC on the retention of data generated or processed in connection with the provision of publicly available electronic communications services or of public communications network[24] are implemented through the Electronic Communications Act.[25]

The law on data retention now requires ISPs to keep data for 12 months. Should an application be made from abroad an Order can be made requiring an extension for a further 12 months. Legislation is also in force that attaches corporate liability to ISP operators. Companies can have assets liquidated and individual officers may be fined for breaches of operating regulations. In addition, Safety Measures may also be imposed preventing convicted persons from accessing the internet and ISPs permitting access by such persons.

From 1 July 2013 new laws will take effect regarding judicial cooperation with EU member states and others.

A Manual of Guidance has been drafted for prosecutors. It describes new criminal acts together with advice on how to collect, preserve and present such evidence in judicial proceedings. There is also a corresponding Manual of Guidance for police, which gives advice on search and seizure. Both manuals will have been printed and circulated by the end of 2012.

---

[23] Directive 2002/58/EC of the European Parliament and of the Council concerning the processing of personal data and the protection of privacy in the electronic communications sector, OJ L 201, 31.7.2002.

[24] Directive 2006/24/EC of the European Parliament and of the Council of 15 March 2006 on the retention of data generated or processed in connection with the provision of publicly available electronic communications services or of public communications network, OJ L 105, 13.4.2006.

[25] Electronic Communications Act, Official Gazette No. 73/08, 90/11

There is a written protocol between the Prosecutors Office and the Ministry of Interior (police) defining "rules of engagement", lines of communication and operational limitations.

It should be stressed that Croatia enacted rules on the handling of digital evidentiary material with a special consideration for conditions and safeguards in connection with the procedural powers defined by the Budapest Convention. During the implementation of the project, the example of Croatia was included in the study on the implementation of Article 15 (Conditions and Safeguards) under the Budapest Convention on Cybercrime and experts from Croatia have been used in activities related to these issues.

The provisions on the protection of children against sexual violence transposed closely the Convention on Cybercrime and Lanzarote Convention and could be used by other States for inspiration in drafting or amending their national legislation.

4.2.3 Recommendation

Although the Assessment report on the implementation of the preservation provisions of the Budapest Convention on Cybercrime, prepared by the T-CY Bureau stated that Croatia is in line with the Budapest Convention, future amendments could consider the recommendations made by the report to adopt specific legal provisions, and promote the use of the provision in practice. Thus in the future amendments the authorities in Croatia may:

- Consider the recommendations made in the report of the Cybercrime Convention Committee (T-CY) assessing the implementation of the preservation provisions of the Budapest Convention on Cybercrime, adopted by the T-CY in December 2012 to adopt specific legal provisions, and promote the use of the provision in practice.

4.3 Specialised institutions

4.3.1 The situation at the outset

There was no specific high tech crime unit within the police or State Attorneys offices within Croatia; however within the Ministry of Interior, high tech crime is dealt with at both state and local levels. At the state level the issue falls within the competence of law enforcement officers of the National Police Office for Suppression of Corruption and Organised Crime, which consists of the Department for Economic Crime and Corruption and the Department for Organized Crime. Specific high tech crime related issues are within the competence of the Sector of General Crime, Terrorism and War Crimes.

At local police administration levels, high tech crime fell within the competence of law enforcement officers of the Department/Section/Unit for Economic, General and Organized Crime and Department for Terrorism.

Within the State Attorney's Office the high tech crimes are processed within the normal category of criminal offences. Annual assignment of duties provides for particular deputy attorneys to be placed in charge of such cases. These attorneys have received additional training.

4.3.2 Assessment and summary of progress made

A High-tech Crime Department was established through the Regulation on the internal organisation of the Ministry of the Interior, which was passed by the Government on 20 June 2012. The Department is located within the Service for Economic Crime and Corruption, which is a part of National Police Office for Suppression of Corruption and Organized Crime.

The High-tech Crime Department systematically analyses, monitors and studies the phenomenological and etiological aspects of cybercrime (computer crime), and proposes solutions in terms of raising the level of efficiency in combating cybercrime; directly implements complex criminal investigations in the field of criminal acts committed against and using computer systems and networks, performs forensic analysis and monitoring of the Internet is providing specialized support to other organizational units of the police, cooperates with other organizational units of the Ministry, Government bodies and legal persons, the police of other countries and international institutions in their jurisdiction, participates in the planning and development of training programs of police officers on cybercrime issues, participates in the preparation of normative documents, reports and expert opinions in the field of cybercrime and performs other activities from its scope.

It has 5 police officers, including the Head of Department. Within each of the 20 Police Districts there are between 1 and 4 officers responsible for economic crime including cybercrimes. This makes a further 35 officers who are capable of conducting basic cybercrime seizures and examinations. The Forensic Science Centre, which is part of the Ministry of Interior, carries out more complex analysis of digital evidence.

There are an additional 8 officers distributed amongst regional centres who are capable of more complicated examination procedures than can be carried out by local officers. These regional centres were seen as a more cost effective alternative to reproducing the Central Cybercrime Unit in 20 police districts. The regional offices will be able to conduct some basic forensic analysis.

4.4 International cooperation

4.4.1 The situation at the outset

Domestic judicial authorities responsible for mutual legal assistance requests are courts and state attorney's offices authorised by a special law to afford mutual legal assistance.

Responses for requests regarding stored computer data may be prioritised and processed on an expedited basis. The Ministry of Interior has on several occasions requested information from large corporations based in the USA, through Interpol in Washington. Responses have been received that such requests require use of mutual legal assistance means. There have been some cases where communication with 24/7 points of contact has been made in order to preserve evidence. These have been followed by mutual legal assistance requests for the release of the information. All police to police cooperation in this respect is conducted through the official channels of Europol, Interpol and the 24/7 network.

The main obstacles encountered by Croatia in international cooperation matters is the refusal of some countries to provide information, such as the identity of web site administrators or the identity of the owners of free email accounts without the submission of official requests for mutual legal assistance.

The United Kingdom was unresponsive as they operate a £5K threshold rule, as well as Italy. Facebook, Google and Yahoo were found to be unhelpful except cases involving child abuse or terrorism.

4.4.2 Assessment and summary of progress made

Regional cooperation and "turnaround" times were on average taking about 3 months. This was attributed to the success of CyberCrime@IPA in establishing effective regional networks. Cooperation with the USA usually involved a 10 to 12 month "turnaround" time period.

The improvement generated by the project was clearly at the IPA regional level, where new networks facilitated communications.

The project organised specific events on international cooperation to discuss issues raised e.g. cooperation with USA, UK and private companies and invited senior officials from UK and USA who provided valuable advice for the project areas.

As advised by the project, Croatia made use of EUROJUST in some successful investigations.

4.5 Law enforcement training

4.5.1 The situation at the outset

Law enforcement training is carried out by a number of organisations under the umbrella of the Police Academy in Zagreb, established within the Ministry of the Interior as an Educational Centre (a specialised institution organising the basic and professional education of apprentice police officers, students, police officers and trainees).

The High Police School is in charge of students' education, i.e. education of the future specialists in criminal investigations and specialists in criminal investigations with a bachelor's degree. The High Police School is formally an institution of higher education for science and education, established as organisational unit of the Police Academy.

The High Police School carries out education of specialists at two levels:

- 3 years Professional Study of Criminalistics, 180 ECTS credits and the
- 2 years Professional Undergraduate Study of Criminal Investigation, 120 ECTS credits.

The Department for Professional Training and Specialisation is an organisational unit of the Police Academy. The duties of the Department for Professional Training and Specialisation are planning, programming, organisation and pedagogic supervision of all aspects of specialist training, professional training and education within the Ministry of the Interior, as well as particular aspects of training for external clients (customs services, personal protection, military police, criminal justice police, humanitarian clearance of mines, traffic police etc.).

The Department, within its annual training plan, has 3 subject related events:

- Network Forensics workshop
- Computer search course
- Software falsification course.

The Department for Law Enforcement Training is an organisational unit of the Police Academy within the General Police Directorate and the only institution for basic law enforcement education in the Republic of Croatia.

There was no documented training strategy for law enforcement officials in Croatia in the area of cybercrime investigation and digital forensics. However, there were significant aspects of the Police High School education programme that dealt with the subject matters.

There was no training centre identified that provides specific training in the subject areas, nor details of any related academic or professional qualifications, nor any cybercrime or digital forensics training courses identified outside the elements of the courses detailed. New recruits were not receiving any training in the subject areas.

The Croatian Academic Research Network (CARNET) is the national research and education network. It is funded by the Government and operates from offices in all the major cities. Its purpose is to promote educational programs and to encourage enterprise through innovative technology for the benefit of society.

4.5.2 Assessment and summary of progress made

Since the initial situation report was drafted there have been a number of developments in the field of cybercrime education.

Within the Police Academy, 1st Responder Training materials have been produced which will be delivered to all recruits commencing in 2013. Students will now be accredited as competent by cybercrime investigations and or computer forensic examinations.

Also a new curriculum has been drafted and is undergoing final review. This training will include modules on:

- Information security
- Terrorist prevention and cybercrime
- Digital evidence and cybercrime
- Investigating cybercrime
- Investigating computer crime

Approval from the relevant Minister will be required before this programme can be delivered. Graduates will receive diplomas, which will be recognised and registered. The Ministry of Science Education and Support will evaluate the curriculum.

The Department for Professional Training and Specialisation is willing to deliver some specific courses and will outsource the trainers mostly from CARNET. The equipment needed to provide this training has been ordered and delivery is expected during the first week of December 2012. Thus they will also be able to provide "in service" training.

The Economic Crime and Corruption Units produce their own specialist training for their own units based on expertise developed operationally. Similarly, the Specialist Investigation Unit conducts its own specific "in house" training.

Both Undergraduate and Postgraduate Law Enforcement Training in Croatia include cybercrime modules. The level of training delivered is as follows:

- High school level (Basic)
- Academy level (More Advanced)
- Professional level (Advanced).

Croatia's Law Enforcement Training Department is not able to deliver advanced training by themselves and so are looking to outsource delivery to academic institutions. Expertise from different Universities will be used for various segments.

Current training institutions lack both the hardware and software required to conduct advanced training and so assistance is being sought from industry, academia and other relevant institutions. The requirement for advanced training is believed to be in the order of about 10 persons per year. As this training is expensive there are plans to implement organisational controls to minimise inappropriate or wasted training delivery.

In addition to structured, targeted training, a number of seminars and ad hoc courses are organised in collaboration with the Croatian Academic Research Network (CARNET), the Ministry of the Interior and Ministry of Science.

Courses for officers dealing with cybercrime matters are run as and when necessary. There is normally one course per year but this can be varied according to demand.

Considerable progress has been made with the introduction of 1st responder training to all new recruits from 2013 being a welcome development. There is considerable other training taking place and it is important that this is coordinated at a central level to ensure consistency. While there is reference to the absence of digital forensics training in the structure, it is known that training is delivered in this field by private sector. The building of relationships with academia and industry is also a good sign of progress and should be continued.

The Workshop on interception of traffic and content data for law enforcement was organised under CyberCrime@IPA in cooperation with the Police Academy in Zagreb.

One law enforcement representative from Croatia (National Police Office for Suppression of Corruption and Organized Crime – Department Zagreb) was funded by CyberCrime@IPA to participate in the Master of Sciences (MSc) programme in Forensic Computing and Cybercrime Investigation offered by University College Dublin (UCD).

In addition, similar to other project areas law enforcement and prosecution services from Croatia participated in several trainings, study visits and other activities.

4.6 Judicial training

4.6.1 The situation at the outset

The central institution for training of judges and prosecutors is the Judicial Academy, an independent public institution. The Judicial Academy is responsible for both initial and in-service training of judges and prosecutors, advisors and trainees in courts and prosecutor's offices.

There was no training strategy in the subject areas identified for judges and prosecutors; however, an element of cybercrime training was delivered as part of the programme entitled "Fight against organised crime, developed under the CARDS 2003 programme and training "Anti-corruption measures", sponsored by TAIEX. These trainings were delivered to a total of 112 prosecutors and 57 judges from across Croatia in 2007 and 2009.

Cybercrime and digital evidence did not appear on the curriculum of training for judges and prosecutors at either the initial or in-service training levels. It was recognised that the training on these subject areas were not sufficiently organised and consistent due to the small number of workshops that have been held.

The following were seen as actions that may be undertaken in Croatia depending on the availability of funding:

- The Judicial Academy should develop standard training and modules that will be easily repeated towards larger number of participants and that will enable them to advance from basic to advanced level of training. This should include incorporating the experience of Croatian cybercrime experts
- Training of trainers would be also very important, first of all by national experts but also in special cases and for special reasons also by foreign, international experts.
- Teaching materials should be developed in accordance with international standards and be available to a larger number of potential participants
- Methods such as on-line training should be explored.
- Judicial officials should network and connect with each other but also with others involved in criminal justice system. They should also participate in various international associations dealing with cybercrime and digital evidence.

4.6.2 Assessment and summary of progress made

Under the project it was agreed that the Regional Pilot Centre for judicial training will be hosted by the Judicial Academy of Croatia. The aim is to provide a centre for disseminating training material and share experience in the region, delivery trainings for judges and prosecutors throughout the region etc.

On 30 April 2013, at the CyberCrime@IPA Closing Conference, the judicial training institutions of all project areas signed a Memorandum of Understanding aimed at enabling future cooperation under the Regional Centre.

Four training events organised by CyberCrime@IPA have been organised in cooperation with the Judicial Academy:

- Regional training of trainers course (15 trainers)
- Regional training on the finalisation of the basic training material on cybercrime and electronic evidence
- Country specific basic training for judges and prosecutors
- Advanced cybercrime training for Croatian and Bosnian judges and prosecutors

These activities have trained 25 prosecutors, 15 judges and 3 participants from other target groups. Post-delivery evaluation by candidates rated this training as "excellent". Two trainers from Croatia (the Deputy of State Municipal Attorney and a judge at Municipal Court of Velika Gorica) participated in the train the trainer course.

Apart from the training delivered under CyberCrime@IPA and training sponsored by TAIEX, the Academy has not delivered any domestic cybercrime training.

Judges and prosecutors have been canvassed as part of a 2013 training needs analysis. When completed, a training programme will be produced detailing training courses to be delivered throughout 2013.

In addition to the benefits above-mentioned, the regional approach has produced a number of ancillary benefits:

- As judges and prosecutors are not getting frequent exposure to the entire spectrum of offences, the regional approach facilitates a rapid exchange of experience and knowledge
- Know how and what works are disseminated amongst professionals
- The identification of emerging trends and common criminal networks
- The Judicial Academy is able to harvest this collective experience and so establish a corpus of knowledge which they can draw upon when delivering future training events.

There are approximately 30 judicial officials currently in training on the prevention of cybercrime.

There are plans to deliver cybercrime training as part of "in service training" but this would be selective as in service training is not obligatory. Cybercrime training will be included in the Annual Training Catalogue. There is a database that when searched by name indicates what training courses an individual attended.

Distance or computer based learning packages are also being considered as a potential method to deliver some material. There is an intention to deliver "blended learning" using a variety of methods including seminars and workshops.

Judicial Academy of Croatia had plans to deliver cybercrime training within its programme in 2013, cybercrime training was included in the proposal to the Programme Council, but the Council's opinion was that this was not one of the training priorities to be financed from the national budget for year 2013. It is expected that their role as the regional centre will see them take the lead in ensuring that the training benefits accrued from the project are carried forward in a structured manner. The MoU concluded between the judicial training institutions of the region (see above) should facilitate this.

4.7 LEA/ISP cooperation

4.7.1 The situation at the outset

Cooperation with Internet and telephone services providers is, as a rule, conducted by the Operative – Technical Centre and exceptionally, if required, in direct contact. For this reason an overview of Internet services providers and any problems encountered in dealing with them was not provided.

The procedures to be followed for access to ISP information is provided when organisational units refer to the Operative – Technical Centre by submitting a written request for data such as the data on the allocated IP address, or data from telephone services providers, such as the identification data on the user of a particular number of a fix or mobile telephone connection, account turnover etc. In the case of a need to obtain the contents of a communication between telephone users, a warrant of the competent court is required. Internet services providers are obliged to retain data during a period of one year.

In the Ministry of the Interior there was no person nominated as a contact point with the Operative-Technical Centre; however contact is made by each organisational unit according to their requirements.

HAKOM is the communications regulatory body responsible for monitoring and licensing of all ISPs and Communication Service Providers (CPSs) in Croatia.

4.7.2 Assessment and summary of progress made

Croatia has an Operational Technology Centre for Telecommunications Surveillance (OTC) which is the institution that acts as the intermediary between LEA and ISPs. The procedure for sending requests to ISPs in Croatia is centralized. All requests are collected in a structured written form by the OTC, which sends them to the ISP. The answers come from the ISP to the OTC and then to the requester.

Internet services providers are obliged to retain data during a period of one year. Within the Ministry of the Interior the Head of Special Criminal Investigation Department is a contact point with the Operative-Technical Centre (OTC). As result each organisational unit send their requirements to the Special Criminal Investigations Department and then the requests are sent to the OTC. The Operational Technical Centre conducts special investigative procedures. This Unit maintains a close working relationship with all ISPs. No problems were reported during the assessment.

LEA and ISP cooperation was reported to be good with the majority responding to requests in less than four weeks. There are no MOUs concluded.

4.8 Financial investigations[26]

4.8.1 The situation at the outset

During 2009 and 2010 the main types of fraud encountered on the Internet were fraud committed by inviting citizens to invest financial resources in various funds on the FOREX market; with false promises of acquiring multiple profits deriving from such investments within short periods. The control of financial transactions falls primarily within the competence of the Financial Inspectorate, Tax Administration and the Anti-Money Laundering Office.

According to Article 81 of AMLTF Law, all reporting entities as defined in Article 4(2) of AMLTF Law are required to keep following records: 1. records on customers, business relationships and transactions referred to in Article 9 of AMLTF Law; 2. records on the supplied data referred to in Articles 40 and 42 of AMLTF Law. Furthermore, on 1 January 2009, Rulebook on the content and type of information on payers accompanying wire transfers, on duties of payment service providers and exceptions from the wire transfer data collection obligation (O.G. 01/09) entered into force. Banks also keep records on all transactions on the basis of Payment System Act. Therefore, it is believed that the Croatian authorities can control financial transactions conducted via Internet.

In Croatia financial investigations are carried out by the National Police Office for Suppression of Corruption and Organized Crime in coordination with the State Attorney's Office; however a warrant for financial investigation in the case of a suspected criminal offence, may be issued by the State Attorney's Office to the various departments within the Ministry of Finance; namely to the Financial Inspectorate, Tax Administration, Customs Administration, Financial Police and Anti-Money Laundering Office[27]. Each of them within their competence, have the capacity and the right to control the money flow of a particular natural or legal person, their revenues and expenditures, owned assets (real estate, securities, movable property etc.); the reports on results are submitted to the State Attorney's Office and the police. The above parties cooperate in all cases relating to the subject matter.

Other institutions considered to be involved in the prevention and control of criminal money flows include the Central Depository & Clearing Company, which is a public company maintaining records of security owners, and the Croatian Agency for Supervision of Financial Services (HANFA), which is the supervisory body for security transactions.

Public-private cooperation in this area is very much through official means; persons subject to the Money Laundering and Terrorist Financing Prevention Act (natural and legal persons defined in Article 4(2) of AMLTF Law which are banks and other reporting entities) are required to cooperate with the Anti-Money Laundering Office, by submission of a notification on suspicious transactions. Banks shall, at the courts direction submit the confidential bank's data in line with the Credit Institutions Act.

As a strategic document with a purpose of further coordination and enhancement of inter-agency cooperation in AML/CFT, on 1st March 2007, the Protocol on cooperation and establishment of the Inter-institutional Working Group on AML/CFT was signed at ministerial level. Inter-institutional Working Group on AML/CFT (IIWG) includes 11 government institutions and agencies, as follows: Anti-Money Laundering Office (AMLO, Croatian FIU), State Attorney's Office of the Republic of Croatia, the Ministry of the Interior – the Police Directorate, the supervisory services of the Ministry of Finance (the Financial Inspectorate, the Customs Administration, Tax Administration), the Croatian Financial Services Supervision Agency, the Croatian National Bank, the Security-

[26] For detailed reports on the functioning of the anti-money laundering systems see the MONEYVAL evaluation and progress reports at: http://www.coe.int/t/dghl/monitoring/moneyval/Countries/Croatia_en.asp

[27] In the meantime the office was abolished and the role was assumed by the Tax Administration Office.

Intelligence Agency, Ministry of Foreign and European Affairs and the Ministry of Justice. Representative of AMLO is elected president of IIWG.

The goals and tasks of IIWG are cooperation and coordination of all 11 institutions involved in achieving strategic and operational objectives in the fight against money laundering and terrorist financing, identifying (and elimination of) weaknesses and risks in the process of combating money laundering and terrorist financing, and identifying obstacles that hinder the achievement of these strategic and operational goals.

4.8.2 Assessment and summary of progress made

There is a Financial Intelligence Unit for Money Laundering within the Ministry of Finance. It is an administrative unit and a member of the Egmont Group of financial intelligence units (a worldwide Financial Intelligence network).

This unit deals with all aspects of money laundering including cybercrime. A suspicion on money laundering or terrorist financing is necessary before any analytical or intelligence activities can be carried out. There are three ways in which such investigations can be initiated:

- As a result of a suspicious transaction notification by one of the financial institutions
- State authority notification i.e. sale of drugs or proceeds; "dirty" money
- Request from a foreign FIU.

Since 2009 there have been 40 verdicts for Money Laundering. A new law has recently been introduced relating to money laundering and terrorism financing.

The FIU has direct or indirect access to a range of databases and is able to use I2 to assist with their analysis. An order to temporarily suspend execution of suspicious transaction for 72 hours can be issued. However, a Prosecutor has to be notified as soon as practicable as a court order is required to extend this period further.

Money remittance services are reporting entities according to the Article 4(2) of AMLTF. Croatian banks and other reporting entities are using lists of indicators (red flags) for detecting suspicious transactions which could also be related to cybercrime.

IIWG has demonstrated ability to operate at the strategic level, working through the regular semi-annual meetings and at the operational level in daily contact of authorities in solving a particular problem. It should be noted that by establishing of the working group a list with 44 person responsible for communication was established, each institution within in the protocol was required to determine the representative in the working group, deputy representative, contact person (liaison officer) and Vice contact person. IIWG from 2007 to 2011 held ten regular and three extraordinary meetings.

In the course of meetings, participants exchange information on all relevant activities in AML/CFT field (including results of members' participation in other meetings, projects, activities in relation to NPO sector etc.) and are informed on results of AML/CFT system in previous period with emphasis on judicial statistics in order to discuss and review effectiveness of the system. At the meeting of IIWG held on 12 May 2011 the Supervisory IIWG subgroup was established. Supervisory IIWG subgroup meets with the aim of strengthening coordination and exchange of experiences and best practices of the bodies responsible for overseeing the implementation of measures and actions to prevent money laundering and terrorist financing. At the meeting held on 8 September 2011 Operational IIWG subgroup was established that meets with the purpose of work on specific cases and coordination procedures and providing mutual feedback in specific cases related to money laundering or the financing of terrorism.

In Croatia, all criminal offences can be predicate crimes for money laundering, including cybercrime ("all crimes approach").

From January 2012 Croatia participated in the project of developing a preliminary national risk assessment with the IMF. This project involves all the bodies of the Croatian AML/TF system (AMLO – Croatian FIU, Police, State Attorney's Office, Croatian National Bank, Financial Inspectorate, Tax Administration, Customs Administration, Croatian Financial Services Supervisory Authority, Ministry of Justice etc.) which have so far responded to the 8 questionnaires and surveys and additional information requested by the IMF. This project ended in January 2013. After finalization of Preliminary national risk assessment, Croatian authorities will start with the process of complete NRA, which will have a section on ML/TF connected with cybercrime.

4.9 Progress made against previous recommendations

Cybercrime situation report March 2011	Progress reported
1. Keeping statistics that provide an insight in the seriousness of cybercrime in the national territory. Such statistics could for example 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
2. Providing for statistics on the application of the specific powers in the criminal procedural code, including with information about application, technical details and cases concerned.	Partially Completed
3. Consideration of the observations made in the report above on criminal law and criminal procedural law in view of amendment where appropriate. Specific attention is demanded with regard the legal concept of seizure of computer data and the possible need for expedited execution of investigative powers, in particular in view of the new criminal procedural code.	Completed
4. Consider the formation of specific police and prosecution units to provide dedicated response to combat cybercrime in accordance with the needs of the country. Consider whether the existing arrangements whereby the police responsibility is given to departments with other responsibilities is sufficient to meet new challenges.	Completed
5. 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. Build upon the existing programmes offered by the Police Academy.	Work in Progress This is well advanced and should be concluded during 2013
6. 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
7. 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 Capability development is underway
8. Incorporate good practice in the handling of electronic evidence in criminal investigations; examining existing guides such as those developed by Interpol and Europol.	Completed Good practice guides produced, circulation imminent.

9. 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	Progress reported
Recommendations made by second progress report 1/11/11 – 31/5/12	
Each Party to the Budapest Convention to publish guidelines regarding mutual legal assistance providing information about competent authorities, form of the request etc. in order to minimize the time needed by the receiving state to respond.	No progress reported
Each Party to the Budapest Convention to publish the relevant legislation on cybercrime on the website. Under the CyberCrime@IPA to collect the above mentioned information and publish it on the website of the Council of Europe	Completed
Establish specialised units for combating cybercrimes within relevant institutions	Completed
Organise regular meetings of the representatives from relevant institutions and reporting entities (the Croatian Chamber of Economics, the Croatian Bank association) injured parties (holders of intellectual property rights etc.)	Completed
Provide training for the judiciary and police officers on the use and admissibility of electronic evidence in court.	Complete
Ease the procedure for reporting cybercrime and provide analysis of reported incidents	No progress reported

4.10 New recommendations

1. Review their existing law in the light of recommendations made in previous reports, including the Cybercrime Convention Committee (T-CY) to ensure complete harmonization.

2. Establish a cadre of specialist prosecutors able to provide assistance guidance at national level.

3. Accelerate the delivery of domestic judicial training events using experts available within the country.

4. Continue to develop the domestic judicial training strategy.

5 Montenegro

5.1 Cybercrime and the criminal justice system

5.1.1 The situation at the outset

A wide variety of cases was reported from copyright violations to credit card and banking card frauds, computer fraud, damaging computer data, illegal access to computer systems and networks, including unauthorized use. In addition, it was pointed at threats and insults by means of e-mail, also in relation with Facebook.

In the past 10 years, a number of surveys have revealed the changing profile of Internet usage in Montenegro:

- In 2005 less than 20% of households had internet access
- Of that 20%, 80% were aged 18 or under and use was mainly related to Internet gaming
- By 2009 the number of households with Internet access had risen to almost 50% and has continued to rise rapidly.

There was indication that use will soon match other European levels and may rise as high as 90%. Computer usage has now extended beyond leisure and gaming and into social networking and purchasing. PayPal and e-banking had been introduced and the country is experiencing a growth in cybercrime.

5.1.2 Assessment and summary of progress made

Montenegro has experienced relatively low levels of cybercrime. The vast majority of their problems are connected with credit card fraud, which tends to be seasonal and associated with peaks in tourism.

They have also experienced some instances of:

- Internet fraud
- Web Site Hacking
- DDOS attacks
- Copyright Infringements.

In the past 4 years there have been 160 charges brought against 110 offenders for these types of offences. Previous statistics used different parameters and so are not directly comparable.

The Government has commissioned a study on the state of the country's cyber security, which will report on threats, vulnerabilities, and the distribution of competencies within its institutions. The process involves the Ministries of Defence, Interior, Justice, Information Society as well as the National Security Agency and the Police. The report will be used to inform the National Cybercrime Strategy and provide focus for the Cybercrime Emergency Response Team (CERT).

The CERT is situated within the Ministry of Information Society. It is comprised of 4 well-trained experts who will be able to provide substantial support to the existing cyber forensic capability. CERT has already provided forensic examinations in several police cases as it is recognised that the existing forensic capacity and capability was insufficient.

5.2 Legislation

5.2.1 The situation at the outset

The State Union of Serbia and Montenegro ratified the Budapest Convention and its Additional Protocol on Xenophobia and Racism on 3 March 2010. Montenegro also ratified the Convention on the Protection of Children against Sexual Exploitation and Sexual Abuse on 25 November 2010.

Most of the substantive law provisions of these instruments were implemented, and some of the procedural law provisions follow the standards of the Convention. The regulation in Articles 157-162 is an excellent example of what should be taken into account when implementing Article 20 (Real-time collection of traffic data). However, the Situation Report and other activities organised under the project identified some gaps.

5.2.2 Assessment and summary of progress made

The Situation Report makes several recommendations for improvement, including of the current provisions of the Criminal Procedure Code in the part dealing with interception of electronic communications, technical operations and technical requirements for operators, as well as legal provisions governing seizure and expedited preservation of computer data.

Montenegro does not have a specific provision on partial disclosure but search and seizure (Article 75 Criminal Procedure Code) and the provisional/temporary seizure (Article 85 Criminal Procedure Code, which includes electronic data) may be used as in the case for preservation requests. Judicial orders are required and they would need to specify what additional information is to be provided on other service providers and the path of a communication. However, these possibilities have not yet been tested in practice as traffic data is also retained under data retention obligations.

In 2010, a new Criminal Code (Official Gazette of Montenegro 25/2010) was adopted, which implements the provisions of Article 9 of the Budapest Convention except for a definition of the term "child pornography".

Legal advice was provided under project on several occasions and the Ministry of Justice set up a working group with the task to review the legislation in order to fully comply with the Budapest Convention. A specific legal opinion was provided on the Law on International Legal Assistance in Criminal Matters of Montenegro.

5.2.3 Recommendations

Although the legislation in Montenegro is largely compliant with the standards of the Budapest Convention amendments could be considered to fill the gaps identified under different activities. Thus the authorities in Montenegro might want to consider:

- The recommendations made in the Assessment report on the implementation of the preservation provisions of the Budapest Convention on Cybercrime, adopted by the Cybercrime Convention Committee (T-CY) to adopt specific legal provisions, and promote the use of the provision in practice.
- Closing the gaps identified in the Discussion paper "Protecting children against sexual violence: The criminal law benchmarks of the Budapest and Lanzarote Conventions".
- The recommendations made during the project on improving cybercrime legislation, as well as the Legal Review of the Law on International Legal Assistance in Criminal Matters of Montenegro.

5.3 Specialised institutions

5.3.1 The situation at the outset

A special unit for the investigation of cybercrime offences, including the protection of intellectual property, was established within the Division for Fighting Organised Crime and Corruption in the Criminal Police Department. The division employed officers with university degrees who are capable to respond to the tasks related to these issues. In addition, the Division for Combating Commercial Crime (total of 22 officers) also dealt with this type of offence. This Division included locally based units. The Forensic Centre in Danilovgrad also recognised the need to employ a forensic expert to provide expert analyses and opinions regarding computer technologies.

The Forensic Centre following seizure by authorised police officers undertook all examinations of seized computers. The special unit did not have a digital forensics capability.

The main challenges identified in performing the assigned tasks relating to combating cybercrime are an insufficient number of trained staff, and insufficient software and hardware.

5.3.2 Assessment and summary of progress made

The police have established a specialised unit within the Organised Crime Department. It is currently comprised of 1 officer. There is another person who conducts, inter alia, forensic examinations. This unit is part of the Department for Organised Crime and Corruption. Its tactical investigation wing investigates a range of criminal activities including cybercrime.

There is no specialised prosecution unit as there is not sufficient demand to justify its creation. This position can be reviewed should the situation change in the future.

Current real or perceived obstacles to developing capability are:

- lack of equipment and analytical software within the Cybercrime "Unit"
- lack of operational experience and operational "know how"
- lack of practical operational training
- lack of resilience and capacity within the cybercrime and forensic units.

The risks for Montenegro with the current capability of only one investigator and one person dealing with digital evidence are obvious.

5.4 International cooperation

5.4.1 The situation at the outset

Police to police cooperation and activities of joint investigation teams were conducted officially through NCB Interpol, Podgorica, according to bilateral agreements and the Police Cooperation Convention for South-East Europe.

5.4.2 Assessment and summary of progress made

The Ministry of Justice has competence for all issues regarding mutual legal assistance. It is responsible for processing of rogatory letters and in urgent cases requests for assistance can be sent via Interpol or directly to the appropriate authority. It is recognised that the procedures with respect to international co-operation are not efficient enough given the nature of cybercrime cases.

Most requests have been in respect of credit card fraud. To facilitate the future production of statistics, the International Legal Assistance Division will appoint one person who will process all future requests and applications relating to cybercrime.

Bilateral agreements are concluded with countries from the region and beyond. With the assistance from the project new legislation is drafted. A legal opinion was provided by the project on the law on international cooperation. It is expected that the new legislation will fully implement the provisions on international cooperation required by the Convention on Cybercrime and facilitate expedited international cooperation.

The project advised on the institutional set up, responsibilities and authority of 24/7 points of contact in line with article 35 of the Convention on Cybercrime. Specific training to increase the efficiency of this network was provided.

5.5 Law enforcement training

5.5.1 The situation at the outset

The Police Academy located in Danilovgrad was the institution in charge of training for law enforcement organisation in Montenegro. There was no documented training strategy for law enforcement officers covering the areas of cybercrime investigation and digital forensics. The police academy has hosted a number of training events on an ad hoc basis, organised by OSCE and other similar organisations.

No arrangements appeared to be in place with any academy or industry to assist in the development or delivery of cybercrime training, nor for individual training plans for investigators.

Training needs identified by Montenegro included detailed use of vendor forensic products, investigation tools, Linux forensics and training for police officers on how to search cybercrime scenes. In addition it was identified that members of the Police Directorate should be able to visit other services in order to find out about their work and see what software solutions they use in solving cases.

5.5.2 Assessment and summary of progress made

Basic training materials from the European Cybercrime Training and Education Group (ECTEG) will be used as the basis for training, which commenced in December 2012. This training will continue throughout the year on an ad hoc basis. A formal training strategy is planned to be drafted.

Police officers receive some basic instruction in recognising and handling electronic evidence. The main thrust of the training is dealing with preservation at the crime scene and referral to expert(s).

There are no plans to deliver advanced training as there are only two investigators who require it and it makes economic sense to send them abroad rather than run in house training.

First responders have not received any training in regard to cybercrime, but under CyberCrime@IPA a first responder course for all areas has been developed and some trainers have been trained to deliver this course in their respective countries.

Progress has been made in that Montenegro has embraced the available training courses through ECTEG and is planning to incorporate them in their programme.

As stated before several training activities were organised under CyberCrime@IPA project for law enforcement in which Montenegro participated. One law enforcement representative from

Montenegro (Police Commissioner at the Criminalistics and Forensic Centre) was funded to participate in the Master of Sciences (MSc) programme in Forensic Computing and Cybercrime Investigation offered by University College Dublin.

5.6 Judicial training

5.6.1 The situation at the outset

The Judicial Training Centre, which is an organisation of the Supreme Court of Montenegro, is the only institution responsible for the education of judges and prosecutors. The training consists of initial and continuous training. The initial training is organised for expert associates in the judiciary (in courts and prosecution services), as well as for graduated lawyers who meet the conditions for working in state bodies and who passed the bar exam. The goal of the initial training is to prepare the students for the judiciary. Continuous training is organised for judges and prosecutors and is aimed at maintaining and improving the knowledge, abilities and skills of the participants.

There was no documented strategy for training of judges and prosecutors that would include cybercrime investigation and digital evidence. However, there was a special programme for training in the field of criminal law that covers the investigation stage. One part of that training refers to the cybercrime investigation.

It is recognised that judges and prosecutors that deal with the cases that involve technology as the key element need advanced training so that they can fight this type of crime more efficiently. The Academy had no arrangements with academia, industry or specialised law enforcement cybercrime units to assist with the development or delivery of cybercrime training. The existing training in the field of cybercrime was considered insufficiently organised and inconsistent mainly because of lack of financial resources.

5.6.2 Assessment and summary of progress made

Montenegro has 110 Prosecutors. 10% have received basic training and 5%, advanced training. In May 2011, 10 Prosecutors and 10 Judges attended the training delivered in Skopje under CyberCrime@IPA. The train the trainer course (one judge and one deputy prosecutor) was completed by two representatives. Furthermore, a training strategy is currently being drafted.

With the assistance of the project, basic training materials were which will be incorporated into the curriculum. One basic training course was held in Montenegro and an advanced training course was delivered for also Montenegrin judges and prosecutors in "The former Yugoslav Republic of Macedonia".

The Judicial Training Centre has plans to introduce regular and continuous training for judges and prosecutors as advised under the project. This will include basic training for all new and appointed judges and prosecutors. It is intended to deliver one introductory training and 3 in-service training courses per year and exchange trainers and subject matter experts with neighbouring countries. There is a judicial training agreement with Croatia, "The former Yugoslav Republic of Macedonia" and the Judicial Academy in Serbia.

It is important that a training strategy is currently being drafted, which includes training on cybercrime and electronic evidence within the overall programme.

5.7 LEA/ISP cooperation

5.7.1 The situation at the outset

There is a special division within the Police Directorate that is, inter alia, responsible for the cooperation between Internet Services Providers and Police. It was reported that cooperation with Internet services providers was very good.

The procedure of issuing the licences to ISPs is defined in the Law on Broadcasting and in the Law on Electronic Communication.

There is an obligation for ISPs to retain data and this is provided by the Law on Electronic Communication.

5.7.2 Assessment and summary of progress made

Formal agreements in the form of MOUs exist between all ISPs, CSPs and the Cybercrime Unit. Contact points have been established who are able to provide IP addresses for suspect transactions and telephony data.

Legislation on the protection of personal data also demands that a court order is required for such information. This process can be completed within 24 hours and is not seen as an unduly arduous obstacle.

The law requires ISPs to provide information to law enforcement agencies when required to do so. Technical assistance for interpretation of this information is commercially available from the ISPs and CSPs in question. In addition, it is intended to organise events to improve knowledge of cybercrime.

There are no issues with ISPs who preserve data based on a phone call.

Progress has been made with regard to the conclusion of MOUs between law enforcement and ISPs, as well as the creation of points of contact. Interagency cooperation appears to work well at the operational level and other areas in the region may learn from.

5.8 Financial investigations

5.8.1 The situation at the outset

The main types of fraud identified were identity theft, counterfeiting of credit cards and non-cash payment cards as well as phishing frauds. Lack of equipment and trained officers were identified as obstacles to dealing with this type of criminal activity. The Criminal Code and the Criminal Procedure Code define the criminal offences that are subject to financial investigation and deal with the manner of conducting the investigations and seizure of property gained through criminal activities.

Financial investigations are the responsibility of prosecution service and police directorate, acting under the orders of the prosecutor. The responsible organisation for following money flows including those on the Internet is the administration for Prevention of Money Laundering and Financing Terrorism. This Administration serves as the financial intelligence unit and has been established as an administrative body and therefore it has the role to follow the money flows and to inform the responsible state bodies of suspicious transactions.

The activities for detecting criminal offences in this field are conducted by the Division for Fighting Organized Crime and Division for Preventing Commercial Crime in cooperation with the Special State Prosecutor.

Public and private sector organisations involved in the prevention and control of illegal money flows on the Internet, include Customs administration, Tax administration, courts, commercial banks, insurance companies, the Bar and companies that organise games of chance. Examples of cooperation between organisation has been seen in cases where criminal money flows on the Internet were notices by a commercial bank and reported to the Police Directorate, which took action under the Criminal Code. It was considered that the establishment of a National Criminal Intelligence Service would enable faster and easier exchange of operational data. This together with closer cooperation with Internet providers and sufficient training for staff would improve the capability to prevent and control illegal money flows on the Internet.

5.8.2 Assessment and summary of progress made

The Administration for The Prevention of Money Laundering and Terrorism receives suspicious transaction reports and regulatory cash transaction reports (> €15K).[28] They refer suspected criminal cases to the prosecution and police for further investigation. It seems that only few cases of money laundering have been investigated and prosecuted. Actual financial investigations appear to be limited.

The vast majority of cybercrime encountered is related to the use of counterfeit credit cards. One such criminal enterprise was identified in August 2012 whose activities accounted for €1.2 Million in fraudulent transactions. This case is currently under investigation.

The agency has the power to block financial transactions for up to 72 hours. An extension to this period requires the Prosecutors Office to apply for a court order. The Prosecutors Office can apply to have assets confiscated.

The agency can trace money flowing through banks and credit agencies only. There is no experience yet of money transfers through PayPal or other similar institutions.

Procedures exist for requesting from and reporting to, allied agencies such as the Tax agency and Customs. However, there is no direct access to their databases and therefore no software to present a consolidated view of these state controlled information assets.

There is regular formal and informal liaison maintained with the main banks, financial institutions and allied agencies. These "meetings" are not subject of any Memoranda of Understanding but have simply evolved in response to operational necessity.

It is reported that in Montenegro, information exchange is based on good relations between organisations. The anticipate having a centralized database for use by all dealing with the problems.

Several activities under the project targeted these issues, including the finalisation of the Typology study on criminal money flows on the Internet (2012) in cooperation with MONEYVAL.

[28] For details on the anti-money laundering system see the Moneyval evaluation and progress report. http://www.coe.int/t/dghl/monitoring/moneyval/Countries/Montenegro_en.asp

5.9 Progress made against previous recommendations

Cybercrime Situation Report March 2011	Progress reported
1. Keeping statistics that provide an insight in the seriousness of cybercrime in the national territory. Such statistics could for example 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.	Not Completed
2. Keeping statics about the application of the specific powers in the criminal procedural code, including with information about application, technical details and cases concerned.	Not Completed
3. Consideration of the observations made in the report above on criminal law and criminal procedural law in view of possible amendments.	Partially Completed. Additional revisions in progress.
4. Consider the formation of a prosecution unit to combat cybercrime in accordance with the needs of the country.	May not be appropriate for needs.
5. 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
6. 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
7. 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	Partially Complete
8. 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"	Not Completed. Not able to trace internet money flows.
9. 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. Investigators not yet trained.
10. 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.
Recommendations made by second progress report 1/11/11 – 31/5/12	
Creation of website and phone line for reporting of cybercrime incidents similar to the already existing for reporting corruption in Montenegro.	No progress reported
The National CERT team is functioning since 2012 under the Ministry of Information Society.	Complete

Organizing Training for members of joint investigative team, including members of FIU and Cybercrime unit.	Some progress
Overcoming the problem of lack of educated professionals and sophisticated technology for tracking and examining of digital evidence.	Some progress reported
Strengthening of international cooperating relating to exchanging data and intelligence of criminal money flow.	Some progress reported
Creating public campaign for raising awareness for issues of all types of cybercrime	No progress reported

5.10 New recommendations

1. Nominate a "portfolio holder" for cybercrime issues within the Prosecutors Office. Nominee to act as an advisor on cybercrime and associated policy issues (instead of creation a specialist Prosecution Unit).

2. Develop a national training strategy to include all police officers, 1st responders and investigators.

3. Assign "ownership" of incomplete recommendations above and review progress.

6 Serbia

6.1 Cybercrime and the criminal justice system

6.1.1 The situation at the outset

Since 2006, a specialised Department to combat cybercrime was established within the District Public Prosecutors Office of Belgrade named Special Prosecutors Office for High-Tech Crime, followed by establishment of Special Department for Combating High-Tech Crime within Special Service for Combating Organized Crime of Ministry of Interior and Special Investigative and Trial Chamber for High-Tech Crime of Higher Court in Belgrade with national wide jurisdiction. Since then a wide range of criminal activity directed against the security of computer crimes was dealt with. Most frequently occurring were unauthorised access to computer systems, computer fraud, forgery and misuse of credit card and violation of copyright and related rights with new increasing trend of child pornography cases.

From 2005 to November 2010, a total of 1010 cases were reported to the Special Department for High-Tech Crime of the Prosecution Office, of which 565 were solved and 154 persons were convicted, including decisions of the Court of Appeal of Belgrade. From information received at a later stage over the whole year 2010 it appears that the majority of cases concerned copyright violations. The second next category was computer fraud together with child pornography. The offences against confidentiality, integrity and availability of computer data and systems were represented by a few cases. The statistics kept by the High Tech Crime Unit showed on which basis an investigation started, in what phase of the prosecution of the case was and whether the case was submitted to the court and what the outcome was.

Reports of cybercrime have been received within this jurisdiction since the 1980s. The number of reported incidents peaked during the 1990s. In 2009 the nature and seriousness of reported crimes changed. Serious frauds, abuse of identity and the emergence of child pornography were becoming more prevalent. This change in the nature of this type of crime proved to be the driver for establishing the National Centre for Cybercrime Investigations.

6.1.2 Assessment and summary of progress made

As a country with mature institutions and capabilities Serbia is aware that the entire spectrum of cybercrimes is being committed within and against entities within their jurisdiction. There is an information system in use for recording and managing such incidents and statistics were readily available, defining the type and nature of the cybercrime threat. Statistics produced by the Prosecutors Office, gave a breakdown of offence types, numbers of victims, conviction rates and the number and nature of requests for international assistance made and rendered. It is therefore possible to empirically demonstrate how successful their institutions are at tackling cybercrime. In 2012, there were 770 cybercrime cases and initial data for 2013 confirm that the number is dramatically increasing.

Discussions with senior managers also revealed ample evidence that anti-cybercrime activities fell within a broader performance management regime. Managers of departments were therefore well informed about threats and the effectiveness of current interdiction activities.

Many criminal acts such as blackmail, extortion, as well as offences involving harassment or threats are now almost entirely technically transmitted. It is difficult to conceive a blackmailer or extortionist typing out their demands onto paper and sending it through the mail.

Detailed statistics were provided to the assessment team for examination.

It should be noted that during the implementation of the project, the team in Serbia showed leadership and made full use of opportunities created by the project. The members were committed and skilled and followed up on the recommendations made by the project. This is an excellent example of authorities taking responsibility for improving their capabilities against cybercrime with the assistance received from the European Union and the Council of Europe.

6.2 Legislation

6.2.1 The situation at the outset

Serbia ratified the Budapest Convention on 14 April 2009 and its Additional Protocol on Xenophobia and Racism on 14 April 2009. The Convention on the Protection of Children against sexual Exploitation and Sexual Abuse was ratified by Serbia on 29 July 2010.

Serbia implemented to a large extent the provisions of the Budapest Convention although some provisions might require a detailed review in the future. However, considering the on-going legal reform and the change in the Government the adoption of amendments might be possible only after the end of the project.

6.2.2 Assessment and summary of progress made

During the inception phase a Situation Report was prepared under the project to provide information on the status of cybercrime legislation in the project areas. The regional Workshop on legislation organised in Sarajevo on 24-25 March 2011 was aimed at discussing the findings and the recommendations made in the Situation Report.

In order to follow up on these activities, Serbia requested a specific event on legislation to discuss possible amendments. The workshop organised under the project with representatives of the Ministry of Justice, Ministry of Interior, Parliament, judges, prosecutors and representatives of the Judicial Academy discussed in detail the Serbian legislation.

Several gaps have been identified in the substantive law provision e.g. no adequate implementation of Article 3 (Illegal Interception); Article 4 (Data Interference), Article 5 (System Interference); Article 6 (Misuse of device) and no implementation of Article 7 (Computer related forgery) as well as Article 12 (Corporate liability).

Subsequently, a legal opinion was provided on the new Criminal Procedure Code of Serbia in view of implementing the Budapest Convention on Cybercrime.

6.2.3 Recommendations

The recommendations made during the project, as well as the findings of the Assessment report adopted by the Budapest Convention and in the Discussion paper on protection of children against sexual exploitation and sexual abuse to be considered by the authorities in Serbia.

- Improve the legislation in light of the recommendations made during the project with regard to both substantive criminal law, including on protection of children against sexual violence and procedural law, including the Assessment Report adopted by the Cybercrime Convention Committee (T-CY) and legal opinion provided under the project.

6.3 Specialised institutions

6.3.1 The situation at the outset

Serbia had a department to fight cybercrime established within the Ministry of Internal Affairs as well as a Special Department within Higher Public Prosecutors Office in Belgrade (the Law on Organisation and Competence of Government Authorities for Suppression of High Tech Crime) with national wide competence and a Special Prosecutor for High-Tech Crime in charge.

The Ministry of Internal Affairs had responsibility for the investigation of criminal acts involving the distribution of illegal content on the Internet and crimes involving the infringement of intellectual property rights. The high tech crime unit was competent to conduct investigations of crimes against computer systems as well as all crimes that involve technology. Digital forensics collection and analysis was not conducted by the HTCU and was entrusted to special services under the Ministry of Internal Affairs.

Cooperation with foreign specialist HTCUs was via direct officer-to-officer communication as well as through various international police organisations such as Europol, the Southeast European Cooperative Initiative centre (SECI), Interpol and the 24/7 Network.

It was considered by Serbia that the main difficulties encountered by the HTCU in performing its assigned tasks were the lack of technical equipment and training; the long and formalised legal procedures for obtaining legal information and the requirement that prior judicial criminal proceedings have been started before such information may be obtained.

6.3.2 Assessment and summary of progress made

There are two sections within the Cybercrime Department, namely the Intellectual Property Violations and the High Tech Crime (Cybercrime Unit). The Cybercrime Unit is comprised of 20 people and ensures the functions of the 24/7 contact point for all law enforcement contact. It is intended to improve capability for investigating cybercrime. The Cybercrime Department is able to demonstrate advanced capabilities in this field and is one of the beacon institutions within the region. The department is well equipped with hardware and analytical software, as well as highly competent and experienced staff.

Advanced software has also been developed "in house", which can geographically locate sources of VOIP communications. This is a sophisticated capability, which will not be within the reach of all Hi Tech crime units within the region.

In addition to conducting these advanced technical investigations, the Cybercrime Department offers advice and assistance to other specialist crime units on search and seizure of devices and equipment; handling procedures and sources of electronic evidence. It has also the capability for live interception of Internet communications (for serious crimes). From 15 October 2013 they will be able to perform Internet interception for all computers based criminal acts, not just serious and organised crimes. This development recognises that electronic evidence is now forming part of mainstream investigations and is not confined to specialised investigations.

Computer Forensics is a service separate from the Cybercrime Department that carries out forensic examinations of computers for the entire Serbia. In common with many such departments there is a backlog of work which causes delays to investigations and prosecutions.

There are 3 Deputy Head Prosecutors with national competence to deal with the most serious aspects concerning Intellectual Property violations. There are two advisors and administrative

support to these Deputies. They are currently dealing with an excess of 500 cases a year, which are rising annually in number and severity.

There is a threshold of 2,000 items or a value of 1 Million Dinars, which governs prosecutorial competence. Below this level, Specialist Prosecutors have the authority to intervene and assume responsibility for cases in certain circumstances.

There was a specialist chamber within the higher court for dealing with the more serious cybercrime cases. Dedicated cybercrime judges have been in use for some time. However, electronic evidence has increasingly become part of "business as usual" within the countries judicial processes. A recent reorganisation now means that all judges may hear "general" cybercrime cases. This change was also implemented, as there were concerns that judges should not be unduly influenced by a small number of specialists.

The Prosecutors Office is the 24/7 point of contact for all legal requests. The Cybercrime Department serves as the 24/7 contact point for all law enforcement requests whilst ensuring that formal procedures are correctly adhered to.

6.4 International cooperation

6.4.1 The situation at the outset

The execution of mutual legal assistance requests was the responsibility of domestic courts and public prosecutors with certain procedural actions conducted by the Ministries of Justice, Internal Affairs and Foreign Affairs. Legal requirements prescribed the structure and contents of applications to be sent. The requests were submitted to the foreign authority through the Ministry of Justice; however the recipient country may request delivery through diplomatic channels. Delivery may also be made directly to a foreign judicial authority, or in emergency cases through Interpol.

The main obstacle seen by Serbia in relation to international cooperation is the lack of promptness of competent authorities and companies who hold data that is requested, as the experience is that requests are not responded to. The lack of means other than international legal requests is seen as an obstacle to collecting necessary information.

6.4.2 Assessment and summary of progress made

Statistics reveal that Serbia makes approximately 15 requests for international assistance each year, mainly to the US and Europe. There have been no instances of jurisdictional conflicts. Detailed statistics were provided to the assessment team for examination.

Formal and informal contacts exist with Interpol. Mutual legal assistance has been rendered to Montenegro, Croatia, Switzerland, Sweden, USA and North Korea.

The main obstacle to international cooperation, with one or two notable exceptions, remains the lack of promptness of competent authorities and companies to respond to requests.

There has been a substantial increase in the number of incoming and outgoing requests dealt with by Serbia.

Under CyberCrime@IPA a Regional Workshop on international cooperation was organised in Skopje, "The former Yugoslav Republic of Macedonia" to provide advice to the Ministries of Justice and prosecution service on how to handle in an expedited manner international cooperation requests relating to cybercrime. Experts from Belgium, France, Romania United

Kingdom, USA as well as private sector were invited to share experience and good practices. The workshop presented practical examples of successful cooperation between countries, cases of success and failure in the cooperation with the private sector, as well as channels for international cooperation, in particular the 24/7 network and Southeast European Law Enforcement Centre (SELEC).

The Cybercrime Convention Committee (T-CY)[29] will assess in 2013 the implementation by Parties of the relevant international cooperation provisions in view of identifying solutions for increasing the efficiency of international cooperation in cybercrime investigations.

6.5 Law enforcement training

6.5.1 The situation at the outset

The Academy of Criminalistic and Police Studies conducted Law enforcement training in Serbia. The Ministry of Education accredits the Academy as does the Ministry of Science and Technological Development to provide education in four fields of study.

The teaching was delivered by staff that was academically qualified to PhD or MA level. The academic studies are supplemented by practical teaching, which is mostly carried out by organisational units of the Ministry of Interior, as well as other institutions dealing with security and safety affairs.

Cooperation with related institutions in Serbia and abroad had been established through specific study modules; exchanges of students, teachers and experts; conduct of scientific research and other related activities.

There was no specific training centre devoted to delivering cybercrime training in Serbia and no documented cybercrime or digital forensics training strategy. There were no specific professional or academic qualifications available to law enforcement officers, specifically in the areas of cybercrime or digital forensics investigation. Most of the training that was available was delivered on an ad hoc basis either taking place in Serbia or abroad. This includes training delivered by the Organisation for Security and Co-operation in Europe (OSCE) on a regional basis.

New recruits to law enforcement did not receive training within their programme to provide them with the skills and knowledge to recognise and deal with electronic devices that may contain evidence in relation to any crime, including traditional crime.

The Directorate for Education, Training, Professional Development and Science, part of the Ministry of Interior was responsible for training of cybercrime investigators. A course was delivered (21 days), which was based upon the introductory forensic computing and network investigation course developed by the European Cybercrime Training Education Group (ECTEG).

A project was underway involving the Ministry of Interior under the Academy's special project: Police, Security and Hi Tech Crime to incorporate the Ministry's needs for basic, Masters and specialist studies; and include on-going practical training for members of the High Tech Crime Unit and other officers. Cybercrime was identified by project members as appropriate for further research.

It was considered that any training should have internationally recognised certificates, thereby enhancing expertise in the testimony of police officers in criminal proceedings.

[29] Serbia is represented in the Bureau of the Cybercrime Convention Committee, T-CY.

6.5.2 Assessment and summary of progress made

The training strategy is based upon deploying a training programme for ICT, Leading to Bachelors and then Master Degree. This proposal is currently awaiting accreditation and expect a decision by the end of 2012 or early 2013.
The Police Academy intends to build capacity within the Programme in order to provide specialist modular training that will include:

- CID courses
- Computer Forensics
- First Responder Training
- ISPs, CSPs and banking, investigations
- Others

This training will be open to law enforcement officers, Ministry of Interior employees and university undergraduates. It will be also open to professionals from all surrounding regions.

Local, "basic" training has been delivered to 30 police officers and first responders. This is considered to be an important part of the training strategy as these officers "feed" the entire criminal justice chain.

The Academy would like to use those individuals who took part in the Masters programme as Professors for the Academy programmes. This will not be possible under the accreditation requirements, as all delivering higher training must have a PhD. This is a major obstacle to maintaining a sustainable programme of continuous development.

There have been strong representations that the MSc be extended to PhD level. Such a move would support the Academy training programme that would be open to applications from international students.

Serbian experts deliver ad hoc cybercrime training on international, national and regional levels.

National and Regional training was delivered in the police academy supported by regional project (OSCE) as follows:

- Malware (National Law Enforcement Training)
- Basic training and train the trainers (Regional police)
- Linux (Regional police)
- Nordic Mule Software (Regional police)
- Digital Evidence (Judges, Prosecutors and police)

Serbia has made use of the opportunities offered by the CyberCrime@IPA project e.g. development of the cybercrime training strategy, ECTEG training materials etc. Furthermore, it has delivered trainings at the international level through a number of projects.

One law enforcement representative from Serbia (Senior Police Inspector, 24/7 Contact Point, Cyber Crime Department, Service for Combating Organised Crime, Ministry of Interior) was funded to participated in the Master of Sciences (MSc) programme in Forensic Computing and Cybercrime Investigation offered by UCD. Serbia participated also in all the trainings organised or supported by the project.

Much work has been conducted in Serbia, with the potential for the country to become a regional centre of excellence that may build on their previous activities.

6.6 Judicial training

6.6.1 The situation at the outset

Judicial training in Serbia was conducted by the Judicial Academy, which is a public institution in charge of the development and delivery of initial and continuous training of judges and prosecutors. There was no documented training strategy for judges and prosecutors covering the areas of cybercrime investigation and digital evidence.

Judges and prosecutors, who are generally trained together, did not receive training in their initial programmes on these subject matters, however there was consensus among members of the Programme Council and the Commission for Developing the Curriculum for initial *t*raining that these issues should be included in this training. The Programme Council also took the position that training on cybercrime and related issues should be part of continuous training modules. In relation to "in-service" training, there had been training events in cooperation with donors, in the subject matters, organised on a frequent basis since 2007. It was recognised that judges of higher courts and prosecutors specialising in cybercrime should undergo advanced training in this area.

The "in-service" training needed to be upgraded to provide the skills and knowledge on this subject and an efficient practice developed in the initial training programmes. Serbia identified that some courses run by Europol, the Federal Bureau of Investigation (FBI) in the USA and the Serious and Organised Crime Agency (SOCA) in the United Kingdom would be advantageous to judges and prosecutors.

6.6.2 Assessment and summary of progress made

There is now a training strategy in place for judges and trainers. Under the project prosecutors and judges have received basic and advanced training. Feedback from attendees has rated this training as excellent. Training will be delivered to all newly appointed prosecutors and judges as well as those already in post. Refresher training will be continuous throughout an individual's career and will be revised to incorporate new developments.

Two representatives (one judge and one prosecutor) participated in the train the trainer course organised by the CyberCrime@IPA project. The basic training provided in Belgrade attended by 14 participants was very successful. An advanced training for 5 judges and 5 prosecutors was also carried out under CyberCrime@IPA project in Skopje. Plans to extend this training are included in the training strategy.

The development by the project of the Electronic Evidence Guide was welcomed as a tool that will make a difference. It is already incorporated into the curriculum and has become part of a training module.

6.7 LEA/ISP cooperation

6.7.1 The situation at the outset

There were about 200 ISPs in Serbia, although the number fluctuates constantly. ISPs provide the entire range of Internet related services as well as 3G Internet and Voice over IP (VoIP) services. The Ministry of Telecommunications and the Serbian Republic Agency for Electronic Communications (RATEL) hold data relating to ISPs. In addition, there is an Association of Internet Service Providers (UISP)[30]. The speed of data exchange in many cases is identified as a

[30] www.uisp.rs

concern, with certain providers providing an inadequate response to requests by the Ministry of Internal Affairs. The problem identified was insufficient regulation of ISPs in terms of their obligation to retain data. In order to obtain traffic and subscriber data, a written request was made by the Ministry of Internal Affairs and in order to obtain content data, a court order was required.

Points of contact exist in most of the important ISP companies, who are obliged by law to retain data. Cooperation between ISPs and law enforcement was based on legal regulations. There were ad-hoc meetings but without special protocols. There were no common training programmes for law enforcement and ISPs.

6.7.2 Assessment and summary of progress made

Serbia has included in the electronic communications law the procedure to be followed when requests for data retention are made. It's a new law that contains specific steps that both sides need to take once the request has been made. In case of disputes there is a regulatory agency that is part of the state mechanisms.

Numerous MOUs have now been signed with a number of ISPs and liaison with the most important providers is good. Although cooperation has improved slightly, some of the problems previously highlighted persist, namely the speed of data exchange remains a concern with some companies providing an inadequate response.

Serbia has progressed in this area since the beginning of the project with the signing of a number of MOUs as recommended by the project.

A number of activities organised under project provided advice on these issues.

6.8 Financial investigations[31]

6.8.1 The situation at the outset

The types of fraud identified included computer fraud, "Nigerian" fraud, misuse of credit cards, fraud involving electronic banking and electronic transfers. No statistical information was available. The main problems identified as obstacles to prevention and control of criminal money flows on the Internet were the technical inability to determine cash flows, especially when anonymous services are used and where data is held in countries where international legal assistance is needed. It was recognised that the speed of the transactions was not matched by the speed of the legal procedures needed to trace the transactions.

In terms of the legal provisions available to follow criminal money flows and to search, seize and confiscate proceeds, the law on confiscation of property of criminal offenders provided general provisions and it was possible to conduct a financial investigation and confiscate assets regardless of how crime occurred. If the offence was committed on the Internet and met the general provisions, a financial investigation was conducted. These investigations began when the prosecutor gave the order for such an investigation and conducted by the financial investigation unit in the Ministry of Internal Affairs.

The roles of the institutions responsible for the subject matters were as follows:

- Ministry of Finance - Administration for the Prevention of Money Laundering

[31] For detailed reports on the anti-money laundering systems see the Moneyval reports at: http://www.coe.int/t/dghl/monitoring/moneyval/Countries/Serbia_en.asp

- Ministry of Internal Affairs – Financial investigations conducted by the Financial Investigation Unit (FIU)
- Ministry of Justice - prosecution, court proceedings and seized property management

These Ministries were institutionally responsible for monitoring the money acquired through criminal enterprise and for the detection, seizure and confiscation of the assets acquired through crime, regardless of whether the crime was cybercrime or not.

Serbia suggested that the efficiency in this type of activity would be increased by the connection of databases of public and private sector in a single system.

6.8.2 Assessment and summary of progress made

A key strand in Serbia's fight against organised crime is the seizure and confiscation of illegally gained assets. Prosecution of key individuals coupled with confiscation of assets has proved to be the most effective method for disrupting criminal enterprise. The financial regulatory services have enjoyed considerable success and have so far confiscated in excess of €100 Million from criminal activity. It was not possible to identify what proportion of this was confiscated as a result of cybercrime.

Assets seized have included apartments, cars, stocks, bonds and cash. Accounts have been frozen and temporarily seized pending judicial adjudication. The proceeds of these seizures are reinvested into community projects, law enforcement and the national Treasury.

There are two separate departments involved in financial investigations, those for organised crime and those for other criminal cases.

There is close cooperation between all law enforcement agencies, tax offices and financial institutions with regard to the prevention of money laundering. A key success factor identified is the ability of all of these agencies to share data. The development of software, which will provide a consolidated view of multiple data sources, will greatly enhance the ability to identify illicit funds, suspects and the confiscation of assets. The integration of data sources is complete and training in system use is on-going.

A specialist department carries out analysis of financial transactions but credit for much of this success must go to individual investigators using old-fashioned pen and paper.

The level of cooperation in this field is excellent and is assisting in this important area of work. The software currently under development will enhance capability. The software should be assessed to establish its suitability for use in other project areas and the wider enforcement community.

6.9 Progress made against previous recommendations

Cybercrime Situation Report March 2011	Progress reported
1. Apart from the statistics held by Special Department for High-Tech Crime of the District Public Prosecutors Office of Belgrade, keeping statistics that provide an insight in the seriousness of cybercrime in the national territory. Such statistics could for example 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.	Mostly completed.
2. Keeping statistics about the application of the specific powers in the criminal procedural code, including with information about application, technical details	Completed

and cases concerned	
3. Consideration of the observations made in the report above on criminal law.	Almost completed
4. Consideration of the observations with regard to present criminal procedural law in view of possible contributions to the new Criminal Procedural Code to be adopted by Parliament mid-2011.	Almost completed
5. 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.	Strategy completed. Awaiting accreditation of ICT training programme.
6. 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.	Training strategy in place.
7. 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. Additional MOU's agreed and signed.
8. 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 Capability development is underway
9. Incorporate good practice in the handling of electronic evidence in criminal investigations; examining existing guides such as those developed by Interpol and Europol.	Content incorporated into the training curriculum for Judges, Prosecutors and Police
10. 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.
Recommendations Made by Second Progress Report 1/11/11 – 31/5/12	
No recommendations made	

6.10 New recommendations

1. Improve the legal framework in line with the recommendations made in the section on legislation.

2. Develop existing capability and operational procedures for securing digital evidence on site from "live" computers. The evolving use of encryption and cloud computing by criminals requires more advanced capabilities.

3. Developing "live" communication interception capabilities. Again, changing criminal tactics and increasing use of VOIP require further technical developments.

7 "The Former Yugoslav Republic of Macedonia"

7.1 Cybercrime and the criminal justice system

7.1.1 The situation at the outset

The main categories mentioned (in brackets the percentage of all cases) were:

- Abuse and forgery of credit cards by ATM, POS and E-commerce [45%]
- Intrusion of computer systems (Phishing, DDoS attacks, SQL Injection, etc.) [20%]
- Child pornography [10%]
- Internet fraud [20%]
- Other (abuse of personal data, software piracy etc.) [10%]

No absolute figures were provided and no period of time specified.

7.1.2 Assessment and summary of progress made

There has been little change in the cybercrime profile up until 2010 when the majority of cases were related to credit card fraud. Since then there has been a shift and a new kind of criminality is emerging:

- Illegal intrusions into computer systems
- Denial of Service attacks
- Phishing and e fraud
- Defacement of websites
- Child pornography.

Precise statistics are not readily available but can be produced with notice. Cases are not logged into an IT system and thus statistics are not readily available for routine management scrutiny and do not form part of any performance management regime.

There have been only a relatively small number of prosecutions in respect of child pornography. However, there are a large number of computers still awaiting examination. These computers were seized largely as a result of information received from Interpol and relate to Macedonian IP addresses accessing web sites containing child pornography.

Penalties for possession of child pornography are high and this is also believed to have a prevention impact. As most cases are reactive, triggered by Interpol, it seemed that there is little or no proactive investigations being undertaken with regards to this type of crime.

7.2 Legislation

7.2.1 The situation at the outset

"The former Yugoslav Republic of Macedonia" ratified the Budapest Convention on 15 September 2005 and its Additional Protocol on Xenophobia and Racism on 14 November 2005. During the implementation of the project on 11 June 2012, "The former Yugoslav Republic of Macedonia" has ratified the Convention on the Protection of Children against sexual Exploitation and Sexual Abuse.

Some gaps have been identified in the Situation Report in the implementation of these treaties.

7.2.2 Assessment and summary of progress made

The substantive law provisions of the Budapest Convention have been mostly implemented in Macedonian legislation, including additional conduct e.g. production and dissemination of computer viruses. Among the gaps identified in the report were missing definitions of "service provider" and "traffic data".

The new Criminal Procedure Code was adopted in November 2010 to enter into force in December 2013 (postponed from November 2012)[32]. Its aim is to improve the efficiency of criminal procedures by strengthening the role of the public prosecutor, establishing the judicial police, improving investigative procedures and introducing a series of new special investigative measures. The new Criminal Procedural Code was mentioned by the project team only after the Situation Report was drafted and thus not analysed in the inception phase. Thus, under the project a legal review was carried out in case the authorities wish to carry out future amendments.

The Discussion paper on protection of children against sexual violence identifies some gaps that should be considered by future amendments. The issue of whether the practice of "streaming" indecent images of children constituted "possession" under local law was the subject of debate during the assessment. This may be decided by future case law. It does, however highlight the challenge of the law keeping pace with rapidly developing technologies. Continuous legal revision or the emergence of more durable legal terminology is necessary in order to keep pace with emerging criminal activities.

7.2.3 Recommendations

- Consider the recommendations made in the legal opinion provided under the project on the new Criminal Procedure Code of "The former Yugoslav Republic of Macedonia" (adopted in November 2010 to enter into force in December 2013)
- Consider the recommendations made in the Assessment report on the implementation of the preservation provisions of the Budapest Convention on Cybercrime, adopted by the Cybercrime Convention Committee (T-CY) to adopt specific legal provisions, and promote the use of the provision in practice
- Consider the gaps identified in the Discussion paper "Protecting children against sexual violence: The criminal law benchmarks of the Budapest and Lanzarote Conventions".

7.3 Specialised institutions

7.3.1 The situation at the outset

The Cybercrime Unit was established on 1 January 2005 in the form of a Section for investigation of cybercrime. From September 2008, the Section was upgraded to a Cybercrime Unit. The Cybercrime Unit was competent to deal with cases such as hacking, illegal interception and data interference as well as data manipulation, web site defacement, Distributed Denial of Service (DDoS) attacks and phishing. In addition, the unit dealt with crimes such as Internet fraud, child pornography, racism and xenophobia as well as other Internet related crimes.

There were seven members of staff within the Cybercrime Unit. At the regional level, there were no specialist investigators, although inspectors from the financial crime unit were responsible for cybercrime investigations at that level.

[32] Criminal Procedure Code of "The Former Yugoslav Republic of Macedonia (Official gazette, 150/10)

The cybercrime unit had regular meetings with ISPs, phone companies and banks to exchange information about cybercrime trends and threats. Cooperation with foreign cybercrime units was through direct contact in some cases, while for requests for digital evidence to be presented were dealt with through the international legal assistance procedures. The main difficulties encountered by the cybercrime unit is related to the slow process of obtaining data from foreign cybercrime units and the slow process of international legal assistance.

7.3.2 Assessment and summary of progress made

The Cybercrime Unit was established on 1 January 2005 in the form of a Section for the investigation of cybercrime. From September 2008, the Section was upgraded to a Cybercrime Unit. Currently the Unit consists of 11 Investigators. It has responsibility to combat all cybercrime activity on national level and to assist the investigation of Organised Crime particularly, the criminal use of technology. This Unit provides the functions of the 24/7 contact point with respect to cybercrime for external law enforcement agencies. Because of the increase in demand on the Cybercrime Unit, there are plans to delegate the less serious cases to "local officers" when sufficient have been trained.

Currently the Cybercrime Unit is preparing Standard Operating Procedures (SOP's) for investigating cybercrime cases and handling electronic evidence. The SOP's will be complete by the end of June 2013 and will be in use as of 1 October 2013. These SOP's will provide a general overview of the procedures for investigation of cybercrime cases and handling of electronic evidence. Furthermore, in the second phase, there are plans to develop practical and technical guidelines for the investigation of cybercrime cases and collecting of electronic evidence.

There are also plans to develop capacity for live data forensics. This would enable, "on site" recovery of digital evidence and minimise the risk of compromising data. The increasing criminal use of encrypted hard drives, malware codes, cloud computing and remote storage have necessitated this tactical development. New Procedural Codes have been introduced which authorises and facilitates such interdiction.

"Technicians" situated in a separate department carry out forensic examinations of computers. This was felt to be an obstacle to effective working as it hampers direct contact with investigators leading to a lack of clarity in some complex cases. There is also a backlog of computers awaiting examination and delays hamper the investigative process. The counter argument proffered was that forensic capability should always be independent of law enforcement influence.

The Public Prosecution Office in Skopje has established a specialist Cybercrime Prosecution Unit. This unit has competence to deal with all cases. There are currently 3 prosecutors working within this department. This is set to rise to 4 or 5 with 3 additional assistants in order to cope with the rise in demand. The Prosecution Service has the responsibility for serving as the 24/7 contact point.

There are 21 basic public prosecutors offices in "the former Yugoslav Republic of Macedonia". Skopje has the only cybercrime specialists in the country as it handles approximately 50% of all cases and is the largest Prosecutors Office at national level.

As far as the rest of the country is concerned the Unit in Skopje provides expert advice and guidance and professional lead in this field. They also provide knowledge resources via special links to a case-database that contains a number of examples of good practice, which has been borne of practical experience. The Unit also offers practical assistance and advice on the best method for handling cases and has proved particularly effective in disseminating good practice throughout the entire Prosecution Service.

The establishment of a Computer Emergency Response Team (CERT) is underway. This team will be responsible for incident handling on the national level, within both private and public sectors. They will provide guidance on handling of incidents and prevention advice. Once established, it is anticipated that they will negotiate the necessary MOUs based upon operational requirements.

Initial scoping activities have begun to consider whether a National Centre of Excellence could be established. So far potential strategic partners have been identified from academia, industry, private sector and law enforcement. Dialogue has already begun and there is a groundswell of support for this as the benefits are manifold.

The creation of the specialised prosecution department is a welcome initiative in line with the recommendations made in the situation report.

7.4 International cooperation

7.4.1 The situation at the outset

"The former Yugoslav Republic of Macedonia" has implemented the relating provisions of the Budapest Convention (including concerning extradition). Mutual Assistance is the subject of Chapter XXX of the Criminal Procedure Code.

7.4.2 Assessment and summary of progress made

The Department of International Cooperation and Legal assistance within the Ministry of Justice has concluded a number of existing bilateral agreements. The department is responsible for mutual legal assistance. Statistical data detailing the types of requests and assistance are not automatically available as no "back office" software supports this business process. Statistics need to be manually counted and so are not readily available.

However, in common with most countries in the region, the process can be lengthy and take many months to complete. Time delays are understandable due to various legal and political considerations. But these delays are not conducive to effective investigation. The sequence of events for such requests is often lengthy involving numerous Ministries" and departments.

Good relationships exist between representatives of Interpol and the members of the Cybercrime Unit. However, in the case of Internet fraud, it was pointed out that about 90% of requests or reports remain unacknowledged. The precise underlying reasons are complex and are due in part to the method of operating. Many enquires do not produce fruitful results. Often enquiries are fragmented and require multi-jurisdictional response when the particular significance of each fraction is not fully understood. Another issue is that many overseas cybercrime capabilities are being swamped and are not able to cope with demand. Some jurisdictions have taken the decision to prevent a particular crime rather than reactively investigate new reports.

The Cybercrime Unit has successfully investigated a number of complex multi-jurisdictional cases. One on-going case involves the counterfeiting of credit cards and internet fraud in collaboration with Slovenia, Croatia and Bulgaria. The Analytical Work File was instrumental to this investigation.

This unit is currently developing "Good Practice Manuals" which will provide practical guidance on how to investigate:

- E commerce fraud

- DDOS attacks
- Phishing
- Defacement.

Cooperation with countries within the Project was described as outstanding. However, responses from Interpol and Europol were described as satisfactory. There have been a number of joint investigations with the FBI in cases of illegal intrusion into computer systems.

A number of Joint investigations have also been undertaken in collaboration with SOCA and FBI in respect of e- commerce, fraud and phishing.

It is clear that operationally, excellent cooperation mechanisms have been created.

7.5 Law enforcement training

7.5.1 The situation at the outset

There was no training strategy for law enforcement staff in the areas of cybercrime investigation and digital forensics and no institution responsible for providing training on this subject. No academic or professional qualifications existed for staff in this area. The cybercrime unit provided internal basic investigation for its staff members. No arrangements existed with academic or industry bodies to assist in the development and delivery of training and cybercrime unit members did not have individual training plans.

It was recognised that training for first responders as well as training for investigators would be beneficial along with digital forensics training. Joint seminars and workshops with foreign investigators with similar legal systems was also seen a beneficial.

7.5.2 Assessment and summary of progress made

There is not yet a strategy in place in respect of cybercrime training. Training for the investigation of child pornography was organised in 2011by the French Embassy and was held using training centre facilities.

Under CyberCrime@IPA:

- Investigators and other officials were trained on the need to ensure the rule of law and human rights principles (Article 15 of the Convention on cybercrime - Safeguards and conditions) when applying the investigative measures foreseen under the Budapest Convention to investigative cybercrime.
- One law enforcement representative from "The former Yugoslav Republic of Macedonia" (Head Inspector – Leader of Team in Cybercrime Unit, Ministry of Interior) was funded to participated in the Master of Sciences (MSc) programme in Forensic Computing and Cybercrime Investigation offered by UCD.
- Law enforcement and prosecution services participated in several trainings (e.g. on interception of traffic and content data for law enforcement purposes), study visits and other activities that resulted in enhanced capabilities of law enforcement and judicial authorities to detect, investigate, prosecute and adjudicate cybercrime.

There are plans to commence cybercrime training for cybercrime first responders with the first course in November 2012. As previously stated, a first responders course, including train the trainers to deliver this course will be organised under CyberCrime@IPA in 2013.

7.6 Judicial training

7.6.1 The situation at the outset

The Academy for Judges and Public Prosecutors was the institution responsible for implementation of training programs for judges, public prosecutors and other legal professionals who works within the judiciary. It was established in 2006 by the Law on the Academy, and has two major fields of activities:

- to develop, organise and implement initial training curriculum for candidates for future judges and public prosecutors, and
- to develop, organise and implement continuous training programme for acting judges and public prosecutors in the country.

There was no strategy for cybercrime and electronic evidence as a separate document; however, it was envisaged in the Framework "Continuous Training Program 2011-2012" of the Academy (two year programme).

Trainings had been organised jointly, for judges and public prosecutors, with participation of the representatives of the cybercrime unit from the Ministry of Interior. Future plans were to organise separate (specialised) training for judges and prosecutors, which are useful for both legal professions, in addition to common training.

As part of the continuous training programme, the Academy had organised several training events related to cybercrime for judges and public prosecutors. A total of 11 events were organised with 136 working hours in the last three years. The overall number of participants was 170; out of which 83 were judges, 65 public prosecutors, 13 legal associates, 3 court administrative staff, 2 representatives of the Financial Police Unit, 2 representatives of the Bar Association and 2 representatives from the Ministry of Interior. It was recognised that more advanced training is necessary for selected judges and prosecutors.

Suggestions for future activities included:

- Increasing the level of mutual international and, especially regional cooperation to strengthen the capacities of the institutions responsible for fight against cybercrime. This recognises that in the past, most accused persons were foreigners from neighbouring countries.
- Introducing international experts as trainers; in order to bring their practical experience to enrich the knowledge and skills of national trainers and target groups.

7.6.2 Assessment and summary of progress made

The "train the trainers" course has been completed by two trainers (two public prosecutors) and judicial training has commenced. Plans are in hand for the accreditation of this training.

Under the project judges and prosecuted participated in the basic and advanced course on cybercrime and electronic evidence. The course was held at the Judicial Institute, which took responsibility for the organisation and logistics of the event.

There is a coherent training strategy, which includes a continuous cycle of training for all judges and prosecutors throughout their practice career. Basic training is mandatory for all and advanced training is available to those demonstrating aptitude and desire.

The Cybercrime Unit provided training on practical difficulties involved with securing and ensuring integrity of electronic evidence. The judges and prosecutors involved rated this as extremely worthwhile.

The development of a training strategy has been completed since the beginning of the project and there is a clear plan to include cybercrime in the upcoming programme. The involvement of the police in the training has been recognised as valuable.

7.7 LEA/ISP cooperation

7.7.1 The situation at the outset

There were 3 main ISPs in "The former Yugoslav Republic of Macedonia" and the procedures for obtaining data from ISPs that cannot be obtained directly, was through a court order. A special unit in the Ministry of Interior carried out any legal authorised interception of communications. The cybercrime unit itself rather than any individual was the contact point for engagement with ISPs.

Data retention is obligatory for ISPs. Regular working meetings take place between the cybercrime unit and ISPs as required on a case-by-case basis. There were no joint training programmes in place.

7.7.2 Assessment and summary of progress made

Informal and formal contacts with the main ISPs exist although all formal requests are still made through a court order. In urgent cases such orders may be obtained in less than 30 minutes.

There is ample evidence of cooperation with international service providers such as Google, Facebook and others both on formal and informal levels.

Cooperation with ISPs appears to be acceptable and as time progresses the conclusion of MOUs as recommended in the Situation Report may ensure that this continues.

The creation of a cybercrime strategy and implementation of CERT project is seen essential along with the need to improve public awareness of cybercrime.

7.8 Financial investigations[33]

7.8.1 The situation at the outset

The main types of fraud and crimes involving proceeds of crime were credit card abuse and Internet fraud (Nigerian fraud, buying expensive wares for low prices, fictitious introduction for fraud, fictitious lottery - spam messages). The Macedonian experience of this type of crime was limited, although a lack of public awareness was considered to be a key issue.

The Macedonian authorities had implemented "all crime approach" regarding the predicate offences for money laundering. Proceeds from crime on the Internet/computer systems were considered to be objects of money laundering. All measures are prescribed in the Law on the prevention of money laundering, other proceeds of crime and financing terrorism (AML/CFT Law).

[33] For detailed reports on the anti-money laundering systems see the Moneyval reports at: http://www.coe.int/t/dghl/monitoring/moneyval/Countries/MK_en.asp

The Office for Money Laundering Prevention and Financing Terrorism (OPMLFT), within the Ministry of Finance, acts as the Financial Intelligence Unit (FIU) and is competent to collect, process, analyse, keep and disseminate data to the competent authorities.

OPMLFT had no experience of interagency cooperation for the prevention and control of fraud and proceeds-generating crime, nor in identifying criminal money flows of proceeds from crime on the Internet.

It was considered that all financial institutions obliged to undertake the AML/CFT measures should be involved in the prevention of criminal money flows on the Internet. For the purposes of AML/CFT prevention these obliged entities regularly cooperate with the OPMLFT.

7.8.2 Assessment and summary of progress made

The Financial Investigation Unit is responsible for investigations of money laundering, corruption, counterfeit currency and tax evasion.

There is not an IT system available to support their activities and statistical data is not automatically available. Manual statistics can be obtained with notice but will require effort, which would remove resources currently involved in live investigations.

Cooperation with banks was reported to be inconsistent as some banks are more cooperative than others. There is a good cooperation on a daily basis with regards to credit card fraud. A meeting takes place with representatives of the major banks bi-monthly. At these meetings information is exchanged identifying emerging frauds, possible rogue "companies" and potential victims.

In relation to money laundering it appears to be effective systems and activity.

7.9 Progress made against previous recommendations

Cybercrime situation report March 2011	Progress reported
1. Keeping statistics that provide an insight in the seriousness of cybercrime in the national territory. Such statistics could for example 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.	Not readily available
2. Keeping statics about the application of the specific powers in the criminal procedural code, including with information about application, technical details and cases concerned.	Not readily available
3. Consideration of the observations made in the report above 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.	Incomplete (limited cooperation with the Ministry of Justice during the implementation of the project)
4. Consider the formation of a specific prosecution unit to combat cybercrime in accordance with the needs of the country	Completed
5. Development of a cybercrime training strategy incorporating the requirements of cybercrime investigators, digital forensics examiners and mainstream law	Capability not

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. Build upon the existing programmes offered by the Police Academy.	developed
6. 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.	Completed
7. 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.	Partially completed
8. 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".	Capability not developed
9. Incorporate good practice in the handling of electronic evidence in criminal investigations; examining existing guides such as those developed by Interpol and Europol.	Completed
10. 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
2nd Progress report 1st November 2011 - 31 May 2012	**Progress reported**
No recommendations	

7.10 New recommendations

1. Conclusion of Memoranda of Understanding between ISPs and law enforcement.

2. Identify specific problematic issues with ISPs and if necessary consider whether legal framework needs to be improved.

3. Ensure that all recruits receive basic training in electronic evidence. The cybercrime "Guide on Electronic Evidence" should be incorporated into the curriculum.

4. Develop capability and procedures for obtaining digital evidence more effectively and in particular obtaining evidence from live computer systems.

8 Turkey

8.1 Cybercrime and the criminal justice system

8.1.1 The situation at the outset

Some examples of cybercrime mentioned were illegal access, illegal interception, child pornography, obscenity, identity theft and fraud.

Case statistics

Type	Article in criminal law	Cases	Pending	Arrested suspects	Convictions
Fraud	158 (1)	7175	4283	7531	1702
Obscenity	226 (1a)	94	60	61	18
Child Porn	226 (1c)	211	122	113	41
Illegal access	243 (1)	635	439	180	35
Computer Sabotage	244 (1)	339	220	205	18
Credit card Fraud	245 (1)	3689	2334	2568	1150
	Total	12143	7458	10658	2964

8.1.2 Assessment and summary of progress made

Turkey continues to experience the entire spectrum of cybercrime. Some statistics were available to the assessment team, which gave an overview of offence types experienced. About 50% of reported offences related to credit card frauds involving counterfeit cards manufactured abroad.

Turkey has the UYAP, Criminal Justice Information system and analysts extract statistics twice yearly. These statistics are subject of regular performance reviews and are used to identify potential areas requiring management intervention.

Anecdotal evidence indicates a shift towards attacks on cyber banking, Internet betting scams, fraud and blackmail via social networking sites. A new breed of intelligent offenders is emerging who are quick to seize new criminal opportunities.

In Ankara, a cadre of five specialist prosecutors deals with approximately 4000 cybercrimes per year. This number includes "traditional" crimes committed using some form of electronic communication in the commission of the offence. These "traditional" crimes include, blackmail and other crimes involving "threats".

Other large cities also have specialist prosecutors.

A particular problem highlighted during the assessment was the need to prosecute offences that are contrary to Turkish law but there are not necessarily offences in other jurisdictions.

8.2 Legislation

8.2.1 The situation at the outset

Turkey signed the Budapest Convention on 10 November 2010 and did not yet ratify it. Turkey did not yet sign the Additional Protocol. During the implementation of the project on 7 December 2011, Turkey ratified the Convention on the Protection of Children against sexual Exploitation and Sexual Abuse.

8.2.2 Assessment and summary of progress made

Although Turkey has not (yet) ratified the Convention and its Additional Protocol, the Criminal Code already contains several provisions that can be applied in case of cybercrimes. Article 9 (Offences related to child pornography) is part of a much broader concept of obscenity under Turkish law. Provisions related to Article 16-18 of the Convention are as such not implemented although some parts may be covered. Turkey maintains a system of data retention as defined under the European Directive.

In Turkey a draft act on information security has been prepared in view of ratification of the Convention. The Bill on ratification of the Budapest Convention was adopted in the Foreign Affairs Commission of the Grand National Assembly of Turkey on 19 December 2012. It is expected that the Bill will be on the agenda of the General Assembly in the forthcoming months. Moreover, work on the amendments to the legislation to implement the Convention is being undertaken by a working group of the Ministry of Justice.

The Draft Bill on the Protection of Personal Data was prepared by the Ministry of Justice and sent to the Prime Ministry. It is expected that the Bill will be submitted to the Grand National Assembly of Turkey shortly.

The Bill on the principles and procedures concerning the freezing the assets for the fight against finance of terrorism and governing the offence of financing of terrorism was approved in the Grand National Assembly of Turkey on 7 February 2013.

8.2.3 Recommendations

- Adopt legislation in line with the Budapest Convention
- Ratify the Convention on Cybercrime and its Additional Protocol as a matter of urgency
- Consider the gaps identified in the Discussion paper "Protecting children against sexual violence: The criminal law benchmarks of the Budapest and Lanzarote Conventions".

8.3 Specialised institutions

8.3.1 The situation at the outset

Turkey is composed of 81 provinces and 921 districts under the authority of these provinces. Throughout Turkey, the Minister of Interior, in provinces the Governors and in districts district-governors are responsible for providing security and public order. The Minister of Interior performs this duty through the Gendarmerie General Command, General Directorate of National Police and Coast Guard Command. In principal, the Police are responsible for security and public order within the municipal borders of provinces as well as districts and the Gendarmerie is responsible for the areas out of the municipal borders.

In the Gendarmerie General Command Headquarters, there is an Anti-Smuggling and Organized Crimes (ASOC) Department within the Operations Division. There are ASOC Section Chief Offices under the subordination of Operations-Public Security Branch Offices in 14 Gendarmerie Regional Commands Turkey-wide. In accordance with population, geographical characteristics and the density of smuggling incidents there are ASOC Branch Offices in 57 Provincial Gendarmerie Commands. There are ASOC Section Chief Offices subordinated to Public Order Branch Offices in 24 Provincial Gendarmerie Commands. These units carry out the tasks of detecting, preventing and investigating smuggling and organized crimes (Financial and cybercrime are included).

A Cybercrime Branch Office and Cybercrime Tracking and a Technical Support Team exist within the structure of Turkish Gendarmerie General Command ASOC Department and there are also Cybercrimes Section Chief Offices within the structure of ASOC Branch Offices in 5 Provincial Gendarmerie Commands where cybercrime incidents are prevalent. It is planned that cybercrimes units in 81 Provincial Gendarmerie Commands will be created before 2014.

Digital evidence detected in crime scenes is dealt with by trained personnel who have the necessary software and hardware upon an order of the judge in accordance with the Turkish Criminal Procedure Code. Staff in these units have also been trained and equipped to carry out these functions.

Forensic laboratories prepare expert reports after completing the investigation of digital evidence. The staff of these laboratories is entitled to give expert reports (Gendarmerie Forensic Laboratory, Police Forensic Laboratory and Forensic Medicine Institution, Specialized Cybercrime and Technology Branch). Staff from the laboratories also received appropriate training and has the relevant equipment.

According to the Turkish Criminal Code, public prosecutors are responsible for conducting all investigations. They carry out these investigations through judicial law enforcement units such as the KOM cybercrime unit, who handle these investigations in response to instructions from the prosecutor assigned to the case. There are public prosecutors specialising in cybercrime cases in the major cities: Ankara, Istanbul, Izmir etc. In addition the prosecutors have the UYAP (National Judiciary Informatics System), which includes public prosecutors in all major courthouses in Turkey.

In addition to the cybercrime units mentioned above, there also exists a special institution called TÜBİTAK. This institution is responsible with cyber security matters rather than digital evidence and cybercrime.

The KOM department has 15 regional digital forensic laboratories in other districts and 1 digital forensic laboratory in the central office in Ankara. Every district is connected to a regional forensic laboratory; digital evidence is sent to these connected laboratories for analysis to be conducted on the evidence.

The Turkish National Police with its KOM/Cybercrime central unit has 20 staff members and the 81 provincial divisions have approximately 250 staff members in total.

Issues identified by the Turkish Police included the rapid changes in technology and its effect on cybercrime methods and trends. The number of the well-qualified staff with a good background in computers and other digital devices is limited. Due to the structure of the Internet, international cooperation has a very important place in cybercrime investigations; however, the actual level of cooperation may be limited.

8.3.2 Assessment and summary of progress made

In July 2011, the Government decided to set up a new cybercrime department within the Turkish National Police. This means that cybercrime is considered now to be at a higher level and at the same level with organised crime. This new department has the authority to investigate cybercrime and related crimes, including child pornography. It is envisaged that this department will investigate all crimes where ICT is either target or tool for committing the crime. At the time of reform the "Specialised cybercrime units, Good Practice Study" was available and its recommendations were considered by the project team (some of them directly involved in its drafting as well as in the reorganisation).

The National Cybercrime HQ is established in Ankara. The building houses 104 staff including forensic, analytical and investigative staff. The department Commander is the national policy owner and acts as "Head of Profession" for all cybercrime matters.

This central unit deals with the more specialised technical aspects as well as offering support and guidance to any other law enforcement or Ministry. They are also the informal 24/7 contact point for Law Enforcement Agencies.

In addition to this central unit, there are 81 satellite units as well as 17 regional computer forensic laboratories. All of these cybercrime Sub Divisions are capable of live crime scene activities including seizures. Examinations and analysis is carried out in the forensic laboratories by trained, accredited staff only.

In total there are 900 cybercrime investigators, however the department is working towards increasing this number to 1500 in the near future.

The forensic technicians are trained to a high standard, have excellent facilities and are well equipped. The investigators and analysts have access to a wide range of analytical software and have extensive operational experience. Most of the staff working within the department have been "head hunted" and as a result, include some of the brightest and talented staff available.
Co-locating, Investigators, Analysts and Forensic staff has improved communication and as a result cases are appropriately prioritised and are also processed quickly. The forensic backlog was estimated to be two months.

All cybercrime staff have access to a secure intranet (Polnet) which affords varying levels of access to more than 60,000 staff nationally.

Headline Cybercrime statistics show that between July and September 2012, there were more than 2706 reported cases nationally. The recent trends indicated a shift toward, "on line" banking fraud, infecting mobile phones and hijacking email accounts as a precursor to fraudulent activity. A new crime typology was the discovery of a website offering payment for organ donations. Selling body organs is a crime in Turkey.

There are a number of emerging issues, which may require further discussion at future conferences: cloud computing and corporate responsibility.

The Scientific and Technological Research Council of Turkey (TUBITAK) is a scientific institute funded by the Government. It has technical awareness of the communications industry and developing threats and thus ideally positioned to inform CERT.

Turkeys Telecommunications Directorate (TIB) is responsible for industry regulation and direct conduit to the ISPs. A member of the Cybercrime Department of the Turkish National Police (TNP) has been nominated as a liaison officer and is currently housed in the TIB. All court orders including authorisations for "live interceptions" must be processed via TIB.

There is established a specialist Cadre of Prosecutors responsible for prosecuting all reported cybercrime cases within its jurisdiction. In addition, they provide advice and guidance to other regional Prosecutors when requested. The vast majority of offences prosecuted involve forged credit cards manufactured abroad. In addition, attacks on personal bank accounts have been also experienced.

A national Case-file support system that records all cases and court results is available. It is possible for analysts to extract statistics which is done periodically.
In the total number of 4000 cases there are crimes such as making threats over the internet, internet banking scams, social networking abuse of data, and blackmail.

The cybercrime prosecutors have highlighted a number of specific challenges:

- Obtaining digital evidence within an effective investigative timeframe.
- Digital Evidence Stored should be established within the Court Building
- Specialised Office Assistant, prosecutors and judges should be responsible for cybercrime prosecution and adjudication. Apart from Office assistant, there should exist electronic an engineer expert working within Prosecution unit.
- 24/7 Point of Contact should be established within the Central Authority, prosecution, polis, Internet Service Provider etc.
- ISPs should be obliged to establish representative in Turkey.
- Legislation amendments to Turkish Penal and Procedural Code should be made.
- ISP records should be retained for a minimum of 12 months and telecommunication records 18 months.
- Requests made to foreign ISPs are slowly. Some responses signpost another foreign ISP and retention time limits can expire.
- There is an initiative with banks to ensure that images are recorded of all ATM transactions.
- The quality of some images is poor.
- Facial recognition software is ineffective. Either due to image quality, camera angle and foreign offenders.
- Banks are obliged to retain images for 30 days. Prosecutors would like this extended to 90 days.
- Problems encountered with log files and multi user systems (Internet cafés).

Under Turkish law any prosecutor may require assistance from any government department and they must comply or respond within 10 days or face sanctions.

Court warrants for search and seizure can be obtained within 24 hours and served on an ISP within 8 to 10 hours.

A National Cyber Security Council has been established. It includes senior representatives from the following institutions or ministries: Transport and Communications; Foreign Affairs; Defense; Telecommunications; Maritime; Military; Financial Intelligence Unit.

This group has been tasked with creating a policy on the national cybercrime threat and in particular, the defence of key strategic assets and raising public awareness.

A tactical sub group has also been established. Monthly meetings are held with representatives from a number of institutions including: Ministry of Justice; Court of Appeal; Judicial Academy; National Police; Information Technology Institute; High Council of Judges and Prosecutors. The terms of reference of this group include problem solving, identifying emerging threats and any associated training needs or tactical response needs.

8.4 International cooperation

8.4.1 The situation at the outset

Turkey under its law can access computer data stored abroad through mutual legal assistance (MLA). It would be possible to request such data within the framework of Mutual Legal Assistance provided that the principle of reciprocity is maintained.

The General Directorate for International Law and Foreign Relations within the Ministry of Justice is the central authority for the execution of all judicial assistance requests in criminal matters. Local judicial authorities prepare a case file with the judicial request, with translations, and send them to the responsible department. The international judicial cooperation in criminal matters is usually provided within bilateral agreements concluded between Turkey and other countries as well as multilateral agreements to which Turkey is a party. If there is no bilateral or multilateral convention judicial cooperation in criminal matters is governed by international customs and principle of reciprocity.

No domestic laws had been adopted to allow expedited or other mutual assistance for accessing stored computer data as proscribed by Article 31 of the Budapest Convention.

Cooperation with foreign police authorities was conducted according to bilateral agreements or via international organisations like Interpol. Police to police cooperation is possible for the exchange information, as well as cooperation in joint teams and to make parallel investigations within the limits of the relevant agreements.

The main obstacles identified by Turkey were the speed of the transfer of information between jurisdictions and lack of data storage obligations in Turkey and other countries.

In order to enhance the effectiveness of the Turkish Gendarmerie General Command on combating against forgery and fraud in the credit card payment system and in accordance with a protocol signed with Interbank Card Centre (BKM), one officer was assigned to the Istanbul Provincial Gendarmerie Command undertaking a course at the BKM with the purpose of providing coordination in clarifying these crimes.

8.4.2 Assessment and summary of progress made

The Ministry of Justice is the central authority responsible for all requests made or received for international assistance. It is also the 24/7 contact point. Requests through email will be accepted to initiate immediate preservation requests but rogatory letters are required in order to freeze and seize obtain evidence.

The Police maintain a 24/7 contact point for police to police contact which can also pre-warn of a formal MOJ to MOJ request.

All requests received are first assessed before they are passed to the correct Ministry for action. There are some issues of "dual criminality" when requests are made for evidence from another jurisdiction when that jurisdiction does not recognise the act in question as a crime e.g. insults or defamations on Facebook are not recognised as crimes in the USA but they are in Turkey.

The MOJ has established a contact point and a liaison officer exclusively dealing with the USA. This was considered as a necessity due to the key role and influence the USA has in coordinating international activities, particularly in respect of Facebook and Google.

There is a bilateral agreement with the USA but about 60% of requests are rejected as they fail to exceed the threshold deemed, serious. More than 400 requests have been made so far this year to the USA for assistance.

In order to assist the process of MLA, the MOJ has published good practice guides together with Formal Application formats on the MOJ web site. These are open source assets available to all.

Some statistics were available but not very detailed.

Turkey has a great deal of experience in dealing with international requests for assistance and has worked hard to overcome obstacles encountered in the investigation. It has concluded bilateral arrangements with countries and organisations that are important to their investigations.

8.5 Law enforcement training

8.5.1 The situation at the outset

The Turkish National Police Academy was the institution responsible for the education of police officers and police superiors. The Training Department was responsible for in-service training of police forces in general. The Anti-Smuggling and Organized Crime Department has also a training academy; the Turkish International Academy against Drugs and Organized Crime (TADOC). This academy provided in-service training for the Department's staff in the context of its responsibilities, including cybercrime and digital forensics training. Lecturers from the central and regional cybercrime units support this training.

There were several types of cybercrime and digital forensics training provided by these institutions but there was not a documented training strategy for law enforcement officers covering the areas of cybercrime.

The staff dealing with digital forensics have "basic" and "advanced" digital forensics training, which is given by Cybercrime Unit experts. Two members of staff were studying for an MSc in Forensic Computing and Cybercrime Investigation, an opportunity provided by the EC funded ISEC 2008 cybercrime investigation training project.

In principle, new LE recruits were taught how to recognise and deal with electronic devices that may contain evidence. There was a lesson on criminalistics in the Police Academy and Police Vocational Colleges to teach all the subjects related to evidence and crime scenes. All police officers and police superiors learnt general information about digital evidence including how to collect it.

Within the 2 week basic course for law enforcement officers to work in the Organised Crime Department and its provincial divisions, there was a half-day lesson "Open source research and using internet in investigations."

A twinning project was planned to improve the investigation capacity of Turkish National Police and Gendarmerie. It is planned to use ECTEG modules in the training programme. Within this project training will be provided by the North Rhine-Westphalia State Criminal Police from Germany.

Within the scope of on-site training activities, training on "Combating Cyber Crimes and International Law Enforcement Cooperation" was provided to 1800 personnel between 2008 and 2010.

Furthermore, in order to train specialist personnel in areas that require special expertise, personnel are given training on "Core Skills in Network Investigation", "Researching, Identifying and Tracing the Electronic Suspect" courses organised by the National Policing Improvement Agency-UK (NPIA). In addition staff receive training in "Encase Computer Forensics I and II", "Encase Advanced Internet Examinations", "EnCase Advanced Computer Forensics", "EnCase Network Intrusion Investigations" and "EnCase Examination of NTFS" courses organised by Guidance Software-UK.

8.5.2 Assessment and summary of progress made

There is a comprehensive Training Strategy document, which details an extensive programme of training activity for a variety of roles for new and existing Officers. Modules are currently being delivered to:

- New Recruits
- First Responders
- Cybercrime Response Teams (On scene specialists)
- Other Cybercrime specialists
- Advanced training
- Forensic Training.

In addition, there is an in house accreditation process for all cybercrime practitioners before they are allowed to practice a variety of roles and functions.

The Cybercrime Unit provides trainers to a wide range of criminal justice and law enforcement institutions.

Under CyberCrime@IPA law enforcement officers, judges and prosecutors were trained on the need to ensure the rule of law and human rights principles (Article 15 of the Convention on cybercrime - Safeguards and conditions). One representative from Turkey (Chief Computer Forensics Laboratory, Cyber Crimes and Systems Unit, Istanbul Police Directorate) was funded to participate in the Master of Sciences (MSc) programme in Forensic Computing and Cybercrime Investigation offered by UCD.

Law enforcement and prosecution services from Turkey participated in the training on interception of traffic and content data for law enforcement purposes, including legal, procedural and technical considerations and based on good practices. Other activities organised or funded by the project provided training for law enforcement (e.g. G8 Training, Octopus Conferences and the Cybercrime Convention Committee (T-CY) etc.).

The sheer scale of the cybercrime training requirement for Turkey is daunting. At the training meeting in Dublin it was reported that the TNP plans to have 1100 operatives in need of specialised training along with a further 800 from the Gendarmerie. Turkey has been the recipient of a number of internationally funded projects, including CyberCrime@IPA.

Coordination between these activities needs to be ensured to allow for a better return on the investment. TNP has an excellent programme of training and other project areas could benefit from examining their approach, ensuring that any outcome is scaled to the needs of the other areas.

Turkey should consider establishing joint programmes with academia that will allow for qualifications to be obtained by staff. This suggestion recognises that it will never be possible to satisfy the demand for places on international programmes.

8.6 Judicial training

8.6.1 The situation at the outset

The Justice Academy of Turkey was responsible to provide training for judges and prosecutors. The mandate of the Academy covers both initial and in-service training. There was no documented cybercrime training strategy for judges and prosecutors.

Judges and prosecutors were trained on these subject matter topics separately. Initial training for prosecutors, includes a lecture on the final stage of the initial training entitled "Prosecution of Cybercrimes".

Judges and prosecutors received training on cybercrime and digital evidence in their initial training.

Since 15 October 2007, 17 training programme have been organised. Each course was four days long and the training was for 4 hours each day. The subject matters were:

- Analysing methods of cybercrimes
- Digital evidence
- Recent developments in the field of cybercrime
- Obtaining evidence via IT systems

It was recognised that some judges and prosecutors require more advanced training. Arrangements to garner assistance to assist in the development and delivery of training were limited to assistance provided by experts of law enforcement units. Furthermore, the level of training was not sufficient. It was seen as beneficial study visits and workshops for judges and prosecutors organised with other jurisdictions and with law enforcement in Turkey in order to improve their knowledge.

8.6.2 Assessment and summary of progress made

There are currently 12,500 judges and prosecutors in Turkey and it is intended to train a further 3000.

The preferred method of training existing judges is through seminars. So far two seminars on IT law have been held and another was planned for December 2013 and will include 200 judges and prosecutors.

Two representatives from Turkey (Judge-Deputy of General Secretary, Supreme Court and Judge-Head of a Department Directorate General of Foreign Affairs and International Law) participated in the regional train the trainer course organised under CyberCrime@IPA. The basic course organised under the project in cooperation with the Turkish Justice Academy in Ankara, which facilitated the organisation and logistical aspects, provided training for 27 delegates. A second module (advanced course) was organised on 1-2 November 2012 in Ankara by the project and trained 24 prosecutors and judges in cooperation with the Turkish Justice Academy and International Law and Foreign Affairs Department.

In 2012, approximately 850 judges and prosecutors candidates were trained and 1000 new candidates will be trained in 2013.

A formal training strategy is currently being drafted. In service training is mandatory and judges and prosecutors are required to attend regular training events throughout a legal career.

It is intended to establish a Centre for Cybercrimes under the umbrella of the Turkish Justice Academy.

A cybercrime training module has been prepared that will be delivered in 2013. There are plans to train 200 judges and prosecutors who will get 10 days training (68 hours). Senior judges, law enforcement officers and foreign experts will deliver this training.

Initial training of Judges and Prosecutors includes 20 hours on cybercrime and electronic evidence. There is a separate curriculum dealing with Intellectual Property Rights where 8 hours of training is given. Investigation techniques for cybercrime is taught as a module (12 hours) for the candidates by law enforcement officials. Investigation and prosecution phases for cybercrime is also another module for the candidates in the final stage of the candidateship term delivered by senior judges particularly from the Court of Cassation.

Internship programmes ensured that trainee judges and prosecutors received workplace training with specialists including Cybercrime Prosecutors, who are used as trainers by the judicial academy.

The training for judges and prosecutors in Turkey is well established and there are clear plans to deliver training to the large number of prosecutors.

It was apparent during the in country and "advanced" training organised under the CyberCrime@IPA project that there is cybercrime experience, although some concern remain about the understanding of how the law enforcement community handles electronic evidence.

8.7 LEA/ISP cooperation

8.7.1 The situation at the outset

There are 115 licensed ISPs in Turkey[34]. The Information and Communication Technologies Authority is the responsible organisation for licensing of ISPs.

The main problem identified in obtaining information from ISPs in Turkey is the speed of processing requests. A request for data requires authorisation from the prosecution service.

There was no standard request documentation to obtain traffic, subscriber or content data. During an investigation, if data from an ISP is needed, law enforcement officers applied to prosecution service with an official letter. Then prosecutor decided if the request should be converted into a request to the ISP.

There were no specific contact points within law enforcement or ISPs through which communications are made. It was intended that written procedures for dealing with ISPs to be developed within the twinning project currently underway.

8.7.2 Assessment and summary of progress made

During an investigation, if data from an ISP is needed, law enforcement officers send an official letter to the prosecution service. The prosecutor decides whether the request should be send to the ISP. If so, they prepare an official letter to the ISP requiring them to comply with the request of law enforcement. All requests from law enforcement relating to users of IP addresses are made through the prosecutor. For the content of the log files LEA need a court order to get information from the ISP.

[34] http://www.tk.gov.tr/doc/lisans/ISS_bildirim_giris.htm

In Turkey ISPs retain data for a minimum 6 months up to 2 years. Backdated collection of data can be done for up to three months. Some ISPs retain data for 12 months or more.

Cooperation with ISPs Cooperation is vital. It is recognised that 24/7 contact points and single points of contact (SPOC) will increase efficiency.

Currently, Turkey is working with Germany in a twining project that will discuss the possibility of an MOU on cooperation between LEA and ISPs. Turkey already has some memorandums of understanding with private companies providing telecommunications services in the country but not with ISPs.

LEA in Turkey has meetings and takes part in working groups not only with the ISPs but also with companies such as Microsoft, Siemens, Telephone Companies, ISPs etc. The meetings are attended by representatives of the Judiciary and Police from the government side.

8.8 Financial investigations

8.8.1 The situation at the outset

The main types of crimes involving the Internet and crime proceeds identified were payment and credit card fraud, Internet banking fraud and frauds committed by using advertisements. The main challenges to prevent and identify criminal money flows on the Internet were: the tracing of the proceeds, especially if broken down into small quantities. Cooperation from banks and other financial institutions are necessary to combat this type of activity.

The Law No. 5549 on Prevention of Laundering Proceeds of Crime, which was drawn up considering international standards in combating laundering proceeds of crime, entered into force on 18 October 2006.

In order to combat laundering proceeds of crime in a more effective way and prevent the use of financial system by criminals, certain obligations for financial institutions and some other professional organizations have been introduced in both international area and domestic law. The Law 5549 requires banks, other financial institutions and some other professional organizations dealing with assets to report suspicious financial transactions to the Financial Crimes Investigation Board/Ministry of Finance (MASAK) Investigation.

Within this scope, those who operate in the field of banking, insurance, individual pension, capital markets, money lending and other financial services, and postal service and transportation, lotteries and bets; those who deal with exchange, real estate, precious stones and metals, jewelry, all kinds of transportation vehicles, construction machines, historical artifacts, art works, antiques or intermediaries in these operations; notaries, sports clubs have been set, by the Article 2/d of the Prevention of Laundering Proceeds of Crime Law No. 5549, as obliged parties in the implementation of Law No. 5549, and the Council of Ministers have been authorized for enabling the imposition of obligations to business owners and professionals not listed above.

In accordance with the general rules that apply to financial investigations, prosecutors are in charge of investigations supported by law enforcement. If a suspicious transaction is identified during an investigation, a request is made of MASAK to collect and analyse data relevant to the transaction and provide a report to the prosecution service.

Additionally, MASAK should collect financial intelligence, analyze deeply the financial profile and other situations of individuals or entities linked with crimes and compare them with other available data; share any important conclusions and findings in terms of AML/CFT with national and international counterparts and related units. If required the report send to the prosecutors.

The following organisations are involved in investigations on criminal money flows on the Internet: MASAK and obliged institutions such as banks, ISPs, the Interbank Card Centre (BKM), the Credit Bureau of Turkey (KKM).

8.8.2 Assessment and summary of progress made

The Financial İntelligence Unit, the MASAK, is participating in the Financial Action Task Force established to promote effective implementation of legal regulatory and operational measures for combating money laundering and the financing of terrorism.

Evaluation and examination of ML and TF offence and supervision of AML/CFT obligations have been performed by examiners on behalf of MASAK and MASAK experts. MASAK has been carrying out its activities under cooperation and coordination with law enforcement authorities, intelligence units, financial and non-financial private and public sector institutions. Furthermore, MASAK has provided online access to various public institutions and organizations and financial institutions.

MASAK developed a relational database and strengthened its data structure by having access to the databases of many external institutions. Based on this system, many channels of information flow were diverted into the electronic environment. Moreover, through data analysis software acquired by this system, MASAK has achieved the capacity to effectively and quickly analyze obtained data. STRs received from banks and the abstracts of accounts have been standardized. The system is mainly focused on systematization of MASAK's data structure and electronic information flow within the scope of fight against ML and TF.

Within the framework of recent developments in information and communication technologies, the opportunity of collecting, storage, processing, transmission, reporting, analyzing of information is also rapidly increasing. Although information system strategies are designed to cover a long term, the current software is constantly updated and many new hardware and software are introduced into the market. Current information systems should also be analyzed, updated and improved periodically due to the needs of the institution and the ongoing rapid changes in the information systems.

Standardized STRs and extracts of accounts have been received electronically from the banks. By extending this system to other obliged parties will make the system more effective. For this reason new project is planned and approved by related authorities. Concerning the potential increase in the number of these obliged parties to more than 150.000 and their insufficient technical infrastructure, by developing a light-weight communication mechanism, this project will enable these parties to report STRs through a secure on-line system.

For the strengthening cooperation between MASAK, law enforcement authorities and judiciary, MASAK has been carrying out trainings and workshops. In order to enhance this cooperation, training or workshops on financial investigations including typologies, case studies and trends still have been organized.

It is considered by law enforcement that the current legislation is inadequate as Turkish law requires the police to prove a direct connection between particular crimes and assets under consideration.

The ability of the authorities to combat this type of activity is hampered by the fact that there is no legal basis for confiscation of proved criminal assets by way of lifestyle as opposed to connection with specific offences. The nature of this type of crime means that this will continue to hamper investigations until resolved.

8.9 Progress made against previous recommendations

Cybercrime situation report March 2011	Progress reported
Keeping statistics that provide an insight in the seriousness of cybercrime in the national territory. Such statistics could for example 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
Consider amendment of the Criminal Code and Criminal Procedure Code in view of the observations made, in particular in those areas where the obligations of the Budapest Convention has not yet been met	Work in Progress
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.	Completed
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. Strategy being drafted.
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 the Global Project on Cybercrime.	Partially completed
Improve capability to combat illegal money flows on the Internet by working on the adoption of the relevant findings of the Council of Europe study "Criminal money flows on the Internet: methods, trends and multi-stakeholder counteraction".	
Examine existing good practice in the handling of electronic evidence in criminal investigations, such as guidelines developed by Interpol and Europol, to ensure that Turkey's procedures are capable of international acceptance in investigations.	Work in Progress
Engage with national and 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
Recommendations made by second progress report 1/11/11 – 31/5/12	
Challenge Government to speed up the ratification process of the Budapest Convention.	Partially Completed
Harmonisation of legislation according to the Convention.	Work in Progress
Upgrade and use an alternative standard form to provide a MLAT on cybercrime cases exclusively.	Completed
Training of judges and prosecutors on using judicial assistance instruments effectively in cybercrime matters, especially focus on handling of electronic evidence in criminal investigation	Partially Completed
Set up periodical meetings with TR-CERT, with participation of relevant agencies to envision new threats and analyse how to react properly against crimes currently occurring.	Completed

Step up cooperation and communication between public and private stakeholders in the fight against cybercrime Turkish Law Enforcement Agencies meet with Banking Regulation and Supervision Agency of Turkey, and National Information Technology Association (regulating GSM operators" actions) few times per year to discuss misuses in communication and online/traditional banking system after analysing cybercrime typologies. In addition, law enforcement agencies join Banker's Association of Turkey when requested. Such meetings and platforms could be expanded with the participant of judicial authorities, MASAK (Turkish FIU) and revised as to be held periodically as Cyber Consultative Forum proposed in Belgrade meeting.	Completed Since 2008 TNP organises periodical meetings with Banking Regulation (BDDK) and since 2006 with Banker's Association when an agreement was also concluded.
Improve interagency cooperation we propose to create a platform gathering public stakeholders such as, Law enforcement agencies, Judicial agencies, and MASAK (Turkish FIU). In order to reify such a platform it is vital to create a working group to prepare a technical report explaining related Turkish authorities why there is need, and recommending what actions should be taken, how to organize and design a taskforce team to run actions of such a platform.	Work in Progress
Establish a [collective] 24/7 Point of Contact consisting of representatives of the prosecution, law enforcement, ISPs and the Interbank Card Centre (BKM).	Work in Progress

8.10 New recommendations

1. Formalise relationships with ISPs.

2. Turkey should consider establishing joint programmes with academia that will allow for qualifications to be obtained by staff.

3. Serious consideration should be given to establishing a national centre of excellence in cybercrime training, research and education to support the needs of the law enforcement community.

9 Kosovo*

9.1 Cybercrime and the criminal justice system

9.1.1 The situation at the outset

In Kosovo* there was no cybercrime department or sector established. The Financial Investigation Unit of the State Police (Organised Crime) investigated a number of credit card frauds.

9.1.2 Assessment and summary of progress made

Kosovo* reported the main offences as those of credit card theft, ATM deception and forgery of credit cards. They were also experiencing incidents of:

- Illegal access
- Interference with data
- Denial of service
- Theft of data from ISPs
- Hackers
- Skimmers
- A few low level cases involving Facebook and Twitter

Individual cases were not recorded i and thus no statistical information was readily available but had to be produced manually.

9.2 Legislation

9.2.1 The situation at the outset

The Law on Preventing and Combating Cybercrime (nr. 03/L-66) was drafted in cooperation with the Ministry of Justice and the Ministry of Transport and Communication, assisted by experts from the Council of Europe. It entered into force in July 2010. Previously the Criminal Code contained only two traditional provisions that could be applied in the field of cybercrime (Article 168 and 264).

The new law is based upon the definitions and structure of the Budapest Convention.

9.2.2 Assessment and summary of progress made

The legislation in Kosovo* is to a large extent compliant with the Budapest Convention. A new Criminal Code and new Criminal Procedure Code entered into force on 1 January 2013.

Overlapping provisions and some gaps identified in the Situation Report could be solved by future amendments and once there is more practical experience in Kosovo* in investigating and prosecuting cybercrimes.

The main challenge for Kosovo* remains international cooperation.

9.2.3 Recommendation

- Consider the observations made in the Situation Report in view of possible amendments, including the enactment of specific offences concerning aggravating circumstances or the protection of specific interests. Some provisions of the Budapest Convention have not been implemented yet.

- Specific attention is to be paid to the legal concept of seizure of computer data and the possible need for expedited execution of investigative powers.

9.3 Specialised institutions

9.3.1 The situation at the outset

There was no operative specialised department in the police or prosecution service dealing with cybercrime. Structural changes in the Kosovo* Police envisaged the establishment of the Sector against Cybercrime as part of the Directorate against Organized Crime. This sector was not operational and police officers were not recruited. The investigation of cybercrime or traditional crimes involving technology was not assigned.

The Sector of Forensics and Information Technology conducted digital forensics activities and dealt only with cases received from other departments.

Standards adopted for handling of digital evidence were based on those that relate to licensed computer forensics programmes and cover examination of digital devices and not the recovery of evidence from the Internet.

The Forensics and Information Technology Sector had 2 members of staff trained in computer forensics. This sector used hardware devices and computer programmes designed and licensed for digital forensics for computer and mobile phone forensics.

9.3.2 Assessment and summary of progress made

The Cybercrime Investigation Unit in Kosovo was established in June 2011 and is responsible for the investigation of offences committed against computer systems and data, as well as those committed by means of computer systems. The unit bases its activities on the law on cybercrime, while the internal regulations and the SOP (Standard Operating Procedures) are currently being developed. It is comprised of 7 staff and there are aspirations for this to increase to 8 or 9 members. The 24/7 responsibilities, currently, resides informally with the Computer Crime Unit.

Currently there are 4 investigators and there are concerns that such a small number will not provide sufficient operational resilience. There is a belief that some cybercrime capability will need to be deployed to some outlying locations in order to best service demand.

Digital forensics activities are conducted by the Computer Examination Laboratory, Kosovo Agency for ForensicStandards adopted for the handling of digital evidence are based on those that relate to licensed computer forensics programmes and cover examination of digital devices and not the recovery of evidence from the Internet.

Judicial institutions are undergoing reformation and significant changes are expected. A Unit for serious crimes will operate within the State Prosecutors Office. These organisational changes are delaying progress on delivering previous recommendations.

Statistics for prosecutions were not readily available but could be manually produced, with notice. Most of the reported cases of cybercrime were simply demands or threats made electronically. There were also cases of illegal access and interference as well as ID thefts. These were however marginal numbers compared with the overall crime profile.

The creation of a cybercrime unit is a welcome development since the beginning of the project. It is clear that Kosovo* is in need of further assistance to make this an effective unit, by way of

improving the knowledge and skills of the unit and the identification and acquisition of suitable equipment.

9.4 International cooperation

9.4.1 The situation at the outset

International co-operation is possible on the basis of Criminal Procedure Code and the powers defined in domestic law.

The central authority for international legal assistance is the Division for International Legal Cooperation (DILC) of the Ministry of Justice. All communications with foreign jurisdictions on mutual legal assistance are processed through embassies accredited in that country and embassies of foreign countries accredited in Kosovo

The main difficulties encountered in relation to international legal cooperation are because Kosovo* is not Party to Council of Europe conventions, e.g. Convention on Cybercrime and the Convention for Protection of Individuals with regard to automatic processing of personal data. Therefore, communication is based on the principle of reciprocity and is limited.

9.4.2 Assessment and summary of progress made

International co-operation is possible on the basis of Law No. 04/L-031 on International legal cooperation in criminal matters.

Considering the need and demand for capacity building in the field of international legal cooperation, as well as adapting to the increasing demands for international legal assistance, in 2011, the Ministry of Justice has established a Department of International Legal Cooperation (DILC) instead of a Division, which is the central authority for international legal assistance.

It was intended to demonstrate the Government's commitment to fight against organized crime by concluding bilateral agreements on judicial cooperation with various countries, which would allow Kosovo* to meet its international obligations and ensure the rule of law.

All communications with foreign jurisdictions on mutual legal assistance are processed through the Ministry of Foreign Affairs. There are two exceptions to this practice. Kosovo* has direct communication with the Ministries of Justice of some countries (Austria, "The former Yugoslav Republic of Macedonia", Croatia, Montenegro and Albania) while with the countries that do not recognise Kosovo* the communication is made through European Union Rule of Law Mission in Kosovo*.

In urgent cases communication is conducted through the Interpol Liaison Office in Pristina and with direct communication between the Ministries of Justice. DILC has held regular meetings with the Interpol Liaison Office in Pristina. The purpose of these meetings is to address threats posed by organized crime, in particular the capture of wanted persons and the exchange of information regarding cases being processed by DILC. These meetings have directly resulted in a number of major criminals being arrested or extradited.

There are a number of regional agreements between Kosovo* and countries from the region (e.g. "The former Yugoslav Republic of Macedonia'', Croatia, Albania, Turkey) on extradition; mutual legal assistance in criminal matters, transfer of sentenced persons etc.

All communications with Serbia and Bosnia and Herzegovina are conducted on the basis of the technical agreement between the Republic of Kosovo* and the European Union Rule of Law Mission in Kosovo.

A number of other agreements are in the process of negotiation, including with EU Member States.

Over the past two years (2011 to 2012), the Department for International Legal Cooperation, this Department has received and processed a total of 15.288 requests and responses regarding the on-going and new cases.

The main difficulties encountered in relation to international legal cooperation are caused by the reason that Kosovo* is not Party to the Council of Europe conventions e.g. Convention on mutual legal assistance, Cybercrime Convention and the Convention for Protection of Individuals with regard to automatic processing of personal data. Hence, communication is limited given that it is based on the principle of reciprocity.

9.5 Law enforcement training

9.5.1 The situation at the outset

The Kosovo* Centre for Public Safety, Education and Development (KCPSED) was founded in January 2006. On 26 March 2008, by the entry into force of UNMIK Administrative Regulation No. 2008/3, the Centre for the Public Safety, Education and Development functions as an executive agency of the Ministry of Internal Affairs. KCPSED is responsible for ensuring professional standards in education and training provided to members of public safety agencies.

As a result of resources and its environment the Centre has become the primary training provider for a wide range of public safety and enforcement branch training. During 2010 KCPSED trained by 12,000 to 13,000 security officers in basic training, advanced and specialised.

Kosovo* did not have a cybercrime training strategy as part of its education and training programme, nor a training facility responsible for delivering cybercrime investigation or digital forensics training. No academic or professional qualifications were available to LE staff in this subject area. Kosovo* did not have any specific training courses in the subject areas but has benefited from training courses dealing with economic crime organized by OSCE and the EU European Agency for Reconstruction (EU-EAR). Some of these courses had elements relating to cybercrime.

New recruits to law enforcement did not receive training within their programme to provide them with the skills and knowledge to recognise and deal with electronic devices that may contain evidence in relation to any crime, including traditional crime.

KCSPED recognised that combating cybercrime was a priority; however providing education and training did not progress as a result of a lack of support tools and professional staff in the relevant field.

9.5.2 Assessment and summary of progress made

The Police Academy has a mandate to deliver basic training and more recently, higher education training to Law Enforcement Officers. The Kosovo* Academy delivers over 100 different types of training but none relate to cybercrime.

Cybercrime and electronic evidence are still not included in any basic training delivered to the wider law enforcement community.

CyberCrime@IPA provided several trainings for investigators on different topics in which Kosovo* participated. One representative from Kosovo* was funded to participated in the Master of Sciences (MSc) programme in Forensic Computing and Cybercrime Investigation offered by UCD. His current position is Chief of Computer Examination Laboratory, Agency on Forensics, Ministry of Internal Affairs. In his current position he is supporting law enforcement agencies in Kosovo related to computer forensics, electronic evidence and cybercrime investigators related to computer forensic examinations.

9.6 Judicial training

9.6.1 The situation at the outset

The Kosovo* Judicial Institute (KJI) is the main institution responsible for in-service training of judges and prosecutors through the Continuous Training Programme (CTR). It also offers training to candidates aspiring to become judges or prosecutors through the Initial Training Programme, as well as specific courses for professional advancement. In addition, a number of international organizations offer trainings for judges and prosecutors in cooperation with KJI.

In past years two trainings were carried for judges, prosecutors and police officials organised with the support of the US Department of Justice (USDOJ) and the European Union Technical Assistance and Information Exchange (TAIEX).

Kosovo* recognised the importance of the provision of basic and advanced training for judges and prosecutors, with particular emphasis placed upon training for special prosecutors, due to their responsibility for cybercrime matters.

9.6.2 Assessment and summary of progress made

With the support of CyberCrime@IPA, two trainers from Kosovo* Judicial Institute have attended basic training for Judges and Prosecutors and the advanced training course in October 2012. They are able now to deliver training to other judges and prosecutors. A two days basic course was delivered to 13 judges, 4 prosecutors and 3 legal officers. The training modules developed under the project are in the process to be translated.

The Modules for training of judges and prosecutors developed under the CyberCrime@IPA project are already included in the programme for 2013.

CyberCrime@IPA project will make available training material in local languages for all project areas, including Kosovo*.

The KJI identifies lack of equipment as an obstacle to delivering more training, in particular a shortage of laptop computers. They would also welcome participation in regional conferences and support to participate in an internship programme in initial training and continuous training.

Two/three day basic courses have been delivered so far which have included as attendees:

- 13 Judges
- 4 Prosecutors
- 3 Legal Officers

There are plans to deliver training to a further 30 participants over the next 2 years. Additional training needs will be identified in response to end user demand. External experts together with KJI trainers and individuals from Hi Tech Crime Unit will deliver this training.

KJI have indicated that they will continue to need assistance beyond the planned lifespan of the CyberCrime@IPA Project. It is believed that Kosovo* has not been exposed to a sufficient number and variety of cybercrime cases in order to have developed sufficient in house experience to be able to deliver an effective training programme beyond basic, unaided.

9.7 LEA/ISP cooperation

9.7.1 The situation at the outset

The Telecommunication Regulatory Authority (TRA) (now Regulatory Authority of Electronic and Postal Communication - RAEPC) was responsible for licensing the telecommunication services in Kosovo*. As of December 2010 the Authority has granted 13 individual licences for Internet Services provider (ISP) and an additional 5 individual licences for International Telecommunication Facilities. Kosovo* has a providers association, namely the Kosovo* Association of Information and Communication Technology[35].

Although there had not been cases of cybercrime investigations, there were occasions when other requests were made for data from ISPs in relation to other technology enabled crimes.

The Authority collects date for capacity of traffic and subscriber data; however it is not responsible for the collection of content data from ISPs[36].

There were no nominated contact points for the police or ISPs and no regulations that obliged ISPs to retain data under data retention regulations; however the law on the prevention and fight against cybercrime foresees that ISPs will be required to retain data if it is needed for the investigation of crime. There were no training programmes for LE and ISPs, although along with the need to create instruments of cooperation between the entities this was recognised as an important requirement.

9.7.2 Assessment and summary of progress made

Data retention is regulated by the Law on Electronic Evidence. It is premature to evaluate the new law compelling ISPs to cooperate with Law Enforcement requests. It is recognised that the law on electronic communications will be of value.

Informal communication with the ISPs is generally good but can be inconsistent. No Memoranda of Understanding exist. There are plans to prepare an MOU with ISPs and hold a regular annual meeting of LE and banks/ISPs, engage in mutual education and create a blacklist of web pages that are damaging.

9.8 Financial investigations

9.8.1 The situation at the outset

The main types of fraud identified were credit card fraud, with 3 such cases being investigated. There were no special provisions for following criminal money flows or search seizure and confiscation of proceeds of cybercrime; however seizure in general is regulated through Article 240 of the Kosovo* Criminal Procedure Code (as of January 2013 replaced by Article 105 - Search and Temporary Sequestration)and confiscation is regulated by Article 83 of the Code (as of January 2013 replaced by Article 112 -Temporary Sequestration). Confiscation of proceeds of

[35] http://www.stikk-ks.org

[36] http://www.art-ks.org/?cid=2,33

money laundering is regulated by Article 36 of the law No. 03/L-196 on the Prevention of Money Laundering and Terrorist Financing.

The Public Prosecutor is the competent authority responsible for investigating all kinds of offences. The Special Prosecution is responsible for prosecuting organised crime. Within the Kosovo* Police, this responsibility lies with the Financial Investigation Unit within the Department against Organised Crime.

The lack of legal infrastructure, communication issues and absence of an agency for the administration of confiscated assets were considered to be the main obstacles to success in this subject area. Legislation aimed at prevention and simplified processes to enable effective communication between institutions was seen as areas where improvements may be seen.

9.8.2 Assessment and summary of progress made

The Financial Intelligence Unit is established within the Ministry of Finance as a central independent national institution responsible for requesting, receiving, analysing and disseminating to the competent authorities, disclosures of information concerning money laundering and terrorist financing. The main objectives of the Financial Intelligence Unit are: detecting, preventing and combating money laundering and terrorist financing in Kosovo.

It has 20 staff members, 11 of which are analysts, responsible to identify suspicious financial or terrorist funding streams. Moreover, it has access to a suit of advanced analytical software to assist in identifying illicit and suspicious financial transactions.

As a result of an analysis of financial legislation, recommendations were made to strengthen and improve existing legislation. These recommendations have been incorporated into draft legislation, which is awaiting approval.

Statistics on cases prosecuted are not available within the Unit as the Financial Investigation Unit carries out Investigations. In order to enhance cooperation and coordination and to accelerate the exchange of information, the Financial Intelligence Unit and the Kosovo Police has signed the MoU on exchange of information relating to the prevention and detection of money laundering and financing of terrorism and other criminal offences which are related to money laundering and financing of terrorism. A coordinator will soon be appointed to supervise the end-to-end processes.

The Financial Intelligence Unit has access to data from a number of sources. It is currently working with most of the European Financial Intelligence Units. Memoranda of Understanding signed exist with (8) eight countries and many other European Financial Intelligence Units are in process of considering the proposal sent by the Financial Intelligence Unit of Kosovo for signing MoUs.

The results of this flagship project will be used to provide useful operational insight to all FIUs within the region and beyond.

This is an area in which progress has been made during the project period. However, there is still room for an improvement in cooperation between national organisations.

9.9 Progress made against previous recommendations

Cybercrime Situation Report March 2011	Progress reported
1. Keeping statistics that provide an insight in the seriousness of cybercrime in the national territory. Such statistics could for example 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 not readily available
2. Keeping statics about the application of the specific powers in the criminal procedural code, including with information about application, technical details and cases concerned.	Some Progress in DILC
3. Consideration of the observations made in the report above 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.	Work in progress
4. Specific attention is demanded with regard the legal concept of seizure of computer data and the possible need for expedited execution of investigative powers, in particular in view of the new criminal procedural code.	Work in progress
5. Establishment of a 24/7 contact point as already provided for under domestic law.	Temporary contact point established.
6. Continue the development of the police unit and consider the formation of a prosecution unit to combat cybercrime in accordance with the needs of the country.	Some progress made. See additional Recommendations below.
7. 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.	Some progress made. See additional Recommendations
8. Develop relationships with academic and private sector institutions that may assist in combating cybercrime through common activities such as research, training and education.	No progress reported
9. 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 progress made
10. 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 the Global Project on Cybercrime.	Some progress made. No MOUs exist yet.
11. 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"	Capability not developed yet
12. Incorporate good practice in the handling of electronic evidence in criminal investigations; examining existing guides such as those developed by Interpol	Some progress made

and Europol.	
13. 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. Political obstacles remain an issue.
Recommendations made by second progress report 1/11/11 – 31/5/12	
Bilateral agreements regarding regional cooperation.	Progress is continuing
Training for judges, prosecutors and police related cybercrime.	Some progress made
Increasing the cooperation with other countries on cybercrime.	Progress is continuing

9.10 New recommendations

1. Make contact with other well established cybercrime units and consider the recommendations made in the Good Practice Study on specialised units developed by the CyberCrime@IPA with a view to:
   - Identifying priority equipment requirements
   - Observing key working practices, procedures and examples of good practice.
   - Adopt and adapt operating procedures and management policies.
   - Obtain, adopt and adapt any operational guides or other useful documentation or material the host sites are able to provide.
2. Provide basic training for judges to include all forms of electronic evidence
3. Appoint an individual prosecutor as portfolio holder with responsibility for policy advice for cybercrime and related matters and to act as consultant for other prosecutors.
4. Further develop knowledge of electronic evidence and cybercrime threats through regional cooperation and through liaison with the Pilot Centre in Croatia for Judges and Prosecutors.
5. Obtain, adopt and adapt training resources from neighbouring regional judicial sites for translation and adaptation on electronic evidence.
6. Provide a basic level of training to all Law Enforcement recruits.
7. Train existing police first responders.
8. If necessary, outsource training provision and use existing subject matter experts within the region
9. Obtain adopt and adapt law enforcement training materials already in existence throughout the region and available
10. Use feedback from Cybercrime Unit from operational reviews and incorporate "lessons learned" into training.
11. Ensure advanced training delivery to Cybercrime specialists.

10 Overall conclusions

Information technologies offer extraordinary opportunities and benefits for societies. Cybercrime puts these benefits at risk. Governments therefore need to invest the necessary resources to protect their society against cybercrime. Such an investment in priority fields is worthwhile.

The Assessment Report suggests that progress has been made in all project areas in all fields of interventions foreseen under the project. Authorities of project areas have implemented important mechanisms to counter cybercrime and engaged the authorities in reforms towards a consistent approach to cybercrime.

The present Report intends to supplement previous reports drafted under the project and provide an up to date assessment of each area's capabilities to combat cybercrime together with an overview of problem areas.

As previously stated, the project areas of the region are and remain at different stages of development in their exposure to cybercrime and their legislative and practical capabilities to respond to the threats of cybercrime.

As may be seen from the details of Internet usage in each project area, the criminality associated with Internet and other forms of technology will continue to increase as usage continues to rise. In the short period since the project began, it is apparent that use of technology is on the increase and countries should not be complacent about the challenges that will continue to be present where criminals misuse technology.

It is important to recognise that as the project has concluded, it will be necessary for countries to set out how they will continue the progress that has already been made towards initial and subsequent recommended action.

Without accurate statistics showing the nature and range of investigations, prosecutions together with disposals, it will be difficult to design comprehensive cybercrime national strategies and training strategies. All previous reports as well as events and Steering Committee meetings have made recommendations regarding statistics and yet for the majority, this still remains an unfulfilled aspiration. Specific information regarding crimes prosecuted and result in convictions set against the number reported would allow the identification of capability gaps. Often the statistics available were partial and fragmented and did not indicate the entire process from report/discovery through investigation, indictment and disposal.

With regard to the legal framework there is in the region a firm legal foundation to engage against cybercrime nationally and internationally. Future amendments should consider the recommendations made by this Assessment Report.

During the assessments it became apparent that there was a wide range of capabilities within various cybercrime units. Some units are adequately resourced with experienced skilled staff, appropriate equipment, facilities, analytical software and possessed sufficient resilience to provide an adequate operational response. Others are not yet. It is necessary to ensure that all cybercrime units within the region are equipped with a standard operating platform, adequate hardware and a basic suite of analytical tools. Standardisation of equipment and software would facilitate the development and promulgation of detailed operating manuals.

New challenges to existing capabilities are emerging such as the increasing criminal use of "cloud computing", encryption, freely accessible Wi-Fi, use of Internet cafés and other tactics employed to defeat law enforcement activity. Developing tactical responses to this and other emerging technologies will require development of new techniques and operational policies.

The numbers of individuals engaged in specialist units can also impact on national cybercrime capability. In some of the project areas visited the cybercrime units consisted of one or two officers with little or no access to specialist technical equipment. Such units are highly unlikely to be able to perform the full range of techniques allowed by law. It is also doubtful whether such small units are resilient enough to cope with sickness, holidays, days off etc. In other project areas, considerably more personnel were engaged in specialist units.

The training and education programme developed by the project together with other initiatives have done a great deal to raise educational standards in the field of cybercrime throughout the region. However, a common request remains for more information and practical training on how to deploy specialist measures such as live interceptions. This knowledge is mainly tacit and remains within the domain of a few specialist practitioners. There is a need for this knowledge to be reduced into operational manuals and standard operating procedures. Such "products" would need to be continuously reviewed as criminal tactics and technology change. They would also be informed by tactical developments by law enforcement worldwide, academic research, initiatives from within the communications industry and beyond. From this would flow the training materials that are so much in demand. The corpus of cybercrime knowledge would thus be developed and nurtured making the region less dependent upon international trainers.

The requirement for specialist products also extends to the development of tools such as forensic and special investigation tools. The existing commercial products are very expensive and may be replaced or supplemented by tools developed specifically for a country or region. In this instance the creation of a centre of excellence may assist and also create new relationships with others in industry and academia that specialise in these matters.

A recurrent theme throughout the latest and previous assessments has been the slow pace of obtaining international assistance. A variety of potential reasons have been put forward such as, systems are too bureaucratic, and prioritisation processes are inadequate along with an associated geographic nonchalance i.e. "this isn't really our problem". There were no statistics available to indicate where delays occurred. The database maintained by the Department of International Legal Assistance in Kosovo* could potentially identify time lines associated with specific types of legal applications and show what parts of the process involve the longest delays.

A core problem identified by project areas is that competent authorities for mutual assistance are overburdened with requests and understaffed. Standardised multi-language request templates, better use of the possibility for direct contacts available under different agreements, a specific regime for subscriber information (IP identification), and a more pro-active role of 24/7 points of contact are among the solutions identified.

The Cybercrime Convention Committee (T-CY) will assess in 2013 the provisions on international cooperation and the efficiency of the 24/7 Network. This will help ensure follow up to the issues identified during the implementation of the project and during the assessment visits.

Training strategies do not yet exist in all project areas. Thus developing such strategies should be considered with priority.

In a number of countries or areas, first responder training was non-existent as cybercrime was seen as a specialist field. The police service and in particular, the first responders are at the front end of the criminal justice system. Ignorance at this point of the process can lead to evidence being overlooked, lost or destroyed. The project will follow on this in the remaining months.

The ability to combat illegal money flows on the Internet was evident in only two or three of the project areas. Generally speaking, one of the key determining factors was the technical ability possessed by the relevant Cybercrime Unit. Access to public and state databases was also variable as was access to analytical software. There were also wide variations in asset confiscation legislation with respect to the burden of proof and standard of evidence required.

The Kosovo* pilot site could provide feedback to other project areas on the holistic techniques required to combat money flows on the Internet, together with any "lessons learnt" during the course of the pilot. Prosecutors and police commanders should draft protocols or operating policies which include, policies on communication, referral, extent of analytical/intelligence investigations and delegated levels of authority.

The level of cooperation with ISPs throughout the region is variable. A common issue is the diversity of software used within the industry and in consequence the variety of formats in which ISP data is presented. This poses a particular challenge when conducting any form of analysis. In addition to variable formats, volumes of data can pose similar problems.

The possibility for law enforcement and judicial authorities to contact US-based ISPs directly to obtain information is not sufficiently made use of.

Feedback from project participants clearly indicates that there is a desire to ensure that the networking benefits of the project continue after it concludes. The creation of the Judicial Pilot Centre in Zagreb for training for judges and prosecutors is one example of an opportunity for continuity for one group of project participants.

For the law enforcement community the creation of a centre of excellence for training research and education for the region should be considered in the future. This would help those project areas that are not as well developed in their programmes as well as ensuring consistency and provide a vehicle for future collaboration. The European Commission has in recent years been very supportive of such initiatives and has helped to fund the creation of a number of national centres through its funding programmes, most notably through the 2CENTRE project. Some project areas have already expressed an interest in developing their own national centre and it is considered that a regional capability would add continuing value to the successes of the CyberCrime@IPA project. It may be appropriate for the project areas to consider a collaboration in order to create such a centre or to support the creation of a national centre in one of the areas. This may also benefit the wider criminal justice community and may work in collaboration with the pilot centre for judicial training.

At the end it has to be stated that with no doubt the project is a tremendous success and has made a serious impact in the region. However, as any project or effort done by international organisations or other donors it cannot achieve the maximum results without the full commitment of the project teams and the authorities in the project areas. The results of the progress made show also the understanding by these stakeholders of the importance of taking such measures, as well as of making full use of the many opportunities created by the project.

The CyberCrime@IPA is subject to regular monitoring. The latest "ROM WBT Monitoring Report" dated November 2012 graded the project "very good" (A) with regard to "relevance and quality of design"; "efficiency of implementation to date"; "impact prospects"; and "potential sustainability". The findings of that report confirm and complement the findings of the assessment exercise.

Extracts of the ROM WBT Monitoring Report (November 2012):

- The project has a strong working discipline for the activities and the production of outputs. The pace set at the outset of the project has been maintained and benefits from the six months extension approved in 2011.
- Good communication has been evident from the project start. The CoE is in daily contact with the beneficiaries. The project is implemented though workshops and conferences and training at regional level and for single countries.
- The project is highly interactive. A participative approach is applied where representatives from the participating countries work with the consultants in round tables or workshops to develop the project deliverables. This approach facilitates the adaptability of the project to the specific needs of each participating country. The beneficiary countries interviewed recognised that the project is tailor fit to meet their needs and is realised with great flexibility in order to reach the targets.
- The project was able to deepen and support commitments of the participating countries to the fight against cybercrime, accelerating the process of implementation of Budapest Convention. It also creates the opportunity for beneficiaries to enter in the cybercrime networks for training and sharing relevant experiences at international level, for example the OCTOPUS Conference, European Cybercrime Training and Education Group (ECTEG) or Cybercrime Centres of Excellence Network for Training Research and Education (2Centre).
- The project steering committee is proactive in meeting to discuss progress, plans and the agenda and to make recommendations. Communication between the countries, the CoE and the EC Task Manager is effective. At local level coordination is ensured by the local "coordination" role played by main stakeholder responsible for national activities and problem solving. Beneficiaries participate with enthusiasm to project activities and planning
- The self-assessment and the peer to peer approach is enhancing ownership of the project results through the project management culture and a strategic attitude towards local issues. The level of awareness about the project among the target group is high.
- The participation at the main conferences and seminars was high (senior officer and government representatives) showing a good level of ownership and sponsorship in the countries and backing for the work by the different offices involved. The practical results already delivered include law modification and amendments, setting up or strengthening of Cybercrime investigation units, and sign off of the Conventions.
- After 24 months of implementation, the project has made considerable progress towards achieving its objectives. The ultimate expected impact is a higher detection and prosecution of cybercrime at national and regional levels. This is seen through the emergence of cybercrime strategies and policies, support for legislative amendments in Serbia and Bosnia and Herzegovina, special training for law enforcement, prosecutors and the judiciary, financial investigations and criminal money flow on the Internet, training for an efficient international cooperation against cybercrime and the establishment of a Pilot Centre on judicial training in Croatia. The early indication is that the number of cybercrime cases being prosecuted is rising in the participating countries. This is the practical reflection of project impact.
- A key factor for impact is the networking of the stakeholders within the countries to coordinate their investigative efforts and to share information to the extent possible. The project has achieved this. The regional dimension has enabled good practices from more advanced countries to be shared. This was welcomed. The initiatives and networks involving public and private sector institutions or NGOs cooperating across borders is a new approach which is appreciated by both sides and provides a basis point which can be further developed. In country efforts to incorporate the cybercrime training within existing programmes at national level (academia, police or magistrates curricula) contribute to impact beyond the immediate target group reached by the project. The countries have applied for membership at ECTEG and are aware of the methodologies and tools provided by ECTG.
- Specific impact has been achieved in Kosovo. The project has supported the establishment of a specific unit for fighting cybercrime and a start to collecting statistics on the impact of technology on crime. The current level of international cybercrime cases surfacing in Kosovo made the project timing particularly relevant. Kosovo is also benefiting from the ability to

work with the licensed organisations to update the ECTEG materials and to create new materials as required. The country is applying for ECTEG membership.

- Awareness, ownership of projects results is very strong. The project impact beyond the primary target beneficiaries and benefits is already apparent. There are no negative external factors influencing potential impact.
- The project is treated as a national priority and the beneficiaries are strongly committed to it. Many of the project impacts are already reached and the benefits are expected to be long lasting. Since the project is a capacity building intervention, its sustainability will be mainly in the further development to maturity of the integrated working approaches to cybercrime. There is a financial commitment to this aim in the participating countries.
- A sufficient number of officials from different countries have participated directly in the project to provide for its sustainability. The inter-institutional relations and inter country relations are excellent. The CoE expects the project to have wider international impact, enhancing long term sustainability of results. Country stakeholders gained visibility and reputation and expect to be involved actively or as experts in network conferences and cybercrime networks. To this regard it's expected that the discussions and updating of documents will remain alive during future international conferences on cybercrime. The beneficiaries are part of an international network and will benefit for knowledge sharing and information coming from other countries.
- The training approach enhanced the capacity building effect beyond the number of beneficiaries directed involved. All the beneficiaries are extending their level of training involvement, and this should ensure a deeper and wide capacity building result. Further dissemination of knowledge and awareness about cybercrime to other judges and prosecutors is a continuous process. The capacities built through this project represent a viable basis for a successful implementation of this multiplication process. The training activities are sustainable as the materials have been also provided to existing training institutions (police school, magistrates, etc.) and therefore they will remain alive and used. The new pilot regional training centre would ensure continuity. Some further external support would be needed to enable more law enforcement officials to participate in the Postgraduate programme at UCD and to provide useful equipment for the investigation units (that was out of scope of this project).
- Cybercrime is an international issue and project has synergy with a large range of initiatives and organisations, in particular developed at the European Union level (e.g. Europol, European Cybercrime Training Education Group (ECTEG), Cybercrime Centres of Excellence for Training, Research and Education (2CENTRE), the European Cybercrime Task Force (EUCTF), the Organization for Security and Co-operation in Europe (OSCE), Southeast Europe Law Enforcement Centre (SELEC) and others). The contribution of the project and outputs has been confirmed on many occasions. A notable result is the consensus reached for electronic evidence guidance, which was presented at the recent Octopus conference in a specific focus section dedicated to the project. There was considerable interest in this output and the document is now receiving a lot of attention in the international community as a best practice example.

11 Appendices

11.1 Appendix A - Assessment methodology

11.1.1 Rationale

The terms of reference of the CyberCrime@IPA project identify a need for an "assessment of progress made":

> Since measures against cybercrime involve different stakeholders and a range of actions, it is important to assess progress made and the effectiveness of different measures in a coherent manner, and to feed the results back in to the policy making process.

Such an assessment would need to cover, inter alia:

- Level of compliance of cybercrime legislation with international standards
- Effectiveness of high-tech crime units and other specialised services
- Level of law enforcement and judicial training
- Level of public-private, in particular LEA/ISP cooperation
- Effectiveness of international police and judicial cooperation
- Effectiveness of criminal justice measures against cybercrime
- Capacities to prevent criminal money flows and search, seize and confiscate crime proceeds on the internet.

A regional project, such as the present one, lends itself particularly well to a process of peer-to-peer assessments.

This need is to be addressed through the following expected result and activities:

> **Result 8** Regional assessments carried out to determine progress made in terms of legislation, the strengthening institutional capacities for the investigation, prosecution and adjudication of cybercrime and international cooperation

Indicators include:

- Methodology adopted and applied
- Assessment reports available

The following activities would ensure the delivery of this result:

- **Activity 8.1** Develop a methodology for the regional peer to peer assessment of progress made against cybercrime
- **Activity 8.2** Carry out a cycle of regional assessments, including compliance reports
- **Activity 8.3** Organise two regional workshops for discussion and adoption of assessment reports.

Result 8 on assessments is closely related to result 1 on cybercrime policies and strategies.

The project rational is this respect to the assessments is the following:

1. A situation report was prepared between November 2010 and February 2011 under CyberCrime@IPA assessing the situation in each project area with regard to legislation, specialised institutions and international cooperation, law enforcement training, judicial training, financial investigations and law enforcement – Internet service provider

cooperation. That report thus established the baseline. It also made recommendations for reform.

2. CyberCrime@IPA supports activities related to these topics under results 2 to 7. These activities provide additional information and lead to additional recommendations.

3. Peer-to-peer assessment visits are to be carried out to each project area to further complete the information of the situation report, review implementation of the recommendations made so far under the project (situation report and project activities). This should lead to an assessment report for each project area that contains:
   - consolidated and accurate information on each of the themes covered
   - an analysis of the state of implementation of recommendations
   - specific recommendations for further action.

4. The draft assessment reports would then be discussed in a regional meeting in view of adopting them.

5. These reports should be fed back into cybercrime policies and strategies (result 1) and are to feed into a regional agreement on priorities with respect to cybercrime (activity 1.4).

11.1.2 Peer-to-peer assessments

Objective

The objective is to provide the authorities of project countries and areas with an assessment of their capabilities to counter cybercrime and with recommendations for further reform.

By the end of the assessment cycle, a report for each project area is to be adopted.

The results of the assessment will inform cybercrime policies, strategies and measures in each project area as well as the region.

The participation of representatives of different project areas in each other's assessment will help share information and good practices within the project region.

Subjects to be covered

The assessments should cover the same topics that were the subject of the situation report and that are being addressed by CyberCrime@IPA:

- legislation (result 2)
- specialised institutions and international cooperation (result 3)
- law enforcement training (result 4)
- judicial training (result 5)
- financial investigations (result 6)
- law enforcement – Internet service provider cooperation (result 7)

As in the case of the situation report, the assessments may also reflect additional information on the threat of cybercrime.

This means that the original questionnaire used for the situation report could be adapted for use in the assessments.

Procedure

1. Agreement on the procedure and timeline for visits to eight project areas (Steering Committee in September 2012)
2. Confirmation of assessment teams (Proposal: 3 members from the project areas, 1 Consultant, 1 representative in the T-CY) (Steering Committee in September 2012)
3. Visits (duration: 3 days, including 1 day for preparation of draft conclusions/recommendations)
4. Preparation of draft reports based on the situation report, progress reports, discussions during the visits and other information
5. Submission of draft reports to project areas for comments
6. Revised draft reports for discussion in a regional meeting ("plenary session")
7. Adoption of final reports
8. Results to be reflected in the regional agreement on priorities regarding cybercrime

Conclusion

This approach will allow for assessments to start within 15 months after the launching conference. By that time, a large number of activities will have been carried out and results should become visible. Sufficient time will subsequently be available to feed the findings into the regional agreement on cybercrime priorities.

11.2 Appendix B – Assessment Teams

Team members	Project area assessed
Branko Stamenkovic (Serbia) Kornelija Ivanušić (Croatia) Gazmend Citaku (Kosovo*) Chris Sparks (UK)	"The Former Yugoslav Republic of Macedonia"
Vlado Miloseski ("The former Yugoslav Republic of Macedonia) Diana Stillo (Albania) Bahadır Tataroğlu (Turkey) Chris Sparks (UK)	Kosovo*
Zarko Pajkovic (Montenegro) Marjan Stoilkovski ("the former Yugoslav Republic of Macedonia" Chris Sparks (UK)	Serbia
Ana Kordej (Croatia) Denisa Asko (Albania) Ljuban Petrovic (Serbia) Chris Sparks (UK)	Montenegro
Arqile Koca (Albania) Bojana Paunovic (Serbia) Tomislav Curic (Bosnia and Herzegovina) Chris Sparks (UK)	Turkey
Skender Abedini Diana Kovacevic Remenaric (Croatia) Chris Sparks (UK)	Albania
Vlado Miloseski ("The former Yougoslav Republic of Macedonia" Markko Künnapu (Estonia, T-CY Chair) Bilal Sen (Turkey) Chris Sparks (UK)	Croatia
Ömer Temiz (Turkey) Marjan Stoilkovski ("The former Yugoslav Republic of Macedonia" Markko Künnapu (Estonia, T-CY Chair) Chris Sparks (UK)	Bosnia and Herzegovina

11.3 Appendix C – Declaration on Strategic Priorities

CyberCrime@IPA

EU/COE Joint Project on Regional Cooperation against Cybercrime

Strategic Priorities in the Cooperation against Cybercrime

Adopted by the

Meeting of Ministers and Senior Officials of Ministries of Interior and Security, of Ministries of Justice and of Prosecution Services of countries and areas participating in the CyberCrime@IPA project[1]

Dubrovnik, Croatia, 15 February 2013

www.coe.int/cybercrime

Funded by the European Union and the Council of Europe

EUROPEAN UNION

COUNCIL OF EUROPE CONSEIL DE L'EUROPE

Implemented by the Council of Europe

[1]Albania, Bosnia and Herzegovina, Croatia, Montenegro, Serbia, "The former Yugoslav Republic of Macedonia", Turkey and Kosovo*.

* This designation is without prejudice to positions on status, and is in line with UNSC 1244 and the ICJ Opinion on the Kosovo Declaration of Independence

Declaration by Ministers and Senior Officials on Strategic Priorities against Cybercrime

We, Ministers and Senior officials representing Ministries of Interior and Security, Ministries of Justice and Offices of Prosecutor's General of countries and areas participating in the CyberCrime@IPA project

- Meeting at this regional Conference on Strategic Priorities on Cybercrime held in Dubrovnik, Croatia, from 13 to 15 February 2013, in cooperation with the Council of Europe and the European Union;

- 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@IPA regional project;

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

We endorse

the strategic priorities on 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

Dubrovnik, Croatia, 15 February 2013

Appendix: Strategic priorities on 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 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 should therefore consider the preparation of specific cybercrime strategies or to enhance cybercrime components within cybersecurity strategies or policies.

Relevant authorities should consider the following actions:

- **Adopt 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. Countries and areas participating in the CyberCrime@IPA 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.[37] However, further strengthening is required and often legislation has yet to stand the test of practice.

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 on law enforcement access to electronic evidence.** 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 or guidelines 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 modernization 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 countries 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.

[37] 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 countries and areas participating in the CyberCrime@IPA 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.

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 not yet fully implemented.[38]

The 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, countries 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.

38 http://www.coe.int/t/DGHL/cooperation/economiccrime/cybercrime/Documents/Cyber%20IPA%20reports/2467_LEA_Training_Strategy_Fin1.pdf

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. Progress was made in countries and areas participating in the CyberCrime@IPA project in that training modules have been prepared, trainers trained and basic and advanced courses have been delivered on pilot basis. In addition, a Regional Pilot Centre for Judicial Training on Cybercrime and Judicial Evidence is being established. These achievements need to be institutionalised.

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:

- **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.

- **Consolidate the Regional Pilot Centre for Judicial Training established in Zagreb, Croatia.** Domestic judicial training institutions from the region should interact with the Regional Pilot Centre for Judicial Training in view of updating course materials, documenting and disseminating good practices and providing regional 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 countries and areas, 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.[39]

[39] 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[40] 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.[41]

- **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 countries and areas. 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.

[40] http://www.coe.int/t/dghl/cooperation/economiccrime/cybercrime/Documents/LEA_ISP/default_en.asp. The guidelines are available in the languages of the CyberCrime@IPA countries and areas.
[41] 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 will be undertaken by the Cybercrime Convention Committee (T-CY). 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 countries and areas 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**.