CyberCrime@IPA

EU/COE Joint Project Regional Cooperation in Criminal Justice:
Strengthening capacities in the fight against cybercrime

Ares(2012)810062

www.coe.int/cybercrime

Version 6 July 2012 (final)

IPA Regional Programme 2010 - Agreement number: CN 2010/248-578

2nd Progress Report

covering the period

1 November 2011 – 31 May 2012

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

Funded
by the European Union
and the Council of Europe

EUROPEAN UNION

COUNCIL OF EUROPE CONSEIL DE L'EUROPE

Implemented
by the Council of Europe

Contact

For further information please contact:

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

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

Disclaimer

LIST OF ABREVIATIONS

24/7 Network	The network of contacts point established under Article 35 of the Convention on Cybercrime
2CENTRE	Cybercrime Centres of Excellence for Training, Research and Education
ATM	Automated Teller Machine
BiH	Bosnia and Herzegovina
BKA	Bundeskriminalamt (Germany)
BKM	Interbank Card Centre
CERT	Computer Emergency Response Team
CEPOL	European Police College
CoE	Council of Europe
CyberCrime@IPA	EU/COE Joint Project Regional Cooperation in Criminal Justice: Strengthening capacities in the fight against cybercrime
ECTEG	Europol, European Cybercrime Training Education Group
ECHR	European Court of Human Rights
EU	European Union
EUCTF	European Union Cybercrime Task Force
EUROJUST	The European Union's Judicial Cooperation Unit
FBiH	Federation of Bosnia and Herzegovina
FIU	Financial Intelligence Units
GPEN	The Global Prosecutors E-crime Network
ICT	Information and communications technology
Interpol	International Criminal Police Organization
ISP	Internet service providers
IP	Internet Protocol
IPA	Instrument for Pre-accession Assistance
IT	Information Technology
LEA	Law Enforcement Agency
MLA	Mutual Legal Assistance
MONEYVAL	Committee of Experts on the Evaluation of Anti-Money Laundering Measures and the Financing of Terrorism
MOU	Memorandum of Understanding
MSc	Master of Sciences programme in Forensic Computing and Cybercrime Investigation offered by University College Dublin
OSCE	Organization for Security and Co-operation in Europe
RS	Republika Srpska of Bosnia and Herzegovina
SECI	Southeast European Cooperative Initiative (Regional Center for Combating Trans-border Crime)
SELEC	Southeast European Law Enforcement Center
UCD	University College Dublin
UK	United Kingdom
UN	United Nations
UNODC	United Nations Office on Drugs and Crime
USA	United States of America
WiFi	Wirelessly connecting electronic device

Contents

1 Executive summary

The aim of the CyberCrime@IPA regional project is to strengthen the capacities of criminal justice authorities of Western Balkans and Turkey to cooperate effectively against cybercrime.

Through CyberCrime@IPA the European Union and the Council of Europe – in cooperation with other partners – support countries of the Western Balkans and Turkey in their efforts to take effective measures against cybercrime based on existing tools and instruments, in particular the Budapest Convention on Cybercrime. The countries/areas covered by the project are Albania, Bosnia and Herzegovina, Croatia, Montenegro, Serbia, "The former Yugoslav Republic of Macedonia", Turkey and Kosovo[1].

The project started in November 2010 with an inception phase which was completed with the launching conference held in Istanbul, Turkey, on 17-18 February 2011.

In the light of a very charged calendar of activities, at the 2nd Steering Committee Meeting (Budva, Montenegro, September 2011), project areas requested an extension of the project by six months. The request was approved by the European Commission and subsequently formalised. The 3rd Steering Committee Meeting (Skopje, "The former Yugoslav Republic of Macedonia", 30 March 2012) agreed on a revised workplan that already takes into account the six months extension.

The 1st Progress Report, Interim Report and Financial Report were submitted and subsequently approved by the European Commission.

This 2nd Progress report focuses on the activities carried out between 1 November 2011 and 31 May 2012.

After 19 months of implementation, the project made considerable progress towards achieving its objectives. During the reporting period, the project implemented activities that are relevant for all expected results, that is, cybercrime strategies and policies, support for legislative amendments in Serbia and Bosnia and Herzegovina, 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.

While during the previous reporting period much attention was paid to the development of tools and while further tools are being developed, the project increasingly supported their implementation and practical application. During the reporting period this was particularly true for the training component. Between February and May 2012, the training materials developed under the project were tested, 15 trainers from all project areas were trained, eight in-country judicial trainings were delivered and the development of a guide on electronic evidence was initiated. By completing these activities, the project can now focus on the integration of the basic material into the curricula of the training institutions, complete the advanced training materials (module 2) and deliver the remaining four advanced trainings foreseen under the project.

[1] All reference to Kosovo, whether to the territory, institutions or population, in this text shall be understood in full compliance with United Nations Security Council Resolution 1244 and without prejudice to the status of Kosovo.

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

Result 1: Cybercrime policies and strategies

- Each workshop organised by the project was addressed by decision-makers from the respective host country.
- The project facilitated large representation from each area in the Octopus Conference (Strasbourg, 21-23 November 2011) and the Cybercrime Convention Committee (T-CY) Plenary (24-25 November 2011). Among other themes, the Octopus Conference discussed and provided good practices regarding policies and initiatives on cybercrime and cybercrime strategies.

Result 2: Harmonisation of legislation

The project:

- Advised project areas on strengthening cybercrime legislation, in particular countries that specifically requested additional support i.e. Bosnia and Herzegovina and Serbia. Thus, two specific workshops on legislation were organised in Belgrade (Serbia) and Sarajevo (Bosnia and Herzegovina) resulting in the decision taken by the authorities to draft amendments to the legislation in line with the Convention on Cybercrime and related standards.
- Provided specific recommendations and legislative advice for improvement of the legislation on cybercrime and protection of children against sexual violence in Bosnia and Herzegovina.
- Participated in the meeting of the Team for tracking of the implementation of legislation in Bosnia and Herzegovina to support amendments to the cybercrime legislation (Sarajevo, 9 May 2012).
- Discussed and exchange views on the latest developments of cybercrime legislation, including protection of children against sexual exploitation and sexual abuse at global level during the Octopus Conference.
- Finalised a study on Article 15 on "procedural safeguards and conditions", including information from Croatian legislation as good practice.[2] An overview of the report was presented during the Octopus Conference (Strasbourg, 21-23 November 2011) and the example of Croatia will be presented in a follow-up workshop to be organised at the next Octopus Conference (Strasbourg, 6-8 June 2012).

Result 3: Enhanced regional and international cooperation

The project:

- Increased the cooperation between Western Balkans and Turkey and the Eastern Partnership region by organising joint activities with the joint European Union/Council of Europe project Eastern Partnership – Cooperation against Cybercrime (Cybercrime@EAP)[3]. Furthermore, it provided the opportunities for project areas to establish contacts with countries all over the world during the Octopus Conference organised under the global Project on cybercrime (Phase 3).
- Organised a regional workshop on international cooperation to follow up on the issues identified in the previous activities as obstacles to efficient international cooperation against cybercrime.

[2] http://www.coe.int/t/DGHL/cooperation/economiccrime/cybercrime/Documents/Reports-Presentations/2467_SafeguardsRep_v18_29mar12.pdf
[3] http://www.coe.int/t/DGHL/cooperation/economiccrime/cybercrime/cy_Project_EaP/Default_EaP_en.asp

- Assessed the progress made under the project with regard to the effectiveness of 24/7 points of contact and of other authorities dealing with international cooperation requests. In addition, it discussed the need for gathering statistics on these issues.
- Created synergies with other channels of international cooperation e.g. EUROJUST, ECTEG, SELEC, Interpol, Europol, GPEN etc. as well as the European Union project - IPA 2008 Police Cooperation: Fight against Organised Crime particular Illicit Drug Trafficking, and the Prevention of Terrorism, implemented by the Criminal Intelligence Service Austria.
- Produced a "good practice study on specialised cybercrime" which was carried out jointly with the European Union Cybercrime Task Force (EUCTF) and finalised during the Octopus Conference (Strasbourg, 21-23 November 2011).[4] This study will provide guidance to any country intending to set up specialised units. In Turkey, a new cybercrime department within the Turkish National Police was established by taking into account the recommendations from the study. Furthermore, the study was presented in an activity organised under the joint European Union/Council of Europe project Eastern Partnership – Cooperation against Cybercrime (Cybercrime@EAP) with the intention to introduce examples from Eastern Partnership countries.

Result 4: Law enforcement training

The project:

- Ensured participation of one representative from each country/area in the Master of Sciences (MSc) programme in Forensic Computing and Cybercrime Investigation offered by University College Dublin (UCD). In this context the project funded the participation in the summer examination of the students.
- The development of a Guide on Electronic Evidence was initiated. The draft document will be discussed in the upcoming Octopus Conference in Strasbourg on 7 June 2012.

Result 5: Judicial training on cybercrime and electronic evidence

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. The course provides legal as well as practical information about the subject matters and concentrated on how these issues impact on the day-to-day work of judges and prosecutors.
- 15 trainers from the 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 was delivered based on the training pack developed and by the trainers trained under the project (with assistance from international trainers).
- Support for establishing a Pilot Centre within the Judicial Academy of Croatia was continued.

Result 6: Financial investigations

The project:

- Raised awareness of the need to confiscate proceeds from crime on the Internet. Participants in the activities identified solutions for overcoming the problems encountered in the prevention and control of criminal money flows on the Internet.

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

- Strengthened inter-regional cooperation (Western Balkans and Turkey and Eastern Partnership) against criminal money on the Internet by organising an event with participation by Eastern Partnership countries (Cybercrime@EAP).
- Contributed to the finalisation of the "Typology study on Criminal money flows on the Internet: Methods, trends and multi-stakeholder counteraction"[5] and supported project areas in the preparation of proposals to follow on the recommendations of this study as well as the new 40 Recommendations of the Financial Action Task Force.

Result 7: Law enforcement – Internet service provider cooperation

The project:

- Promoted cooperation between law enforcement and the private sector during several activities organised during the reporting period (e.g. Octopus Conference, the Intra-regional Workshop on Moneyflows on the Internet, the Regional workshop on handling international cooperation requests relating to cybercrime).

Result 8: Regional assessments carried out to determine progress made

The project:

- Drafted a methodology for carrying out regional assessments to determine progress which was agreed by the Steering Committee in September 2011. The assessments that will be carried out under this methodology in 2012 will subsequently feed into regional policies and strategies and the regional agreement that is to be adopted towards the end of the project.

Based on the above-mentioned achievements, it is clear that the project has sustained a broad process of reform towards a concerted and consistent approach to cybercrime, which can be considered an important strategic achievement, important tools have been prepared to be made available in the project areas and a number of activities foreseen by the project were completed.

In all events organised within the project, good practices were presented by partner countries (France, Slovenia and Romania), European Union Member States (e.g. Belgium, Estonia, Germany, Ireland, Portugal, the Netherlands and United Kingdom), as well as from the United States of America and the private sector (August & Debouzy – a law firm based in Paris representing several major ISPs that includes: Microsoft, Orange etc.). 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), Southeast European Law Enforcement Center (SELEC) and others).

The cooperation with multi-agency project teams from each project area is excellent and the relevance of the project was confirmed on many occasions.

During the Octopus Conference in November 2011, the project was presented to more than 200 participants representing countries from all continents, international organisations and the private sector followed by interventions from the project teams that underlined the importance of the project.

Meetings, including at the level of the United Nations, confirmed global consensus on the need for capacity building against cybercrime. In this context, the CyberCrime@IPA project as well as

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

cooperation with European Union on cybercrime issues are presented as best practices that can be followed by other organisations.

In short, CyberCrime@IPA is very much on track. In the coming months, the finalisation of additional tools and the implementation of activities will be accompanied by a series of assessments (Result 8). This will add further impetus to reforms and to an agreement on regional priorities regarding measures against cybercrime in early 2013 (Result 1, activity 1.4).

2 Description of the Action

Title of the Action	Regional Cooperation in Criminal Justice: Strengthening capacities in the fight against cybercrime (DGHL/2010/2467)
Name of beneficiary of grant contract	Council of Europe/Data Protection and Cybercrime Division
Name and title of the Contact person	Alexander Seger, Head of Data Protection and Cybercrime Division
Contract number	2010/247-988
Project area	Western Balkans and Turkey: Albania, Bosnia and Herzegovina, Croatia, Montenegro, Serbia, "The former Yugoslav Republic of Macedonia", Turkey and Kosovo*
Duration	30 months (1 November 2010 – 30 April 2013)[6]
Budget	EUR 2,777,778
Funding	European Commission (IPA Regional Programme 2010) and Council of Europe
Implementation	Data Protection and Cybercrime Division (Directorate General of Human Rights and Rule of Law, Council of Europe)
Target countries	Albania, Bosnia and Herzegovina, Croatia, Montenegro, Serbia, "The former Yugoslav Republic of Macedonia", Turkey and Kosovo*
Final beneficiaries	Media, civil society and general public in the Beneficiaries and international justice and human rights professionals and organizations worldwide
Project partners	France (Ministry of Interior), Italy (Postal and Communication Police Service), Romania (Prosecution Service and National Police), Slovenia (Criminal Police), University College Dublin (Ireland)

[6] Original duration: 24 months (1 November 2010 – 31 October 2012)

The objective and expected results of the project are:

Objective	To strengthen the capacities of criminal justice authorities of Western Balkans and Turkey to cooperate effectively against cybercrime
Result 1	Cybercrime policies and strategies: Policy- and decision-makers are aware of cybercrime threats and human rights implications and have reached agreement on strategic priorities regarding cybercrime for Western Balkans and Turkey
Result 2	Harmonisation of legislation: Amendments are drafted to bring relevant legislation fully in line with the EU acquis, in particular the Convention on Cybercrime (CETS 185) and its Protocol on Xenophobia and Racism (CETS 189), and thus ensure harmonisation of legislation within Western Balkans and Turkey
Result 3	International cooperation: Enhanced regional and international law enforcement and judicial cooperation against cybercrime based on Chapter III of the Budapest Convention on Cybercrime
Result 4	LEA training: Law enforcement training strategy agreed by Ministries of Interior and implementation initiated
Result 5	Judicial training: Judicial training on cybercrime and electronic evidence integrated into the curricula of training institutions for judges and prosecutors
Result 6	Financial investigations: Capacities of financial investigators, Financial Intelligence Units (FIU), and/or relevant law enforcement units in charge of fighting against cyber criminals in following crime proceeds on the internet improved and their cooperation with the financial sector strengthened
Result 7	LEA-ISP cooperation: Cooperation between law enforcement and Internet service providers (ISPs) in investigations related to cybercrime strengthened
Result 8	Assessments: 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

3 Assessment of implementation

The CyberCrime@IPA project started on 1 November 2010. The first progress report was submitted and approved in October 2011. Following the progress report an interim report and the financial report were submitted in December 2012 including activities until the end of October 2011.

This present report summarises the activities implemented under the CyberCrime@IPA project between 1 November 2011 and 31 May 2012.

The following activities were carried out during the reporting period:

Date	Place	Activity
8-10 November 2011	Rome, Italy	Participation in the G8 Training Conference for 24/7 Points of Contact
21-25 November 2011	Strasbourg, France	Octopus Conference and Cybercrime Convention Committee (T-CY) meeting.
21/23 Nov 11	Strasbourg, France	International training meetings for 24/7 points of contact and high-tech crime units with regard to international law enforcement cooperation and information exchange (workshop in the Octopus conference)
16 December 2011	Zagreb, Croatia	Visit to Judicial Academy to discuss the establishment of the Pilot Centre on Judicial Training
27 January 2012	Belgrade, Serbia	Country Specific Workshop on Legislation
January – October 2012	Strasbourg	Development of a guide on electronic evidence in cooperation with the global Project on Cybercrime (draft to be discussed in the Octopus Conference 2012)
14-15 February 2012	Paris, France	1st Expert Meeting for developing a Guide on Electronic Evidence
20-24 February 2012	Zagreb, Croatia	Train the trainers regional course (Judiciary and Prosecution)
27-29 February 2012	Kyiv, Ukraine	Intra-regional conference on Money Flows in the Internet
26 March 2012	Sarajevo, Bosnia and Herzegovina	Country Specific Workshop on Legislation
28-29 March 2012	Skopje, "The Former Yugoslav Republic of Macedonia"	"Regional Workshop on Handling International Cooperation requests relating to Cybercrime"
30 March 2012		3rd Steering Committee Meeting
11-13 April 2012	Zagreb, Croatia	Basic In-country training on Cybercrime and Electronic Evidence for Judges and Prosecutors in Croatia
16-18 April 2012	Tirana, Albania	Basic In-country training on Cybercrime and Electronic Evidence for Judges and Prosecutors in Albania
19-21 April 2012	Pristina, Kosovo*	Basic In-country training on Cybercrime and Electronic Evidence for Judges and Prosecutors in Kosovo*
23-25 April 2012	Skopje, "The Former Yugoslav Republic of Macedonia"	Basic In-country training on Cybercrime and Electronic Evidence for Judges and Prosecutors in "The Former Yugoslav Republic of Macedonia"
26-28 April 2012	Podgorica, Montenegro	Basic In-country training on Cybercrime and Electronic

		Evidence for Judges and Prosecutors in Montenegro
2-4 May 2012	Ankara, Turkey	Basic In-country training on Cybercrime and Electronic Evidence for Judges and Prosecutors in Turkey
9 May 2012	Sarajevo, Bosnia and Herzegovina	Meeting with the members of the Team for tracking of the Implementation of legislation in Bosnia and Herzegovina to discuss amendments to cybercrime legislation
9-11 May 2012	Banja Luka, Bosnia and Herzegovina	Basic In-country training on Cybercrime and Electronic Evidence for Judges and Prosecutors in Bosnia and Herzegovina
15-16 May 2012	The Hague	Participation in the ECTEG Meeting
17-19 May 2012	Belgrade, Serbia	Basic In-country training on Cybercrime and Electronic Evidence for Judges and Prosecutors in Serbia
29-30 May 2012	Wiesbaden, Germany	2nd Expert Meeting for developing a Guide on Electronic Evidence

3.1 All expected results: Participation in the Octopus Conference and the Cybercrime Convention Committee (Strasbourg, 21-25 November 2011)

3.1.1 The Conference[7]

Cybercrime experts representing countries from all continents, international organisations and the private sector met at the Council of Europe to review the global cybercrime situation, to share experience on effective responses and to enhance cooperation against cybercrime at all levels. On the occasion of the 10th anniversary of the Budapest Convention (23 November), the Conference included a special session on the impact of this treaty. Senior representatives of Australia, the European Union, Hungary, the United Kingdom and the USA expressed strong support for global implementation of this Convention. Experts from Argentina, Senegal, Sri Lanka, Tonga and the private sector underlined its impact and potential in different regions of the world.

Three representatives from each of the project areas were funded by the Cybercrime@IPA project to participate in the Octopus Conference.

Among the key messages resulting from plenary and workshop discussions are:

- The challenge of cybercrime continues to increase. It is a transversal threat affecting people and their rights, generating large amounts of crime proceeds, causing major damage, and targeting economic, social, economic and security interests of societies worldwide. Cybercrime should, therefore, be considered a priority concern by all, including by decision-makers in parliaments and governments.

- Technical assistance helps build the capacities of countries to implement standards, tools and good practices already available. Progress was made since 2010 in that new technical assistance programmes have been launched by different organisations. More programmes are required to support countries in all regions of the world.

7 http://www.coe.int/t/dghl/cooperation/economiccrime/cybercrime/cy_Octopus_Interface_2011/Interface2011_en.asp .

- International organisations should reinforce their cooperation with each other to provide a better service and more coherent support to societies worldwide. Technical assistance programmes are conducive for such partnerships.

- Comprehensive legislation, harmonized with international standards is a key element of the response to cybercrime. The Budapest Convention serves as a guideline in this respect. Progress was made in many countries around the world since Octopus 2010. Nevertheless, the pace of adopting legislation must be accelerated.

- Responses to the sexual exploitation of children include criminal law measures. The Convention on the Protection of Children against Sexual Exploitation and Sexual Abuse (CETS 201) and the Cybercrime Convention (CETS 185) of the Council of Europe provide benchmarks.

- Specialised cybercrime units at the level of police-type agencies but also prosecution services allow for the effective investigation and prosecution of offences against and by means of computers and the forensic analysis of electronic evidence related to any crime. Good practices are available and have been documented.

- Cybercrime strategies – aimed at crime prevention and criminal justice – may help ensure a comprehensive response to cybercrime and other offences involving electronic evidence. They can provide a framework for a range of different measures and the participation of multiple public and private sector stakeholders. They should be closely linked to cybersecurity strategies.

- Law enforcement needs to be provided with the powers necessary for effective investigations, but such powers need to be subject to conditions and safeguards as foreseen in Article 15 of the Budapest Convention.

- The future of international cooperation against cybercrime depends to a large extent on the effective implementation of already existing standards and tools, on the removal of obstacles preventing efficient cooperation at all levels, including with respect to public-private as well as international information exchange, and the level of engagement of decision-makers.

The update session provided updates on:

- Threats and trends of cybercrime (Symantec)
- The scale of online sexual exploitation and abuse of children (Interpol)
- Threat assessment of Europol
- The state of information security in Europe (ENISA)
- The role and responsibility of CERTs (CERT-LEXSI)

The session underlined the scale and impact of cybercrime and thus the need to enhance cooperation at all levels. Decision-makers need to be made aware and need to be become more engaged in devising and adopting criminal justice and other responses.

Discussions confirmed the progress made in many countries towards cybercrime legislation and the use of the Budapest Convention as a guideline.

Workshop 1: Capacity Building

The workshop provided an overview of the capacity building activities in the fields of judicial training, law enforcement in different participating countries as well as of the technical assistance delivered by the Council of Europe, European Union, the initiative of the Commonwealth and capacity building activities by the UNODC.

In the context of the Global Project on Cybercrime of the Council of Europe and the joint projects with the European Union (CyberCrime@IPA and CyberCrime@EAP), the following aspects were underscored:

- Implementation of different projects needs to consider also raising awareness among policy makers and legislators about the need to take measures against cybercrime.
- Technical assistance requires work at different levels and with all institutions responsible in order to make a sustainable impact. This is also beneficial for inter-agency cooperation.
- Sustainable training should be available for police, prosecutors and judges as well as for agencies dealing with anti-money laundering and financial investigations.
- Setting up regional pilot centres for judicial training is a good practice and provides a good basis for a better regional and global cooperation.
- Sharing good practices and tools have provided great benefit for countries.

Workshop 2: Specialised services

The workshop examined the issues faced in the development of specialised law enforcement cybercrime units and the 24/7 points of contact provisions and requirements as set out in Article 35 of the Budapest Convention. The workshop discussed case studies that highlighted some of the challenges of dealing with cross-jurisdictional malware investigations and the good practice study on specialised units conducted under the CyberCrime@IPA and the Council of Europe global Project on cybercrime (Phase 2) projects.

The aim of the good practice study on specialised cybercrime is to help countries to establish or strengthen such units as a key element of the response to cybercrime. The study focuses on specialised units within police; however it is recommended that prosecution departments create their own units to deal with cybercrime. The study provides examples of different types of units.

The following recommendations were made that are relevant for the implementation of the Cybercrime@IPA project:

- Emphasis should be made on the importance of cascading knowledge and skills across law enforcement in order that responsibility for investigations may be spread more efficiently.
- Continue the support for creating effective 24/7 points of contact with particular emphasis on the importance of organisations being nominated rather than individuals. The organisation should be responsible for managing access to individuals. Regular checks on the 24/7 points of contact list should be made by the Council of Europe to ensure that redundant information is not present, as well as ensuring the effectiveness of the network of contact points. Countries should also be encouraged to use the 24/7 regime in advance of the issue of letters rogatory; as well as a resource for identifying experts within country.
- Countries should also consider developing 24/7 processes such as appropriate contacts with industry, CERTS and other relevant public/private parties on that basis.

Workshop 3: Cyber Crime Strategies

The workshop discussed the cybercrime strategies and provided an overview/comparison of how cybercrime strategies and cybersecurity strategies interact in the effort of governments and private sector to tackle cybercrime.

An overview of cybercrime and cybersecurity strategies draft paper[8], common areas and specificities was presented.

The workshop made the following recommendations:

- Increased cooperation between the governments, NGOs and private sector in the establishing and implementing the cybercrime and cybersecurity strategies.
- Increased cooperation through public private partnerships as well as improved cooperation between players in the private sector
- Enhance cybercrime components within cybersecurity strategies.
- Mainstreaming of law enforcement response to cybercrime.
- Through the Global Project against Cybercrime and other projects, the Council of Europe will continue to support countries in their efforts to tackle cybercrime through the establishment of effective cybercrime strategies.

Workshop 4: Responses to the sexual exploitation of children

The workshop examined the legislative, technological impacts and limitations (that is, notice and take down) and preventive aspects of the responses to sexual exploitation of children.

The Council of Europe together with INTERPOL, European Commission, Virtual Global TaskForce, International Center for Missing and Exploited Children, European NGO alliance for child safety online, Association des Fournisseurs d'Acces at de Service Internet, InHope and Microsoft all agree on the importance of developing and harmonising national legislations in place with the relevant international legal instruments.

Panel: Article 15 – protecting you and your rights in cyberspace

The panel explained the purpose and requirements of article 15 on conditions and safeguards of the Budapest Convention on Cybercrime. The report on the Internet case law of the European Court of Human Rights illustrated that this case law is a valuable resource also for non-European countries.

Article 15 specifically mentions that State Parties should provide for the protection of human rights and liberties pursuant to obligations undertaken by ratifying the 1950 CoE convention for the Protection of Human Rights and Fundamental Freedoms, the 1966 United Nations International Covenant on Civil and Political rights and other applicable international human rights instrument. The most pertinent article from the European Convention on Human Rights relating to the implementation of Article 15 of the Convention on Cybercrime are Article 8 (protection and retention of personal data falling within private life) and Article 10 (right to hold opinion without interference, right to freedom of expression, freedom to seek, receive and impart information), a structured approach to these two articles provides for key safeguards against state interference. It was agreed that questions related to Article 15 should be addressed in capacity building programmes.

[8] http://www.coe.int/t/DGHL/cooperation/economiccrime/cybercrime/Documents/Reports-Presentations/2079_cy_strats_rep_V23_30march12.pdf

Panel: Cooperation against cybercrime – what future

The panel focused in particular on the cooperation between public and private sector entities and the need for a holistic approach to tackling cybercrime. While governments are tackling cybercrime with the goal of protecting citizens against crime, the interest of the private sector in investing in the fight against cybercrime is the protection of their businesses and customers. Complementary of interests favours cooperation.

One of the best ways for expedited international cooperation is the use of the 24/7 network of contact points. However, there is a great number of countries that are not yet members of the network.

European Union member states have established several mechanisms for cooperation and the European Commission is currently establishing an European Union Cybercrime Centre. Although this centre is being created for member states, third countries may also benefit from the coordinated effort of European Union countries.

It was agreed that there is a need for increased cooperation between the many stakeholders including the consideration of public-private partnerships. Panellists called on the private sector to increase their support for initiatives undertaken by the public sector to tackle cybercrime. While some major companies are very much involved already, other major private sector players seem to lack engagement.

3.1.2 Sixth Plenary of the Cybercrime Convention Committee (T-CY) (Strasbourg, 23-24 November 2011)

The meeting discussed:

- Results from technical assistance/capacity building Programmes. In this context, it took note of the results achieved under the technical assistance programme, including the joint projects of the Council of Europe and the European Union on cybercrime i.e. CyberCrime@IPA and CyberCrime@EAP.
- Established an ad-hoc sub-group of the T-CY on jurisdiction and transborder access to data and data flows. Two representatives of the project teams (Serbia and ‘’The Former Yugoslav Republic of Macedonia’’) are members of the group.
- Compliance by Parties with Article 35 of the Convention on 24/7 points of contact.
- Effective implementation of the Budapest Convention by the Parties: provisions to be reviewed in 2012.
- Priorities and workplan of the T-CY for the period 1 January 2012 – 31 December 2013.
- Accession criteria and procedure under Article 37 of the Convention on Cybercrime.
- State of ratification, signatures and accession to the Convention and its Protocol.

Mr. Branko Stamenkovic (Serbia) was elected member in the T-CY Bureau ensuring the representation from IPA region in the work of the Bureau, including a greater involvement in the decision-making process of the T-CY.

3.1.3 Follow up

- Considering the prestige and recognition of these events, the broad level of representation and the relevance of the topics discussed, the Cybercrime@IPA project to continue to support the participation of project areas in the next Octopus Conference (6-8 June 2012, Strasbourg, France) and in the Cybercrime Convention Committee (4-5 June 2012).

3.2 All expected results: 3rd Steering Committee Meeting (Skopje, "The former Yugoslav Republic of Macedonia", 30 March 2012)

Participants: European Union Delegation to "The Former Yugoslav Republic of Macedonia (Danica Stoshevska), Council of Europe, and partners in the project (Romania, France).

An overview of the status of the implementation of the Cybercrime@IPA project was provided. In this context, the recommendations of the Monitoring Report (MR-143002.0125/11/2011) were discussed.

The Report stated that the project is performing well with some results already achieved. It made the following recommendations:

1. To consider if a baseline and target level can be provided for the Objectively Verifiable Indicators (OVIs) for mutual assistance requests in Result Area 3. If not possible, the indicator should be redefined;
2. In consultation with the beneficiaries, further develop the actions needed at national level by separating those required before completion of the project from those that will be delivered later, setting milestones for achievement and by identifying who is responsible for implementing the activities;
3. To address the strong recommendation in the situation report on the establishment of a small set of statistics for regional Cybercrime by reference to available international references on this subject. This should be taken up in future project activities under Result Area 3;
4. To include a summary of the use of financial and human resource inputs in the six monthly progress reports.

In this context, the project management underlined the importance of gathering statistics on cybercrime cases, including the number of requests on international cooperation received/sent and the number of requests dealt by the 24/7 points of contact. Such information is extremely relevant for designing any cybercrime strategy as well as for providing targeted training on cybercrime.

Representatives from the project areas informed about the difficulties of gathering such statistics and various approaches taken e.g. while in Croatia a specific project is likely to solve this problem in other countries this issue is not currently addressed.

3.2.1 Follow-up activities

- Establish a judicial training pilot centre in Croatia: A visit to Croatia will be organised to discuss with Judicial Academy the next steps.
- Eight basic in-country trainings (in each project area) on cybercrime and electronic evidence for judges and prosecutors will be organised between April and May 2012.
- The Octopus Conference: Cooperation against Cybercrime (Strasbourg 6-8 June 2012). Four participants will be covered from the CyberCrime@IPA project.
- Cybercrime Convention Committee (T-CY) Plenary Session: Four additional countries nominated representatives in the T-CY (Albania, Montenegro, Serbia and "the former Yugoslav Republic of Macedonia"). Turkey informed that the Ministry of Foreign Affairs is currently working on ratification of the Cybercrime Convention. The expected ratification should be done within the lifetime of the project
- The working group on judicial training should be prepared to follow up on finalising the training material (basic and advanced) and support their implementation by training institutions.

- Preparation of additional tools and guidelines: Guide on electronic evidence in cooperation with the global Project on Cybercrime. It was agreed to organise a workshop on electronic evidence on 4-5 September 2012 in Skopje to discuss the document.
- Application for ECTEG (European Cybercrime Training and Education Group) training materials and ECTEG membership. The remaining project areas were encouraged to apply for membership emphasising the importance and the benefits from participating in such meetings and obtaining training materials provided by ECTEG.

3.2.2 Adoption of the revised workplan

- Participants agreed on the revised workplan (see appendix).

3.3 Result 2 – Harmonisation of legislation: Country-specific workshop on legislation for Serbia (Belgrade, Serbia, 27 January 2012)

3.3.1 The workshop

Based on these findings and the recommendations made in the Situation Report and following the discussions in the Regional Workshop on legislation (Sarajevo, Bosnia and Herzegovina, 24-25 May 2011) during the 2nd Steering Committee meeting, Serbia requested a specific event on legislation to discuss possible amendments.

Representatives of Ministry of Justice, Ministry of Interior, Parliament, judges, prosecutors and representatives of the Judicial Academy participated in the workshop. Experts from Belgium, France and the Netherlands contributed to the event.

The Workshop resulted in the following:

- Provided legal advice to the Serbian authorities with regard to the provisions that require further consideration to adequately implement the Budapest Convention and the EU standards.
- Discussed challenges in implementation of the Budapest Convention Cybercrime providing good practices.
- Participants drafted recommendations to be considered in the process of reviewing of the Serbian legislation.

During discussion the Assistant Minister of Justice of Serbia, Mr Slobodan Boskovic confirmed the commitment of the Serbian authorities in the fight against cybercrime. The establishment of the Specialised Prosecutors Office to deal with High Tech Crime as well as the amendments to the legislation to implement the Convention on Cybercrime attest this commitment. The contribution from Serbia is recognised by the international partners and the election of the Head of the Specialised Prosecutors Office on High Tech Crime as member of the Bureau of the Cybercrime Convention Committee (T-CY) is an example.

The Council of Europe underlined the objectives of the Joint EU/CoE joint project on Cybercrime and the importance given to the harmonisation of the legislation in the region. From this perspective Judicial Academy, which is responsible with judicial training for judges and prosecutors, is an excellent venue to host such discussion.

The workshop focused on the analysis of the Serbian legislation in view of fully implementing the Convention on Cybercrime and related international standards, concluding the following:

- Article 3 (Illegal Interception) - articles 298 and 302 of the Criminal Code do not adequately implement this article. In addition, separate provisions are needed to criminalise illegal access and illegal interception.
- Article 4 (Data Interference) and Article 5 (System Interference) – the two articles aim at protecting different legal interests and thus separate criminalisation is recommended.
- Article 6 (Misuse of device) - Serbian legislation criminalise the act of making virus. Such approach is too limited and narrow since it does not cover all the malware. In addition to software there are devices that can be misused for the commission of cybercrimes. Article 6 in the Budapest Convention also refers to access codes. This article is very important since it deals with the distribution of malware on the Internet. Therefore the provisions relating to article 6 need to be broad.
- Article 7 - Computer related forgery - There is no implementation of Article 7 in Serbian legislation. Article 355 of the Criminal Code relates to forgery of physical documents and not to electronic documents. The only way to treat computer files is if the electronic forgery is considered as preparation to commit an offence in relation to article 355.
- Article 8 – Computer related fraud - Countries encounter difficulties in the implementation of the computer fraud mainly because traditional criminal law refers to defrauding a person and does not foresee that a computer could be defrauded. Article 301 in the Serbian legislation satisfies the requirements of Article 8 of the Convention.
- Article 9 - Offences related to child pornography - Serbia criminalised child pornography in Article 185; however one important element was left out related to "realistic images representing a minor engaged in sexually explicit conduct". There may be a need to reconsider the provisions in the Serbian legislation. Serbia has ratified the CETS 201 (Lanzarote Convention) and there are additional requirements/standards to be implemented. A definition of child pornographic material is still missing.
- Article 12 Corporate liability - Serbian legislation provides only for sanctions by imprisonment. This is limiting and there may be a need to make amendments to include fines for legal persons and not only the individuals that have committed an offence. It is recommended that legal entities are also held liable for crimes that are committed on behalf of the legal entity. Paragraph 2 of Article 12 of the Convention clearly states that it should be possible that legal persons to be held liable and this liability may be criminal, civil or administrative.

With regard to the procedural law:

- Article 15 (Conditions and safeguards). This provision is very important but is left to domestic legislation to establish such safeguards. Article 15 refers to the obligations a country has undertaken when implementing international treaties such as the European Convention on the Protection of Human Rights and Fundamental Freedoms (CETS 005).
- Article 16 (Expedited preservation of stored computer data); Article 17 (Expedited preservation and partial disclosure of traffic data); Article 16 and Article 17 of the Convention are not fully implemented in the Serbian legislation. According to the representatives from Serbia, the country has established a working group to discuss the future amendment of the Criminal Procedure Code, which will include implementation of these articles. The Serbian law on electronic communications regulates data retention by the ISPs who are obliged to keep the data for one year. To disclose this data there is a need for a request from competent authorities based on a court warrant. All definitions relating to the ISPs and to the powers of the authorities are included in this law and are in compliance with the Convention.
- Article 18 (Production order) - The new Serbian Criminal Procedure Code includes provisions on production order concerning any offence. Article 82 of Serbian Criminal Procedure Code can be used for this purpose. Police can search and seize items, but citizens can decide to provide items voluntarily.

- Article 19 (Search and seizure of stored computer data) - In Serbian legislation there is no need for a court order to search of a specific computer. Police use a warrant to search a building and all equipment within the premises can be sent to the forensic department for analysis.
- Article 20 (Real time collection of traffic data) - Article 20 of the Budapest Convention is not implemented as the country has a data retention system. However there is still room for the implementation of this provision.
- Article 21 (Interception of content data) - Articles 166-170 in the new Criminal Procedure Code[9] deal with lawful monitoring/interception of communications. This includes secret monitoring of communication/ following and recording, controlling delivery, undercover investigations etc. The new Criminal Procedure Code provides for the real time monitoring of computer communications, recording of this communications etc.

Recommendations made by the Serbian delegation

- Include in the Serbian law a new criminal offence - computer forgery. In article 300 of the Criminal Code to establish as an offence production and the use of malware.
- Include in article 112 the definition of the term "child pornography."
- Amend article 185 with offences related to the production of animations which represent minors in explicit conduct with a sexual connotation.
- Within the law on electronic communications of Serbia in the article that deals with the meaning of terms to consider the definition of ISP.
- Concerning procedural law include provisions on expedited preservation of traffic and content data.
- Consider more precisely the provision for court order in relation to the submission and seizure of specific data instead of seizure of the entire computer.
- It is also necessary to provide fines for individuals who do not comply with such court order.

3.3.2 Follow up:

- The new Criminal Procedure Code to be reviewed from the perspective of its compliance with the Convention on Cybercrime.
- Subsequently, the project to submit to the Serbian project team recommendations for amendments to the legislation by considering the conclusions of the legal review and the detailed discussions in the workshop.

[9] The new Criminal Procedure Code will enter into force on 15 January 2013

3.4 Result 2 – Harmonisation of legislation: Country-specific workshop on legislation for Bosnia and Herzegovina (Sarajevo, 26 March, 2012)

3.4.1 The workshop

Bosnia Herzegovina ratified the Cybercrime Convention and its Additional Protocol on Xenophobia and Racism on 19 May 2006. On 12 November 2011 Bosnia Herzegovina signed the Convention on the Protection of Children against Sexual Exploitation and Sexual Abuse.

The Situation Report prepared in the beginning of the project, 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 and made recommendations for improvement. During the 2nd Steering Committee meeting (Budva, Montenegro, 12 September 2011), the delegation of Bosnia and Herzegovina confirmed the previous request for a country specific workshop on legislation.

The specific Workshop on legislation took place in Sarajevo on 26 March 2012 and it was aimed at providing further assistance on cybercrime legislation to the country. The meeting was attended by Representatives of Ministry of Justice, including the State Secretary of this Ministry Mr. Jusuf Halilagic, members of the TEAM for tracking of the implementation of criminal legislation in Bosnia and Herzegovina, representatives from the Ministry of Security, representatives from the entities (Ministry of Interior of the Federation of Bosnia and Herzegovina, Ministry of Justice of Republika Srpska and representatives from the Brcko District), prosecutors, judges etc.

The Workshop resulted in the following:

- Provided additional legal advice to Bosnia and Herzegovina on the provisions that require further reform to implement the Cybercrime Convention and the European Union standards.
- Discussed challenges in drafting amendments considering the fact that in Bosnia and Herzegovina different criminal codes and criminal procedure codes are enacted.
- Provided good practices from the Netherlands, Belgium, as well as private sector.

Mr Jusuf Halilagic, State Secretary, the Ministry of Justice, attended the whole event. He emphasised the importance of the Project and the support given to Bosnia and Herzegovina to increase its capacities in the fight against cybercrime. The country had asked for legislative support and thus this event is very useful, in particular by bringing in a high level of expertise and experience in the field.

The Council of Europe underlined the importance of the project, which provides a consistent and comprehensive assistance for the region in tackling cybercrime. The project countries should fully explore this opportunity. The interest at decision-making level in Bosnia and Herzegovina for the project activities was welcomed.

The workshop reviewed the gaps identified at state, entities and district level and discussed possible amendments to the legislation.

3.4.2 Follow up:

- Participate in the next meeting of the TEAM for tracking the implementation and harmonisation of legislation in Bosnia and Herzegovina (9 May 2012) to discuss the approach to draft amendments.

- A document with specific recommendations to be prepared by the project, translated and submitted for consideration to the TEAM for tracking the implementation and harmonization of legislation in Bosnia and Herzegovina.

3.5 Result 2 – Harmonisation of legislation: Meeting with the Team for tracking of the Implementation of legislation in Bosnia and Herzegovina (Sarajevo, 9 May, 2012)

3.5.1 The meeting

The aim of the meeting was to support measures for harmonising cybercrime legislation among the entities', district and state level. Mr Jusuf Haligalic, State Secretary, Ministry of Justice and Chair of TEAM opened the meeting.

The representatives of the Council of Europe provided information on the activities related to legislation organised under the CyberCrime@IPA project, including the in-depth analysis of the current legislative gaps in Bosnia and Herzegovina and the recommendations made. It was underlined that the discussion should focus on major problems identified in the legislation since detailed explanations are available in different reports drafted under the project.

It resulted that most of the members of TEAM were not fully aware of these reports and requested that the country profile to be completed with additional information on international cooperation and mutual legal assistance.

Mr Mato Tadić, judge at the Constitutional Court, made proposals for two possible options to be taken in order to harmonise and amend cybercrime legislations, namely:

- Option 1: Amend the Criminal Code at State level with offences including international characteristics and thus the entities and the district will have to amend their cybercrime legislations accordingly.
- Option 2: Prepare a set of recommendations to be submitted to the Committees of Ministers for approval; subsequently, amend the cybercrime legislation at the entities and district levels.

The Council of Europe expert suggested that the State could set standards by drafting model laws which then would have to be implemented at the level of both the entities and the district.

The roundtable resulted in the following:

- the project team will review the legislative country profile of Bosnia and Herzegovina;
- the TEAM will study and consider the recommendations of the Report on harmonisation of legislation;
- the TEAM will examine possible approach to draft amendments of the cybercrime legislation.

3.5.2 Follow up

- The project will provide further support to the Ministry of Justice of Bosnia and Herzegovina on drafting amendments by providing legal advice and examples of implementation from other countries.
- The project will support the participation at the next meeting of the TEAM for monitoring the implementation of legislation in Bosnia and Herzegovina, which will take place in July 2012.

3.6 Result 3 - Enhanced regional and international cooperation: Participation in the G8 Training Conference for 24/7 Points of Contact (Rome, Italy, 8-10 November 2011)

3.6.1 The Conference

Article 35 of the Convention on Cybercrime, which provides for the creation of the 24/7 network, was inspired by the network established within the G8 High-Tech Crime Sub-Group in 1997. It envisages that the contact points will ensure immediate assistance in investigations and proceedings concerning criminal offences related to computer systems and data and action is taken to ensure that data and evidence is not lost or altered during the time that formal procedure for MLA is executed.

Therefore, ensuring training to increase the efficiency of the 24/7 points of contact is an important element for an efficient international cooperation against cybercrime. Several activities under the project focused on this issue e.g. regional workshops in Dubrovnik and Budva, as well as international workshop in the Octopus Conference (Strasbourg, 21-23 November 2011).

The "Third Training Conference for 24/7 Points of Contact for High Tech Crime Emergencies" was organised by the G8 and hosted by the Italian Police. The event provided opportunities for networking between the two networks and among each other.

It discussed challenges in the work of the 24/7 points of contact as well as new trends in the field of cybercrime. The G8 Sub-Group on High-Tech Crime presented the newly developed secure web server which would provide for better and more efficient communication between the 24/7 points of contact which are members of the network. Following the presentation the organisers distributed security tokens to the members of the network.

A number of experts representing various governmental institutions and international organisations made presentations during the training on various topics related to international cooperation, new trends and modus operandi used by offenders etc.

Mr Santi Giuffre, Central Director of the Italian Police, stressed the importance of the international cooperation and joint action against cybercrime. He mentioned that this conference precedes the 10th anniversary of the Budapest Convention on Cybercrime, which is a tool that unifies the efforts to combat cybercrime. There is a need for sustainable efforts from the governments to fight against cybercrime. The ultimate goal of successfully combating cybercrime can be achieved only by having a joint approach with harmonised laws and regulations and the Budapest Convention on Cybercrime is an important tool in this respect.

Mr Thomas Dukes, US Department of Justice underlined the need to increase the number of member countries in the network as a response to the growing number of cybercrimes that occurs globally. The 24/7 network is one of the means that can be used to combat cybercrime, especially for fast exchange of data. He mentioned also the important role played by the Convention on Cybercrime to harmonise legislation worldwide.

Mr Sergio Staro, Italian Police, presented the G8 network within the Sub-Group on High Tech Crime and the Cybercrime Convention 24/7 network of contact points, established in accordance with Article 35 of the Budapest Convention on Cybercrime. These networks are additional tools to be used in fighting cybercrime and important elements in the international cooperation. However, there is a need

for expanded efforts and support from the private sector which is a key player in the fight against cybercrime.

A number of presentations were made by different speakers on:

- Convention on Cybercrime and the role of the 24/7 network under Article 35.
- Synergies and role of the 24/7 networks of the Convention and the G8.
- The role of Interpol in the international cooperation against cybercrime and the contribution of the national Central Reference Points Network.
- UNODC efforts against cybercrime.
- Examples of successful international cooperation involving the 24/7 points of contact (Case study on the halting of the coreflood botnet).
- Presentation of the secure web-server for communication between the G8 24/7 points of contacts.
- Technical presentations on:
  - the exploitation of the DNS (Domain Name Service);
  - Actions against the botnets;
  - Search and seizure, best practices and forensic tools (presentation by 3 countries);
  - Tracking the origin of communications (presentation by 3 countries).

The conference provided a good opportunity for networking among the members of the G8 and the Cybercrime Convention 24/7 networks. Over 60 countries are members of the two networks and more are expected to join.

3.6.2 Follow up:

- Promote the 24/7 networks in order to increase the number of member countries
- Ensure that current members are responding to the requests sent by their counterparts. For this purpose there should be frequent ping tests for testing the responsiveness and effectiveness of the two networks.
- The 24/7 points of contact of the two networks will further discuss and interact during the international workshop organised in the Octopus Conference (Strasbourg, 21-23 November 2011).

3.7 Result 3 – Enhanced regional and international cooperation: Regional workshop on handling international cooperation (Skopje, "The former Yugoslav Republic of Macedonia, 28-29, March 2012)

3.7.1 The workshop

Expected Result 3 is related to international cooperation:

> Enhanced regional and international law enforcement and judicial cooperation against cybercrime based on Chapter III of the Budapest Convention on Cybercrime

Under this result the project will support measures to enhance the regional and international cooperation against cybercrime in the project areas by increasing the efficiency of the 24/7 points of contact and of the authorities responsible for mutual legal assistance (MLA).

The project has already organised several activities that identified areas for improvement and further assistance. For instance:

- Training of practitioners in handling international cooperation requests;
- Establish best practices for joint investigations and successful cooperation;
- Provide examples of the format of request letters and a list of competent authorities to handle these requests etc.;
- Provide guidance in cooperation with specific countries (e.g. USA, UK).

The aim of the Regional Workshop on international cooperation was 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.

Participants in the event were representatives of the Ministries of Justice and prosecution services from the areas participating in the Cybercrime@IPA project. In addition based on the discussions in previous activities, a number of experts from Belgium, France, Romania United Kingdom, USA and the private sector were invited to share experience and good practices.

The main achievements of the workshop are:

- Provided and overview of the progress made under the project with regard to international cooperation.
- Presented practical examples of successful cooperation between countries.
- Presented cases of success and failure in the cooperation with the private sector.
- Discussed channels for international cooperation, in particular the 24/7 network and Southeast European Law Enforcement Center (SELEC).
- Each delegation prepared a set of recommendations for measures to be taken in their respective country/area.

In the opening session Mr Marko Zvrlevski underlined the importance of the Cybercrime@IPA project in supporting the countries in their efforts to increase the capacity of the countries to fight cybercrime. Cybercrime is a type of crime that is being taken seriously in the country and in the region. The objective of the workshop is to discuss the ways of expediting the cooperation between the countries to effectively investigate and prosecute cybercrime.

Mr Lukas Melka addressed the participants on behalf of the EU Delegation to "The Former Yugoslav Republic of Macedonia". Mr Melka pointed out the fast development of technology and the spread of the use of ICT in the world. Although these technologies provide great advantages to the human kind, unfortunately there are people that abuse the ICT for their interests. Cybercrime as a new type of crime poses new challenges to the authorities, especially considering its global spread and nature. The nature of cybercrime makes the investigation and prosecution difficult. The best way to fight cybercrime is to have a successful international cooperation and take coordinated measures.

The Council of Europe (Cristina Schulman) underlined the regional approach of the Joint EU/Council of Europe project Cybercrime@IPA to tackle cybercrime. The European Union and the Council of Europe joint their efforts to support the countries in the region. The project is producing results which are being promoted beyond the region through the other projects on cybercrime implemented by the Council of Europe. The general conclusion of the previous events was that international cooperation is not achieving the desired results; concerns were expressed about the delays in the cooperation with certain countries and/or with the private sector, in particular large companies based in the USA.

A number of experts presented in the sessions that followed. Mr Richard Downing (Deputy Chief, Computer Crime and Intellectual Property Section, Department of Justice, United States of America) focused on the procedure to be followed when requesting international cooperation from the USA, including practical suggestions for MLA requests. Most of the ISPs based in US might respond directly to requests for international cooperation by providing non-content information only. The most common reasons that can result in a negative or delayed response to a request from US are insufficient factual basis and insufficient support for particular facts. A successful case investigated by Romanian and the US authorities was provided as example of cooperation. This case resulted with the indictment of 22 people in Romania and the arrests of money laundering targets in the USA.

In addition, presentations in the workshop discussed:

- Experience of Belgium, France, Romania, United Kingdom and the USA.
- Recommendations for cooperation with the UK (Nick Vamos, Head of Central Authority Judicial Co-operation Unit) and France (Frederique Dalle, Deputy public prosecutor at the Magistrates' Court of Paris).
- International Cooperation: Possible solutions from the private sector perspective (Uwe Rasmussen, Senior Attorney, August & Debouzy). There are a number of initiatives from the private sector to assist law enforcement authorities e.g. Microsoft action against botnets, the Signal Spam initiative, anti-botnet initiative etc.
- Cooperation with the private sector: Belgium vs. Yahoo case showed that there are different approaches to international cooperation.
- An update on the 24/7 network of points of contact underlined the level of responsiveness of these points of contact in the latest ping tests.
- Regional and international channels that can facilitate cooperation in the region (e.g. SELEC)

Regarding cooperation with EUROJUST, two countries signed agreements, namely Croatia in 2007 (entry into force: 5 June 2009) and in 2008 ''The Former Yugoslav Republic of Macedonia'' (entry into force: 23 June 2010). Most of the other project areas are currently negotiating their membership.

The workshop included a presentation on the achievements of the European Union project - IPA 2008 Police Cooperation: Fight against Organised Crime, in particular Illicit Drug Trafficking, and the Prevention of Terrorism (DET-ILECUs II). The participants in the meeting interacted and exchanged views with the Project Manager.

The workshop concluded with a discussion on the future steps to be undertaken under the project to support the project areas.

Recommendations made by delegations:

Albania

- Increase the efficiency of the 24/7 contact point.
- Sign an agreement on cooperation with EUROJUST.
- Organising training courses on cybercrime, in particular for prosecutors, judges, Ministry of Justice personnel responsible with MLA requests.
- Standardisation of MLA requests.
- Develop training manuals, including a glossary of the terms the cybercrime field.
- Consider electronic communications on MLA between Parties to the Conventions.

Bosnia and Herzegovina

- Sign an agreement on cooperation with EUROJUST.
- Consider the possibility of standardising the forms of requests
- Establish a web-portal ("Center 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.
- Harmonisation of the legislation with the Budapest Convention on Cybercrime.
- Define and provide continuous training for representatives of judicial and police bodies with the goal of increasing the efficiency of international cooperation.

Croatia

- Each Party to the Cybercrime 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.
- Each Party to the Cybercrime 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

"The Former Yugoslav Republic of Macedonia"

- Improved internal and international cooperation to fight cybercrime, including good cooperation and use of the resources offered by GPEN.
- Intensive trainings at local level to increase the capacities of judges and prosecutors in handling cybercrime cases and electronic evidence.
- Maintain good cooperation and communication between the prosecution and the high-tech crime unit in the police.
- Improved communication with ISPs to provide for expedited cooperation and information sharing.

Turkey

- Challenge governments to speed up the ratification process of the Cybercrime Convention.
- Harmonisation of legislation according to the Convention.

- Upgrade and use an alternative standard form to provide a MLAT on cybercrime cases exclusively.
  Training of judges and prosecutors on using judicial assistance instruments effectively in cybercrime matters, especially focus on handling of electronic evidence in criminal investigation.

Kosovo*

- Bilateral agreements regarding regional cooperation.
- Training for judges, prosecutors and police related cybercrime.
- Increasing the cooperation with other countries on cybercrime.

3.7.2 Follow up

- The training manual on international cooperation to be developed under the project to include the information requested in the recommendation above.
- Continue the assistance to ensure adequate legislation and implementation of the relevant international treaties on cooperation in criminal matters.
- Support for the remaining project areas to join GPEN, EUROJUST, ECTEG etc.

3.8 Result 4 – Law enforcement training: Participation of representatives from project areas in the ECTEG Meeting (15-16 May, 2012, The Hague, Netherlands)

3.8.1 The meeting

The Cybercrime@IPA project under result 4 provides support participation of the beneficiary countries in various networks on cybercrime. In this context, under activity 4.1 the project at their request funded the participation of one representative from Turkey and one representative from "the Former Yugoslav Republic of Macedonia".

Currently, Croatia, "The Former Yugoslav Republic of Macedonia" and Turkey are ECTEG members. Kosovo* applied for membership during the implementation of the project and Serbia intends to apply.

The meeting provided an opportunity for participants to learn about the current activities of ECTEG, the available materials as well as the status on the discussions relating to current and future management of cybercrime training by CEPOL and ECTEG. In addition, the event provided useful information about the implementation of other EU projects which deal with cybercrime training such as the "Cybercrime Investigation - Developing and disseminating an accredited international training programme for the future" a project which is funded by the EC under the ISEC 2010 and is implemented by the Bundeskriminalamt (BKA) – Germany.

The representative from "the Former Yugoslav Republic of Macedonia" expressed during the project an interest in establishing a Centre of Excellence based on the 2CENTRE approach. The event was also a good opportunity to receive more information on the functioning of these centres.

3.9 Result 4 – Law enforcement training: Preparing a guide on electronic evidence

Under Activity 4.5: Organise at least three multi-disciplinary investigative training courses on case studies and new trends, techniques and technologies, the project undertaken to develop a Guide on electronic evidence in cooperation with the global Project on Cybercrime of the Council of Europe.

This document was requested in several activities organised under CyberCrime@IPA, as well as in a number of activities organised by the Council of Europe under other projects.

Five experts from UK, Germany and Spain were tasked to prepare a draft to be discussed in June 2012. For this purpose, two expert meetings (Paris, France, 14-15 February 2012 and Wiesbaden, Germany, 29-31 May 2012) discussed the document.

The Guide will provide an important tool for law enforcement and judges in their efforts to investigate, prosecute and adjudicate cybercrimes.

The purpose of the guide is to provide support and guidance in the identification, handling, and examination of electronic evidence. This guide has been prepared for use by countries that are developing their response to cybercrime and establishing rules and protocols to deal with electronic evidence. Most of the existing guides have been created for the law enforcement community. This guide is for a wider audience and includes judges, prosecutors and others in the justice system such as private sector investigators, lawyers, notaries and clerks.

Guide Structure and Content

- Introduction
- Evidence sources
- Data held by third parties
- Search and seizure + on site / suspect
- Dead Box
- Live Data Forensics
- Capturing evidence from the Internet
- Online Sources
- Covert Online Investigations
- Analysing evidence
- Preparation and Presentation of the Evidence
- Jurisdiction
- Role Specific Considerations
- Law Enforcement
- Prosecutors
- Judges
- Private Sector
- Case Studies
- Glossary
- Further Considerations
- Appendices

The draft document will be discussed during the Octopus Conference (6-8 June 2012) and in a specific event to be organise together with CyberCrime@EAP project in Skopje, "The Former Yugoslav Republic of Macedonia" on 4-5 September 2012.

3.10 Result 5 – Judicial training on cybercrime and electronic evidence: Training of trainers course (Zagreb, Croatia, 20-24 February 2012)

Expected result 5 is related to *judicial training*:

> Judicial training on cybercrime and electronic evidence integrated into the curricula of training institutions for judges and prosecutors

The approach of the project with regard to judicial training consists of the following:

- Development of basic and advanced training modules
- Training of trainers
- Integration of these modules into the initial and in-service training curricula of judicial training institutions
- Delivery of pilot courses in each project area
- Establishment of at least one pilot centre in the project region.

3.10.1 The Train the Trainers Course

A regional "Train the Trainers" course was held at the Judicial Academy in Zagreb, Croatia from 20 to 24 February 2012. The underlying course is entitled "Introductory Cybercrime and Electronic Evidence Training for Judges and Prosecutors".

Each project area was invited to send two delegates to the course[10]. This particular course was held for the trainers who in the future will deliver the course in their own countries/areas as part of the project and also as part of the national training programme. The requirements for nominating the participants were the following:

- Good level of knowledge of cybercrime issues/ trends and legal framework in their country of origin.
- Good command of English (the training was offered in English language only).
- Candidates agree to act as trainers in their respective countries based on the programme they attended.
- Candidates commit to continuing their cooperation with the training institutions, including after the closure of the Cybercrime@IPA project.
- Previous experience as trainers desired.

There was a balanced mixture of judges and prosecutors, with many countries sending one of each as delegates. The mix helped keep the course dynamic and should help the in country delivery.

The trainers for the course were Mr Nigel Jones and Ms Esther George from the UK. Both trainers have extensive experience in developing and delivering cybercrime training both in the UK and internationally with professional backgrounds in Law Enforcement and Public Prosecution.

Countries and areas in the IPA region have varying levels of cybercrime training incorporated within their national training programmes. This course for trainers was necessary in order to enable a standardised course to be delivered in the region and to provide additional skills for the trainers to be able to deliver the underlying course in their own countries.

[10] Bosnia and Herzegovina provided one student and the two students from the "Former Yugoslav Republic of Macedonia" were delayed by a cancelled flight and did not attend the first day of training

This course was designed to provide judges and prosecutors with an introductory level of knowledge on cybercrime and electronic evidence. The course provided legal as well as practical information about the subject matters and concentrated on how these issues impact on the day-to-day work of judges and prosecutors. By the end of the course judges and prosecutors acquired basic knowledge of cybercrime and electronic evidence, how they can deal with them, what substantive and procedural laws as well as technologies can be applied, and how urgent and efficient measures as well as extensive international co-operation may be taken. In addition this course provided delegates with skills to enable them to prepare and deliver presentations on the subject for their peers.

The course content consisted of the material to be delivered in each project area as well as training skills[11] to enhance the abilities of the delegates to deliver the underlying materials during the 3-day module in country.

All delegates participated fully in the course and provided clear evidence that they will be able to undertake their role as trainers for the in country training. The course gave them the opportunity to explore different methods of training delivery as well as the opportunity to practice their skills. Constructive feedback was provided to each delegate by the trainers and the other delegates.

The course was considered a success by the students and the trainers alike. The facilities for the course were provided by the Judicial Academy in a very professional manner.

The comments made by the students on their evaluation included:

- Very useful course, which provides excellent information about conducting trainings. Maybe to include one day more into the course since there is a lot of new and important information, preparing presentations etc. which would improve attention of participants
- It was a very good course
- It was very important for us to comprehend the material from top to the end
- Very useful in every day job
- One of the best training sessions. Well organised, well prepared and presented. Lead trainer outstanding
- Very interesting and useful.

3.10.2 Follow up

- Eight training events (one in each project area) based on the course will be delivered between April and May 2012.
- Based on the feedback from the ToT and the in-country trainings to update the content of the basic training module.
- Organise a regional workshop for the finalisation of the basic and advanced modules for judicial training in July 2012. The workshop will bring together the experts who contributed to the material, as well as the members of the working group and the participants in the ToT.

[11] The materials used in the training skills elements were created by Nigel Jones using background sources from an associate who had given permission for them to be used for this purpose

3.11 Result 5 – Basic in-country trainings on cybercrime and electronic evidence for judges and prosecutors

The course that was delivered in each country of the region[12] was designed to provide judges and prosecutors with an introductory level of knowledge on cybercrime and electronic evidence. The course provided legal as well as practical information about the subject matters and concentrated on how these issues impact on the day-to-day work of judges and prosecutors. By the end of the course judges and prosecutors acquired basic knowledge of cybercrime and electronic evidence, how they can deal with them, what substantive and procedural laws as well as technologies can be applied, and how urgent and efficient measures as well as extensive international co-operation may be taken.

Each of the courses was delivered in accordance with the aims and objectives set out by the project management during the "Train the Trainer" course. Countries made changes to the course content to meet local needs. Some also introduced guest presenters to support their delivery of certain technical materials.

The delivery of each course was in its own right a success and the trainers trained in Zagreb worked extremely hard to deliver the content that had learned as well as demonstrating the new training skills they had acquired.

There were several changes to delivery methods made by countries that enhanced the original product and will be included in the final version. In addition the observers also identified that improvements could be made to the way in which the underlying course was structured.

3.11.1 Course 1 (Zagreb, Croatia, 11-13 April 2012)

- Trainers: Kornelija Ivanusic and Ivan Glavic
- Observers: Nigel Jones and Russell Tyner

This was a well-organised course with excellent facilities. Delegates were provided with individual computers in order that they could do practical exercises during the course. The trainers delivered their material with authority even though at times the subject matter was not one in which they had experience or expertise. Secondly, they had clearly taken onboard the lessons of the Training for Trainers course.

The trainers had made changes to the template-training package for which they must be commended, adapting it for local conditions. They dealt with the provisions of the Budapest Convention particularly well in linking the various articles to domestic legislation and in discussing the forthcoming amendments to the Croatian Criminal Code.

The case studies introduced by the trainers were very well thought out and delivered at the appropriate point in the programme. It was clear that the delegates were challenged by the case studies, which stimulated lively debate. It is worth mentioning how impressive the delegates were.

With a couple of minor exceptions each of the 20 delegates attended all of the sessions and each was happy to fully participate in the discussions and willing to share their experiences. The delegates appeared to be interested and to be enjoying the course. It was also clear that the course was of

[12] The courses were supported and observed by Nigel Jones, who attended all courses. In addition Pedro Verdelho attended five courses, Matthew McCabe two courses and Russell Tyner, one course.

relevance to them and that most would be utilising knowledge gained during the course in their daily work.

3.11.2 Course 2 (Tirana, Albania, 16-18 April 2012)

- Trainers: Edmond Koloshi and Ida Ahmetlli
- Observers: Nigel Jones and Pedro Verdhelo

The School of Magistrates of Albania, whose representatives were always present, friendly and cooperative, facilitated the organisation and logistic aspects of the course. The opening of the seminar had the personal intervention of the Director of the School, who also attended one of the sessions of the last day, to deliver certificates of attendance to the participants.

The course began with about 20 attendees; however this fell to 6 after the lunch break. It was very surprising and found that this unfortunately, is very common. The solution was proposed to work through until about 3pm each day and not take a lunch break in order to try to retain as many students as possible.

By 9.30 am on day 2 of the course, the start of the day, 6 students had arrived. It should be said that the intervention of the attendees that did attend the sessions was very good. Most of them where young judges or prosecutors and it was clear that many of them had a good background on technology, computers and networks. On the other hand, some of them; both prosecutors and judges, already have had cases that shared with the rest of the participants. The discussions on concrete cases where very often intensive and alive.

It seemed that those participants that took the time to attend all of the sessions were very much interested in the improvement of their knowledge on cybercrime and the obtaining of electronic evidence.

The resources that were expended on this activity could have received a better return, if there was some mechanism to encourage those nominated or volunteering for the course to remain throughout the course. This in no way is a reflection on the performance of the trainers, both of whom were very efficient.

They delivered all the sessions in accordance with the aim and learning objectives of the course and could captivate the attention of the audience. They created good conditions to allowed attendees to interact and discuss particular questions. They were a very good training team and supported each other throughout the course and individual lessons. They should be commended for their efforts, especially in the face of such a fluctuating audience.

3.11.3 Course 3 (Pristina, Kosovo*, 19-21 April 2012)

- Trainers: Skender Cocaj and Laura Pula
- Observers: Nigel Jones and Pedro Verdhelo

The course was opened by the Director of the Kosovo* Judicial Institute, which also assumed the organisation and logistics of the event as well as providing someone in class at all times who provided support and also monitored the timeliness of the sessions and the breaks. The sessions of the course followed, in general terms, the model timetable and achieved the aim and objectives.

Throughout the course there was very good use of practical examples on child abuse, people smuggling to Italy for prostitution using Facebook, as well as ATM fraud, hacking into public institutions and credit card fraud. These examples very much enhanced the experience of the participants

During all the training days, the effective participation of the attendees in the sessions was very good. Even if only a few of them where young professionals, most of the participants were sensitive to technologies, computers and networks. They were interested in improving their understanding on computers, cybercrime and digital evidence. On the other hand, as most of them where senior professionals, with some years of experience, they could provide questions that allowed rich discussions on concrete cases they already had, both in prosecution and in court. The discussions were particularly intensive regarding the new law on cybercrime that entered in force in Kosovo* in 2009.

The participants demonstrated themselves very much interested in improving their capacities to handle cases of cybercrime and cases where the obtaining of electronic evidence is required. They identified that it would be interesting to explore more the topic, using concrete cases to discuss.

The local trainers/experts were very efficient. They delivered all the sessions and attracted the attention of the audience. Skender Çoçaj also provided very dynamic sessions, facilitating interesting discussions about concrete and "real live" questions.

3.11.4 Course 4 (Skopje, "The Former Yugoslav Republic of Macedonia", 23-25 April 2012)

- Trainers: Vladomir Milosevski and Nataliija Taseva
- Observers: Nigel Jones and Matthew McCabe

The course was held at the Judicial Institute, which took responsibility for the organisation and logistics of the event.

The nominated trainers were both present at the beginning of the course; however after the first session Vladomir Milosevski was on his own as Natalija Taseva was attending a European Union mission at the prosecutors' office for the last two days of the course. It was most unfortunate that the second trainer could not be present for the rest of the course, because she demonstrated in the first session excellent communication and training skills. She had obviously prepared her material, which she presented with clarity and authority.

Whilst this may have been unavoidable at the national level, it detracted from the overall delivery of the course. The fact that he was on his own was somewhat offset by the fact that Mr Milosevski has strong background as a prosecutor in cybercrime matters and was able to bring real cases to add to the learning. In addition he introduced computer hardware to demonstrate the learning points in the technology sessions and this was very effective. This was particularly important as the new criminal code passes the responsibility for leading investigations to prosecutors.

The timetable and the structure of the course broadly followed the structure and timetable envisaged by the pilot and as recommended, changes had been made to the training package template to adapt it to local needs, and to incorporate domestic legislation where it mirrored the provisions of the Budapest Convention. Delegates were provided with a training pack, which included copies of the slides used by the trainers in their PowerPoint presentation.

The venue for the training was well appointed, although it was necessary on the final day of training to switch rooms, in order to accommodate another training event. Although the Academy was equipped with a network of computers for training purposes, the delegates on this course did not have access to a computer and the internet. In future, consideration might usefully be given to permitting delegates such access and, thereby enabling the trainer to have at his disposal an additional tool with which to explain and demonstrate various aspects of computer technology.

The overall content of the course was admirable and the course achieved its purpose in providing judges and prosecutors with an introductory level of knowledge on cybercrime and electronic evidence, which should equip them in the future to better understand and deal with such cases that may come their way.

The willingness of delegates to fully participate in the training was somewhat uneven, and the same 4 of 5 delegates provided the majority of contributions. Disappointingly, a minority of the delegates who attended appeared to be making up the numbers and showed little interest in the subject. Such lack of interest was certainly not the fault of the trainer and should not be seen in any way as a reflection on his performance, which was of a consistently high standard throughout the entire course.

It was only on the final day that some of the delegates appeared to fully appreciate the relevance of the training, and come to realise the pivotal role imposed by the revised Code upon the public prosecutor to direct the cybercrime investigation and to ensure the proper collection and examination of electronic evidence.

If similar training is to be delivered in future, it is essential that such training should be delivered (as originally envisaged) by 2 trainers and that the timetable should represent an even split of sessions to be delivered by each trainer.

3.11.5 Course 5 (Podgorica, Montenegro, 26-28 April 2012)

- Trainers: Valentina Pavlicic and Zarko Pajkovic
- Guest presenters: Dusan Polovic, IT manager MOJ, Technology sessions; Jaksa Backovic – Cybercrime Investigator – Electronic Evidence session
- Observers: Nigel Jones and Pedro Verdelho

The organisation and logistic aspects were facilitated by the Centre for the training of judges and prosecutors of Montenegro, which representatives were always present, very friendly and quite cooperative. The opening of the seminar had personal intervention of the Director of the Centre Ms. Maja Milosevic that also attended most of the sessions. This was a very clear commitment from Centre with the programme.

16 delegates were present at the course opening. The number of delegates present fluctuated throughout the course.

In general terms, the sessions followed the model timetable and were adapted to the local requirements. The use of the IT manager to deliver the technology sessions made some sense; however he does not have the same level of presentation skills as the other trainers and did not appear to have prepared the presentation to give the relationship of technology to cybercrime and electronic evidence. The presentation was very technical. If guest presenters are to be used, it is essential that they are briefed on the aim and objectives of the sessions they are presenting and adhere to these. The experience with the second guest presenter was completely different as his presentation related to the role of judicial system. It was an excellent idea to use an experienced

police officer to give practical examples in relation to electronic evidence and this session was greatly enhanced by the level of presentation and the use of case studies to reinforce the learning objectives.

During all the training days, the effective participation of the attendees in the sessions was good: most of the participants where young professionals, showing themselves very sensitive to technologies, computers and networks. They were curious and seemed interested in improving their understanding on computers, cybercrime and digital evidence. There were some good discussions on concrete examples.

The participants demonstrated themselves very much interested in improving their capacities to handle cases of cybercrime and cases where the obtaining of electronic evidence is required.

The local trainers who had benefited from the train the trainer course were very efficient and should be congratulated on their efforts.

3.11.6 Course 6 (Ankara, Turkey, 2-4 May 2012)

- Trainers: Dr Servet Yetim and Levent Kurt
- Guest presenters:
- Murat Turan - Judge of the High Council of Judges and Prosecutors IT Department
- Ali Ardam - Police Superintendent of the Turkish National Police
- Dr Ali Karagulmez – Member of the Supreme Court of Turkey
- Observers: Nigel Jones and Pedro Verdelho

The organisation and logistical aspects were facilitated by the Turkish Justice Academy, in Ankara. The opening of the seminar counted on the personal intervention of the vice Director of the Academy and Director of the Training Centre. The representatives of the Academy, always present, were very friendly and cooperative. 27 delegates were present at the commencement of the course and this number was maintained for the majority of the sessions.

The trainers made good use of physical hardware to support the presentation on technology and in future deliveries they may consider passing them round the delegates. There was good reference of hardware to that available in the Ministry of Justice for their on line management system.

The trainers made good use of additional resources such as a video to show how data is stored on hard disks and provided lots of additional information about operating systems. The trainers engaged with the delegates at an early stage by engaging in a discussion on cases that have been encountered by the judges and prosecutors in the room

The electronic evidence session was very well presented by Dr Yetim. He was well supported by Police Superintendent Ali Ardan from the Turkish National Police digital forensics unit, who explained the procedures they follow in dealing with electronic evidence and demonstrated some of the tools they use. This was a very effective session. The lawyers who were very keen to see the equipment used by the police expressed a great deal of interest in the subject area.

The training session was very successful. It was felt that, besides enjoying the programme, as it was generically drafted to support the planned learning objectives, the participants also exchanged impressions on many related matters, sharing their experiences in concrete cases. Beyond the programme, the seminar created thus an interesting opportunity for the exchanging of experiences, both on cybercrime and on digital evidence.

The delegates were mostly experienced professionals, and quite sensitive to technologies, computers and networks. They were very much interested in improving their understanding on computers, cybercrime and digital evidence and in discussing the practical aspects of the cases. Besides, as all of them were judges or prosecutors with experience in court, concrete cases were provide, for discussions - that were very intensive and rich.

The local trainers adapted the model timetable; however all the topics were covered. They adapted the presentations to the local needs and context. Dr Yetim, Assistant General Secretary of the Supreme Court introduced very successfully, interactivity in his presentations, for example bringing and giving the participants some parts of a computer or challenging the audience with concrete questions. Murat Turan gave concrete examples of how to obtain evidence on line, doing it in real time on the Internet. Levent Kurt provided dynamic presentations, facilitating interesting discussions about concrete and "real live" questions.

Mr Ali Karagulmez, a member of the Supreme Court of Turkey attracted the attention of the participants discussing the concrete application, to the concrete case, of the domestic law on cybercrime.

There was an excellent use of additional presenters to enhance the delivery of the training material and this added to the value and success of the course.

3.11.7 Course 7 (Banja Luka, Bosnia and Herzegovina, 9-11 May 2012)

- Trainer: Ramiz Heuremagic
- Observers: Nigel Jones and Matthew McCabe

The training was conducted at the Public Institution Centre for Judicial and Prosecutorial Training of the Republika Srbska in Banja Luka. The organisation and logistical arrangements were conducted by the Academy and staff were always present and available to assist it the management of the course, which was opened by the Director of the Centre Mr Drago Seva.

The course commenced with 11 participants and this was the average number that attended all the sessions of the course. The first day of the course was a holiday in Republika Srpska and 3 more delegates arrived on day 2. Mr Heuremagic was the only person from Bosnia and Herzegovina that attended the Train the Trainer course in Zagreb and therefore he delivered this course alone. It is right to say that he had incorporated local requirements into the training materials while meeting the aim an objectives of the course. He has an excellent technical background and was able to deliver the technology aspects of the course with ease and in a very effective manner. During the training he helpfully drew on his wide experience to illustrate and explain by way of well-chosen examples or comparisons some quite intricate points of computer technology.

Delegates were provided with a training pack, which included copies of the slides used by the trainer in his PowerPoint presentation and helpfully included a table which usefully set out where the provisions of the Budapest Convention had been incorporated into domestic legislation.

Although the Academy is equipped with a network of computers the delegates on this course did not have access to a computer and the Internet. In future, consideration might usefully be given to permitting delegates such access, as this will provide the trainer with an additional tool to explain and demonstrate various aspects of computer technology.

Mr Heuremagic had prepared a short scenario for the delegates to consider and use at the end of the course to check knowledge gained. This was a very useful initiative. The scenario is an amateur attack and for the delegates to Identify the crime that may have been committed, and who would investigate.

The audience comprised judges and prosecutors drawn from all over the country. There was a good balance between judges and prosecutors. The majority of delegates were experienced practitioners, but two of the younger delegates were Associate Prosecutors who had not been previously exposed to cybercrime. Audience participation and interaction with the trainer was generally good throughout the course.

In future, it is essential that such training should be delivered (as originally envisaged) by two trainers, and that the timetable should represent an even split of sessions to be delivered by each trainer.

3.11.8 Course 8 (Belgrade, Serbia, 17-19 May 2012)

- Trainers: Bojana Paunovic and Sasa Radulovic
- Observers: Nigel Jones and Pedro Verdelho

The training session was very much successful. The organisation and logistic aspects were facilitated by the Judicial Academy of the Republic of Serbia, in Belgrade. The opening of the seminar counted on the personal intervention of a representative of the Academy. The training room was large and set out quite well.

14 participants were appointed to the seminar and most of them attended all the sessions, including day 3 of training, which was a Saturday. The sessions followed the model timetable. There was good use of technology examples to enhance to delivery of the session on hardware and very good practical examples given in the Internet section.

The local trainers were very active and competent. They adapted the presentations to the local needs and context. Some concrete cases and examples were added to the standard presentations. Besides, both of them showed they are very confident and comfortable in the subjects they had to explain to the audience. The trainers interacted well with each other and this created a good relaxed atmosphere for the delegates.

The participants interacted with the trainers, generally for discussing the concrete application, to concrete cases, of the national legal framework. Most of them were experienced professionals, but very much interested in improving their understanding on computers, cybercrime and digital evidence and in discussing practical aspects. Some of them already had handled cases with requirements on digital evidence.

3.11.9 Follow up

- On 11-12 July 2012 the members of the working group established in Ohrid, the participants in the Training of Trainers and the experts who contributed to the content of the modules will meet in Zagreb to discuss and finalise the basic module for judicial training.
- Judicial training institutions with assistance of the working group to incorporate the training pack into curricula.

3.12 Result 5: Develop training modules for basic and advanced training courses (Strasbourg, April - September 2012)

3.12.1 Introductory Cybercrime and Electronic Evidence Training Course for Judges and Prosecutors

Two consultants were tasked to prepare drafts of:

- 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 final draft of the training manual (basic) was available for the Train the Trainer Programme that took place in Zagreb in February 2012. Based on this material eight in-country basic training courses were delivered by the trainers trained under the project and with the assistance of international trainers.

The course is designed to provide judges and prosecutors with an introductory level of knowledge on cybercrime and electronic evidence. It provides legal as well as practical information about the subject matters and concentrates on how these issues impact on the day-to-day work of judges and prosecutors.

The course covers the following subjects:

- Introduction to cybercrime – trends and tools
- Technology involved in cybercrime
- Cybercrime as a criminal offence in domestic legislation
- Electronic evidence practice, procedure and legislation
- Procedural law/ investigative measures in domestic legislation
- International Cooperation.

3.12.2 Follow up

- Based on the feedback from the ToT and the in-country trainings the basic training pack will be updated.
- Organise a regional workshop for the finalisation of the basic for judicial training in July 2012.
- Develop the advanced judicial training by September and deliver in country trainings by the end of 2012.
- Continue the work with the training institutions from the project areas to include the training material into curricula.

3.13 Result 5 - Judicial training on cybercrime and electronic evidence: Visit to the Judicial Academy to establish a Pilot Centre on Judicial Training (Zagreb, Croatia, 16 December 2011)

3.13.1 Visit to the Judicial Academy of Croatia

The establishment of the Pilot Centre for Judicial Training was discussed in several events including the first meeting of the Steering Committee in which the participating countries/areas agreed that the Pilot Centre should be established in Croatia. The Steering Committee took into account several advantages that Croatia provides for the establishment of this Pilot Centre, including the geo-political factors, the current position of Croatia as one of the leaders from the region in the development of curricula and training on cybercrime matters, the fact that the Croatian language is close to most of the languages from the project area (except for Albanian and Turkish). In addition to the above the Croatian authorities and the Judicial Academy of Croatia have agreed to host and contribute to the Pilot Centre.

In a follow up discussion in relation to the establishment of the Pilot Centre during the Regional Workshop on Judicial Training, which was held in May of 2011 in Ohrid, the participants confirmed their support to have the Judicial Academy in Croatia as the host of the Pilot Centre.

Two representatives from the project management team and a Council of Europe consultant visited the premises of the Judicial Academy in Zagreb. The visit was used to evaluate the capacities and the needs of the Judicial Academy of Croatia to establish such centre. Furthermore, the meeting provided an opportunity to discuss the role and responsibilities of the potential partners involved in the establishment of the Pilot Centre and the additional support for the Academy to become a sustainable regional centre for judicial training on cybercrime matters.

The Judicial Academy of Croatia currently has four class rooms with a maximum of 25 students, all classrooms are equipped or able to install training equipment in the classrooms. The Academy has in its inventory a number of laptops available for trainings. In addition the Academy has access to a large conference room, which can be used for conferences and meetings of larger groups of students.

However, during the discussion it was pointed out that the Judicial Academy of Croatia will receive a new location from the Government of Croatia, which is expected to be available in spring 2012.

The Judicial Academy currently maintains a website which will be updated and modernised (new site is under construction). The representatives of the Academy claimed that the site is visited by around 5000 visitors a day. The Academy is currently working on an IPA funded project which has an e-learning component, features of which can be utilised by the Pilot Centre for the various training programs in the future. This e-learning component could provide for a lower cost of organizing the cybercrime related trainings and long-term sustainability of this centre.

The Judicial Academy currently has 49 members of staff and offered the services of current personnel employed in the Judicial Academy as support to the Pilot Centre. In addition the Academy has budget to increase the number of staff, which provides a good grounds of support for the Pilot Centre in terms of covering the cost for human resources.

The project will cooperate with the Judicial Academy of Croatia and the Ministry of Justice of Croatia in the establishment of the Pilot Centre for Judicial Training. This cooperation will include the provision of

advice in the setting up of this Pilot Centre, support in providing regional training and development of training modules and materials.

In order to support the establishment of the Pilot Centre, the Judicial Academy was selected to organise the ''train the trainers'' course and hosted the in-country judicial training for Croatia.

3.13.2 Follow up

- The project will follow-up on this activity once the location of the Academy is certain.
- In July 2012 the Judicial Academy will organise a regional workshop for the finalisation of the basic training pack. This will be an opportunity to further discuss and the pilot centre.

3.14 Result 6 – Financial investigations: Intra-regional Workshop on criminal money flows on the Internet (Kyiv, Ukraine, 27-29 February 2012)

3.14.1 The workshop

Expected result 6 is related to *financial investigations*:

> Financial investigations: Capacities of financial investigators, Financial Intelligence Units (FIU), and/or relevant law enforcement units in charge of fighting against cyber criminals in following crime proceeds on the internet improved and their cooperation with the financial sector strengthened.

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

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

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

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

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

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

The main achievements of the intra-regional workshop are:

- Raised awareness of the need to confiscate proceeds from crime on the Internet.
- Strengthened interagency and public-private cooperation against criminal money on the Internet.
- The new FATF Recommendations were presented to take measures for their implementation.
- The (draft) Typology study on Criminal money flows on the Internet: Methods, trends and multi-stakeholder counteraction was presented and discussed and additional information was included in the draft study before its subsequent adoption by MONEYVAL.[13]
- Participants identified solutions for overcoming the problems encountered in the prevention and control of criminal money flows on the Internet.
- Good practices were presented.
- Each delegation prepared a set of recommendations for measures to be taken in their respective country/area.

The FATF Recommendations[14] set out a comprehensive and consistent framework of measures that countries should implement in order to combat money laundering and terrorist financing, as well as the financing of proliferation of weapons of mass destruction. In February 2012, the FATF recommendations and special recommendations were revised and consolidated into new 40 recommendations. A representative of the FATF Secretariat presented the new recommendations and explained their practical effect on the existing procedures and standards. An important development is that the new recommendations encourage the countries to implement, among other relevant international standards and conventions, the Budapest Convention on Cybercrime.

Furthermore, the Council of Europe (Moneyval and Global Project on Cybercrime) has carried out a typology exercise on criminal money flows on the Internet. The Typology study was presented in the workshop as a response to the general need of law enforcement authorities to learn about trends, methodology and multi-stakeholder counter-action. The Report identifies in most instances the types of crime they are encountering on the Internet. These include: computer fraud, electronic banking and electronic transfer fraud, credit card fraud (including counterfeiting of cards), identity theft, as well as phishing type frauds.

The discussions in the workshop pointed out that:

- Effective mechanisms for confiscating proceeds of crime on the Internet are vital for an effective fight against cybercrime and other forms of serious and economic crime.
- Cooperation at all levels – interagency cooperation, public-private cooperation and information exchange, as well as regional and international cooperation is a prerequisite for an efficient confiscation. Predicate offences to money laundering (such as different types of fraud, offences related to child abuse material, counterfeit medicines, offences against intellectual property rights etc.) are committed through the Internet and different mechanisms are used for channelling criminal proceeds by using the Internet with the aim of disguising their origin and transforming them into cash.

[13] http://www.coe.int/t/DGHL/cooperation/economiccrime/cybercrime/Documents/Reports-Presentations/MONEYVAL_2012_6_Reptyp_flows_en.pdf
[14] http://www.fatf-gafi.org/dataoecd/49/29/49684543.pdf, International Standards on Combating Money Laundering and the Financing of Terrorism & Proliferation, FATF, February 2012.

- Involvement of different stakeholders is required to trace and seize criminal money on the Internet (AML system, anti-cybercrime institutions, financial sector, ISPs, institutions monitoring the Internet), and a number of possible countermeasures needs to be taken, including reporting on e-crime, raising public awareness, managing risks in the private sector, legal framework, specialised high-tech crime units etc.

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

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

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

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

Recommendations made by delegations

Albania

- Setting up a report system through Albanian State Police Webpage, for cybercrime reporting.
- Awareness campaign about cybercrime and system of reporting, to encourage community to report computer crime.
- Extending cooperation with Albanian Bank Association not just for credit card fraud, but computer crime related to bank system.
- Establish a common way of cooperation through Law Enforcement, ISP, Electronic and Postal Communication Agency, National Information Society Agency, FIU, in the field of combating cybercrime, crime proceeds and money laundering through Internet, by creating a kind of forum under EPCA authority.
- Training of Law Enforcement in the area of cybercrime and money flows on Internet.

Bosnia and Herzegovina

- Enacting, adapting and harmonising the law in BiH (regarding, confiscation illegally acquired property) formation at all levels Agency for the Management of seized property
- Networking and access to databases of financial institutions and other relevant institutions in the private and public sector (electronic reporting and accessing)
- Strengthening of specialist training for prosecutors and investigators
- Amendments of the law on communications in BiH concerning the obligations of ISP and telecom operators regarding obligation to deliver data.

Croatia

- Establish specialised units for combatting cybercrimes within relevant institutions
- 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.)
- Provide training for the judiciary and police officers on the use and admissibility of electronic evidence in court
- Ease the procedure for reporting cybercrime and provide analysis of reported incidents

Montenegro

- Creation of website and phone line for reporting of cybercrime incidents similar to the already existing for reporting corruption in Montenegro.
- Entering in to the final phase of forming of National CERT team.
- Organizing Training for members of joint investigative team, including members of FIU and Cybercrime unit.
- Overcoming the problem of lack of educated professionals and sophisticated technology for tracking and examining of digital evidences.
- Strengthening of international cooperating relating to exchanging data and intelligence of criminal money flow.
- Creating public campaign for rising awareness for issues of all types of cybercrime.

Serbia

- Improvement of inter-agency cooperation and exchanging data
- Establishing of central account register
- Integration of public sector databases
- Improvement of international cooperation and cooperation with ISPs
- Enhance educational and training capacities of competent state bodies and private sector
- Amending of legal provisions
- Organising of forum between public and private sector
- Continuous development of typologies and list of indicators for STR
- Enhance cooperation with money exchange companies
- Enhance human capacities especially in analytic departments.

"The former Yugoslav Republic of Macedonia"

- Improving cooperation and communication with international institutions
- Strengthen the capacity of national institutions in dealing with Cybercrime and criminal money flows on the internet
- Improving cooperation and communication with the international service providers
- Improving cooperation in public-private sector - establishing Forum – in which would participate representatives from the first five institutions in the country who are dealing with Cybercrime.
- Creating web site for reporting any abuse about Cybercrime
- Electronic exchanging of information within national institutions
- Training courses for Law enforcement and prosecutors
- Forming interagency teams working on cases.

Turkey

- 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.
- 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.
- 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.
- Establish a [collective] 24/7 Point of Contact consisting of representatives of the prosecution, law enforcement, ISPs and the Interbank Card Centre (BKM).

3.14.2 Follow up:

- Training for the staff to be considered under other activities.
- Organise regional workshops to support the establishment of trusted fora for information/intelligence exchange between financial investigators, financial intelligence units, high-tech crime units and the private sector, including the financial sector.

4 Partners and other co-operation

The cooperation and interaction with the project teams consisting of representatives of relevant counterpart institutions in project areas has been excellent. In all events high officials and participants working on cybercrime expressed their strong commitment and confirmed the relevance of the project.

The private sector was invited in specific activities carried out under the Project. In particular, the expertise of the August & Debouzy, a law firm working with Microsoft, Orange and other major ISP's was used in the project activities to raise awareness on the challenges of collecting electronic evidence and share good practices on public-private cooperation in cybercrime investigations.

France, Italy, Romania, and Slovenia participated and contributed to several activities and reports conducted.

The project management maintained contact with the EU Delegations in the project areas. The EU Delegation in Skopje participated in the 3rd Steering Committee Meeting and the Regional Workshop on handling international cooperation requests (28-30 March 2012).

5 Visibility

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

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

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

In the Octopus Conference (workshop 1) the two projects of the Council of Europe and the European Union were presented to more than 200 participants from all over the world[15].

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

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

[15] http://www.coe.int/t/dghl/cooperation/economiccrime/cybercrime/cy_Octopus_Interface_2011/Interface2011_en.asp

6 Conclusions

The CyberCrime@IPA project is very well on track and is likely to achieve its objective and expected results. It continues to produce results in terms of institution building, training, regional, international, interagency and public-private cooperation as well as capacities to investigate and prosecute cybercrime.

Good practices are shared, strategies and practical tools have been developed, and the participation of representatives of project areas in international meetings was ensured.

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

Among the main achievements are:

- Better understanding of the need to take measures against cybercrime at national and regional levels, among relevant institutions, including decision-makers.
- Initiated the process of drafting amendments to the cybercrime legislation in Bosnia and Herzegovina and supported a similar decision in Serbia after elections.
- Good practice study on Article 15 – conditions and safeguards completed.
- Good practice study on specialised cybercrime units completed in cooperation with the EU Cybercrime Task Force.
- In view of sharing practices and benefit from initiatives within the European Union, associate membership in the EUCTF, application for training materials and membership in the Cybercrime Training and Education Group (ECTEG), as well as associate membership in EUROJUST supported.
- Developed a training pack on cybercrime and electronic evidence to be included in the regular programmes of training institutions and initiated the development of an electronic evidence guide.
- Trained 15 trainers on cybercrime and electronic evidence, thus increasing the capacity of training institutions in project areas to deliver such training in a sustainable manner.
- Provided training for approximately 140 judges and prosecutors in all project areas on cybercrime and electronic evidence based on the training pack developed under the project.
- Project areas contributed to the finalisation of the Typology study on criminal money on the Internet and developed specific proposals for measures to be taken based on this study and the new 40 Recommendations of the Financial Action Task Force.

Bosnia Herzegovina signed the Convention on the Protection of Children against Sexual Exploitation and Sexual Abuse (12 November 2011).

The project created important synergies with other relevant projects, namely the Council of Europe Global Project on Cybercrime[16] and the CyberCrime@EAP Project on Cooperation against Cybercrime under the Eastern Partnership Facility of the European Union and the Council of Europe[17].

The project areas now play an active role in the Cybercrime Convention Committee, and are thus more integrated in European efforts against cybercrime.

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

In the coming months, the finalisation of additional tools and the implementation of activities will be accompanied by a series of assessments (Result 8). This will add further impetus to reforms and to an agreement on regional priorities regarding measures against cybercrime in early 2013.

_____

Name of the contact person for the Action:	Alexander Seger Head of Data Protection and Cybercrime Division
Signature:	
Location:	Strasbourg
Date report due:	30 June 2012
Date report sent:	

7 Appendices

7.1 Logical framework and workplan (20 June 2012)

	Intervention logic	*Details*	*Timeline*
Overall objective	**To enhance the ability of countries of the region to prevent and control cybercrime**		
Specific objective	**To strengthen the capacities of criminal justice authorities of Western Balkans and Turkey to cooperate effectively against cybercrime**	***Indicators:*** - Legislation on cybercrime assessed and strengthened - Increased level of regional/international police and judicial cooperation against cybercrime as reflected in requests sent and received - Law enforcement – Internet service provider functioning in each country based on agreed upon guidelines, memoranda of understanding and trained personnel - Regional law enforcement training strategy adopted - Cybercrime and electronic evidence training integrated into the training curricula for judges and prosecutors - Trusted fora established for information exchange on criminal money flows on the internet between public and private sector stakeholders - Regional assessments carried out on progress made against cybercrime	
Inception phase		Planning meeting Strasbourg Country/area visits: - 16 Nov Serbia	2 Nov 10 Nov 10 – Dec 10

	Intervention logic	***Details***	***Timeline***
		- 16 Nov "the former Yugoslav Republic of Macedonia - 18 Nov Kosovo*[18] - 29 Nov Montenegro - 30 Nov Albania - 14 Dec Croatia - 15 Dec Bosnia and Herzegovina - 16 Dec Turkey - Launching conference - Adoption of the updated work plan	Istanbul, Turkey 17-18 Feb 11
Result 1	**Cybercrime policies and strategies. Policy- and decision-makers are aware of cybercrime threats and human rights implications and have reached agreement on strategic priorities regarding cybercrime for Western Balkans and Turkey**	***Indicators:*** - Participation by senior representatives in regional meetings - Adoption of a document with regional strategic priorities regarding cybercrime by month 18	
Activities		*Details:*	
1.1	Prepare a situation report reflecting current knowledge of the cybercrime situation and effects on the region, as well as an analysis of current measures taken in the fields covered by this project	2 Nov 10: Meeting with Henrik Kaspersen and Nigel Jones in Strasbourg: agreement on structure of report, questionnaire to collect information to be prepared, country-visits and timelines: - Replies to questionnaire by 10 January 11 - Draft report by 6 February 11	2 Nov 10, Strasbourg
1.2	Hold a regional conference for policy- and decision-makers (such as senior representatives from Ministries of Justice and Interior, Offices of Prosecutors General) to review the threat of	Regional conference in conjunction with launching conference - Presenting the Situation Report and discuss the cybercrime priorities - Finalisation of the Situation Report	17-18 Feb 11, Istanbul, Turkey 27 Feb 11

[18] All reference to Kosovo, whether to the territory, institutions or population, in this text shall be understood in full compliance with United Nations Security Council Resolution 1244 and without prejudice to the status of Kosovo.

	Intervention logic	***Details***	***Timeline***
	cybercrime and current measures undertaken by countries of the region (within first six month of project) as well as compliance of measures taken with the European Convention on Human Rights, Article 15 of the Budapest Convention and relevant case law of the European Court of Human Rights24-25 March	- A specific report on procedural safeguards and conditions to be prepared Workshop on safeguards and conditions (in cooperation with Cybercrime@EAP) Participation in the Internet Governance Forum	April 11 – September 12 5 November 12, Baku, Azerbaijan 6-9 November 12, Baku, Azerbaijan
1.3	Support the drafting of an agreement on regional priorities regarding cybercrime taking into account European policies	To be drafted between September and November 2012 based on the results of assessment visits (activity 8.2 in Sept – Oct 2012) and adopted reports (October 2012)	Sep – Nov 12
1.4	Organise a follow up high-level conference to review progress made and to reach agreement on regional strategic priorities regarding cybercrime	Regional conference to be organised in January 2013 - Discussion of assessment reports (activity 8.3) - Adoption of a possible regional agreement (activity 1.3)	January 2013
Result 2	**Harmonisation of legislation. Amendments are drafted to bring relevant legislation fully in line with the EU acquis, in particular the Convention on Cybercrime (CETS 185) and its Protocol on Xenophobia and Racism (CETS 189) and thus ensure harmonisation of legislation within Western Balkans and Turkey**	***Indicators:*** - Reports prepared and recommendations adopted on the effectiveness of legislation - Amendments to legislation available to enhance the effectiveness of legislation	
Activities		*Details:*	
2.1	Regional review of legislation against the Budapest Convention Cybercrime (CETS 185), the Protocol on Xenophobia and Racism committed through Computer Systems (CETS 189) and of relevant	Regional workshop on legislation: Legislative review based on situation report Council of Europe Regional Meeting on Stopping Sexual violence	24-25 March 11, Sarajevo 27-28 Oct 2011

	Intervention logic	*Details*	*Timeline*
	provisions of the Convention on the Protection of Children against Sexual Exploitation and Sexual Abuse (CETS 201)	against children – Ratifying CETS 201	Zagreb, Croatia
		Regional Workshop on effectiveness of legislation (in cooperation with the twining Project in Turkey)	January 2013, Turkey
2.2	Provide advice to countries in the strengthening of legislation and follow up to recommendations from regional reviews	In-country workshops	27 Jan 2012, Belgrade Serbia 26 March 2012, Bosnia and Herzegovina
		Meeting with the TEAM for tracking of implementation of criminal legislation - support of amendments to legislation	9 May, 2012, Sarajevo, Bosnia and Herzegovina
		Recommendations and legal advice provided to draft legislative amendments in Bosnia and Herzegovina	May – June 2012
		Participation in the Octopus Conference and the Cybercrime Convention Committee	4-8 June 12, Strasbourg, France
2.3	Establish an online resource on legislative developments for sharing experiences and good practices	On-going since January 2011 Project teams will provide regularly update on new legislation adopted, links to relevant legislation and court decisions	Jan 11 - Mar 13
Result 3	**Enhanced regional and international law enforcement and judicial cooperation against cybercrime[19] based on Chapter III of the Budapest Convention on Cybercrime**	***Indicators:*** - Number of requests handled by 24/7 points of contact - Number of requests sent/received from law enforcement authorities	

[19] This component will help provide follow up to the analysis and suggestions made in the study on the functioning of 24/7 points of contacts and mutual legal assistance in cybercrime matters in which countries of South-eastern Europe participated in 2008.
http://www.coe.int/t/dghl/cooperation/economiccrime/cybercrime/Documents/Points%20of%20Contact/567_24_7report3a%20_2%20april09.pdf

	Intervention logic	***Details***	***Timeline***
		- Number of requests sent/received and response time for MLA requests related to cybercrime - Level of cooperation between high-tech crime units - 24/7 points of contact are fully functioning in line with Article 35 of the Budapest Convention	
Activities		*Details:*	
3.1	Provide advice on the institutional set up, responsibilities and authority of 24/7 points contact in line with article 35 of the Budapest Convention on Cybercrime	1 regional workshop (combined with 3.2) Participation in G8 24/7 training event (one representative from each area) Participation in Octopus Conferences 2011	15 Sep 11, Budva, Montenegro 8-10 Nov 11, Rome 21-23 Nov 2011
3.2	Provide advice on the set up of high-tech crime units and specialised prosecution departments, including study visits and other opportunities for the exchange of information	1 regional workshop (back-to-back with 3.1) To be preceded by preparation of final draft of the good practice document on high-tech crime units (Aug 11 – Sept 11) and finalised in Octopus in Nov 11. 2 study visits - one to Interpol under activity 3.3 and Paris/French HTCU - one to Romania	13-14 Sep 11, Budva, Montenegro Lyon/Paris, Dec 12 Romania, Mar 13
3.3	Strengthen participation of high-tech crime units in the Interpol network of National Central Reference Points for cybercrime	1 workshop/study visit to Interpol (combined with one study visit under 3.2)	Dec 13 Lyon

	Intervention logic	*Details*	*Timeline*
3.4	Organise regional and international training meetings for 24/7 points of contact and high-tech crime units with regard to international law enforcement cooperation and information exchange	2 regional meetings (50 participants) (International workshop in the Octopus conference) Participation in Octopus conferences	21/22 Nov 11, Strasbourg 21-23 Nov 11 Strasbourg; 6-8 June 2012
3.5	Provide advice to services of the prosecution and ministries of justice regarding the handling of international cooperation requests related to cybercrime in an expedited manner	1 regional workshop (30 participants)	28-29 March 12 Skopje, "The Former Yugoslav Republic of Macedonia"
3.6	Organise regional training meetings on international judicial cooperation for services of the prosecution and ministries of justice with the participation of high-tech crime units and 24/7 points of contact	2 regional training meetings (50 participants) Participation in Regional Conference on Cybersecurity and Cybercrime for South East Europe Participation in Octopus conferences 2011 and 2012	Dubrovnik, Croatia, 16-17 May 2011; and Serbia, Feb 13 19 Oct 11, Sofia, Bulgaria 21-23 Nov 11, Strasbourg 6-8 June 2012
3.7	Prepare a training manual on international police and judicial cooperation against cybercrime	Research contract	Jan – Dec 12
Result 4	**Law enforcement training strategy agreed by Ministries of Interior and implementation initiated**	***Indicators:*** - Adopted law enforcement training strategy - 16 trainers trained in the delivery of basic law enforcement training courses	

	Intervention logic	***Details***	***Timeline***
		- 35 law enforcement officers trained in basic cybercrime investigations and cyberforensics - Feasibility study on regional and domestic centres of excellence for cybercrime training - Interagency cooperation promoted through up to 3 regional multi-disciplinary training workshops - One expert from each project area (8 in total) participating in Masters programme on computer forensics and cybercrime investigations	
Activities		*Details:*	
4.1	Create a regional working group for law enforcement training to prepare a proposal for a law enforcement training strategy in cooperation with the European Cybercrime Training and Education Group coordinated by Europol (www.ecteg.eu). This includes an assessment of current law enforcement training capabilities in this region and the role of academia	Study visit/meeting at University College Dublin: - creation of a regional working group for law enforcement training - draft strategy for law enforcement training with specific strategies for each project area - application for ECTEG (European Cybercrime Training and Education Group) training materials (related to 4.1) - application for membership in ECTEG; - discussion on 2Centre project (related to 4.4) - nominations for participants in the Master of Sciences (MSc) programme in Forensic Computing and Cybercrime Investigation offered by UCD (activity 4.6) Participation in ECTEG meetings LEA Training Strategy available Support the implementation of the LEA Training Strategy	23-27 May 11, Dublin, Ireland 15-16 May 12 June- Sep 11 Jan –Dec 12

	Intervention logic	***Details***	***Timeline***
4.2	Select trainers from each project area and carry out a training the trainers course	1 train the trainers regional course	Oct 12 – Feb 13
4.3	Hold standard basic training course as revised by UCD and a second training course for up to 30 law enforcement officers for up to 30 law enforcement officers (staff of high-tech crime units) in cybercrime investigations and cyber forensics each	1 training course for law enforcement	Oct 12 – Feb 13
4.4	Carry out a needs assessment and prepare a proposal regarding the creation of regional or domestic centres of excellence for cybercrime training in Western Balkans and Turkey (www.2centre.eu)	Discussed proposals for 2 Centres as part of training strategy	23-27 May 11, Dublin
4.5	Organise at least three multi-disciplinary investigative training courses on case studies and new trends, techniques and technologies	Workshop on interception of communication, gathering of electronic data from wireless networks Prepare a guiding paper on electronic evidence with involvement of experts from in cooperation with the global Project on Cybercrime (draft to be discussed in the Octopus Conference 2012) • Experts meeting on the development of the guiding paper on electronic evidence • Side event organised in the Octopus Conference Workshop on electronic evidence (legal and practical aspects) for institutions of the criminal justice chain (investigators, forensic experts, prosecutors, judges).	Zagreb, Croatia 27-28 June 2011 Jan – June 12 Paris, France 14-15 Feb 12;Wiesbaden, Germany, 29-31 May 12 Strasbourg, France 6-8 June 12 Skopje, 4-5 Sep 2012

	Intervention logic	***Details***	***Timeline***
4.6	Support the participation of one law enforcement expert from each project area in the distance learning MSc programme in Forensic Computing and Cybercrime Investigation offered by University College Dublin[20]	See activity 4.1 Initiate during meeting in Dublin MSc programme in Forensic Computing and Cybercrime Investigation offered by University College Dublin MSc Residential Workshops at the UCD	23-27 May 11, Dublin Sep 11 – Apr 13 June 12
Result 5	**Judicial training on cybercrime and electronic evidence integrated into the curricula of training institutions for judges and prosecutors**	***Indicators:*** - Basic and advanced training courses reflected in the initial and in-service training curricula of judicial training institutions - Training modules for basic and advanced training available in local languages - Up to 16 trainers trained - Up to 12 training courses carried out - At least one pilot centre established and able to maintain a repository of trainers, keep training modules up to day, carry out research, maintain a resource for online training and networking among trained judges and prosecutors	
Activities		*Details:*	
5.1	Create a regional working group of members of judicial training institutions and analyse training systems	Regional workshop on judicial training analysis to create a regional working group of members of judicial training institutions Regional workshop with the regional working group and trainers to finalise training material	11-12 May 11, Ohrid, "the former Yugoslav Republic of Macedonia" Croatia, 11-12 July 12
5.2	Develop training modules for basic and advanced training courses and make them available in local	Training modules for basic and advanced training to be discussed during the workshop in Ohrid and finalised by the experts and	May 11 _ Dec 12/Apr- Dec 12

[20] http://cci.ucd.ie/content/cybercrime-courses?q=node/17

	Intervention logic	*Details*	*Timeline*
	languages	the working group of judicial training institutions	
5.3	Train trainers in the delivery of the training courses	Train the trainers regional course (2 trainers per project area)	Croatia, 20-24 Feb 12
5.4	Support the establishment of at least one pilot centre for judicial training	Establishing a pilot centre in Croatia Confirmed in the workshop on judicial training (Ohrid)	Nov 11 – March 13
5.5	Support the integration of basic and advanced courses into initial and in-service training curricula	In-country visits	Oct/Nov 12
5.6	Support the delivery of at least one basic training course in each Beneficiary and one advanced training course in four Beneficiary countries	12 in-country workshops **Basic Training** Albania (16-18 April, 2012); BIH (9-11 May, 2012); Croatia (11-13 April, 2012); Kosovo* (19-21 April, 2012); Montenegro (23-25 April, 2012); Serbia (17-19 May, 2012); Turkey (2-4 May, 2012); FYR Macedonia (26-28 April, 2012) **Advanced (Module 2)** Turkey, "The Former Yugoslav Republic of Macedonia", Croatia, Kosovo*	April – May 12 October 12
Result 6	**Financial investigations: Capacities of financial investigators, Financial Intelligence Units (FIU), and/or relevant law enforcement units in charge of fighting against cyber criminals in following crime proceeds on the**	***Indicators:*** - Joint training courses carried out for cybercrime investigators, financial investigators and financial intelligence units	

	Intervention logic	*Details*	*Timeline*
	internet improved and their cooperation with the financial sector strengthened	- Regional and domestic trusted fora for regular information exchange between public and private sector stakeholders established	
Activities		*Details:*	
6.1	Organise regional meeting on typologies of criminal money flows on the internet, including indicators and red flags for FIUs, high-tech crime units, financial investigators and regulators	Regional workshop on typologies of criminal money flows on the internet	17-18 Mar 11, Belgrade
6.2	Organise joint training course for cybercrime investigators, financial investigators and financial intelligence units on criminal money flows on the internet	1 regional training course (2 days, 30 participants)	27-29 Feb 12 Kyiv Ukraine (with CyberCrime@EAP)
6.3	Support the establishment of trusted fora for regular information exchange between financial investigators, FIU and the private sector (including financial sector) at regional and domestic levels	Participation in Octopus conference 2012 1 regional workshop (30 participants) (Istanbul to provide for participation of ISPs)	Strasbourg, France 6-8 June 2012 Nov 12, Turkey - Istanbul (with EAP and Activity 7.4);
Result 7	**Cooperation between law enforcement and Internet service providers (ISPs) in investigations related to cybercrime strengthened**	***Indicators:*** - Assessment report on the functioning of LEA-ISP cooperation - Regional guidelines on LEA-ISP cooperation - Memoranda of understanding on LEA-ISP cooperation concluded in each project area - LEA and ISP staff responsible for cooperation trained	
Activities		*Details:*	

	Intervention logic	***Details***	***Timeline***
7.1	Carry out an assessment in project countries on the cooperation between law enforcement authorities and Internet service providers including recommendations for the strengthening of such cooperation[21]	Part of regional workshop (7.2) and based on situation report 1.1	June 2011
7.2	Organise a regional meeting for LEA and ISP to discuss guidelines on LEA-ISP cooperation to be followed in each project area	Regional meeting for LEA and ISP	6-7 June 2011, Durrës, Albania
7.3	Support the conclusion of memoranda of understanding between law enforcement and (associations of) ISPs in each project area.		Jan 12 - Dec 12
7.4	Organise a regional meeting for the training of LEA and ISP staff responsible for cooperation and for developing standard procedures for cooperation	1 regional meeting (combined with 7.3)	Nov 12, Turkey (with EAP and Activity 6.3)
		International workshop on public-private exchange information in the Octopus Conference	Strasbourg, 6-8 June 12
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:*** - Methodology adopted and applied - Assessment reports available	
Activities		*Details:*	
8.1	Develop a methodology for the regional peer to	Draft prepared in August 2011, discussed in the 2nd Steering	Aug 11, Strasbourg

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

	Intervention logic	***Details***	***Timeline***
	peer assessment of progress made against cybercrime;	Committee Meeting. Methodology agreed by the Steering Committee (with deadline for comments 26 September 2011)	 12 Sep 11
8.2	Carry out a cycle of regional assessments	To be carried out between Oct and Nov 2012	Oct - Nov 12
8.3	Organise a regional conference for discussion and adoption of assessment reports.	Regional conference to be organised for: ▪ Discussion and adoption of assessment reports ▪ Adoption of a regional agreement (activity 1.3) Regional Conference and closing event	Jan – March 13 April 13

7.2 Calendar of activities

Date	Place	Activity	Status	Related result # and activity #
2 Nov 10	Strasbourg	Planning meeting (with Henrik Kaspersen and Nigel Jones)	completed	Result 1: Activity 1.1
2 – 15 Nov	Strasbourg	Drafting questionnaire to obtain the information necessary for the preparation of the situation report	completed	Result 1: Activity 1.1
Nov/Dec 10	All project areas	Country/area project visits - 16 Nov Serbia - 17 Nov "the former Yugoslav Republic of Macedonia" - 18 Nov Kosovo* - 29 Nov Montenegro - 30 Nov Albania - 14 Dec Croatia - 15 Dec Bosnia and Herzegovina - 16 Dec Turkey	completed	Result 1: Activity 1.1
Nov/Dec 10	Strasbourg	Sending out the questionnaire and draft country profiles	completed	Result 1: Activity 1.1
Dec/Jan 11	Strasbourg	Drafting of the situation report	completed	Result 1: Activity 1.1
From Jan 11	Strasbourg	Online resource on legislation	on-going	Result 2: Activity 2.3
17-18 Feb 11	Istanbul/Turkey	Launching event	completed	Result 1: Activity 1.2
18 Feb 11	Istanbul/Turkey	Regional conference for policy- and decision-makers (part of the launching event)	completed	Result 1:Activity 1.2
27 Feb 11	Strasbourg	Finalisation of the Situation Report	completed	Result 1: Activity 1.2
17-18 Mar 11	Belgrade/Serbia	Regional workshop on typologies of criminal money flows on the internet	completed	Result 6: Activity 6.1
24-25 Mar 11	Sarajevo/BiH	Regional workshop on legislation	completed	Result 2: Activity 2.1
March 11	Strasbourg	The concept paper for the training of judges and prosecutors in cybercrime and electronic evidence matters available in Albanian, Bosnian, Macedonian and Turkish.	completed	Result 5: All activities
March 11	Strasbourg	The Guidelines for the cooperation between law enforcement and internet service providers against cybercrime available in Albanian, Croatian, Macedonian and Turkish	completed	Result 7: All activities
11/12 May 11	Ohrid/"the former Yugoslav Republic	Regional workshop on judicial training analysis to create a regional working group of members of judicial training institutions	completed	Result 5: Activity 5.1

	of Macedonia"			
16-17 May 11	Dubrovnik, Croatia	Regional meeting on international judicial cooperation	completed	Result 3: Activity 3.6
23-27 May 11	Dublin, Ireland	Study visit to UCD	completed	Result 4: Activity 4.1
6-7 June 11	Albania	Regional workshop on LEA – ISP cooperation	completed	Result 7: Activity 7.1
22 June 11	The Hague, Netherlands	European Union Cybercrime Task Force (EUCTF)	completed	Result 3: Activity 3.2
27-28 June 11	Zagreb, Croatia	Workshop on interception of communication, gathering of electronic data from wireless networks	completed	Result 4: Activity 4.5
June-Sep 11	Strasbourg	Drafting LEA training strategy document	completed	Result 4: Activity 4.1
August – Sep 11	Strasbourg	Drafting and adoption of the methodology for the assessment of progress made against cybercrime	completed	Result 8: Activity 8.1
Apr 11 – Sep 12	Strasbourg	Preparation of a report on procedural safeguards and conditions	on-going	Result 1: Activity 1.2
April 11 – Dec 12	Strasbourg	Develop training modules for basic training courses and make them available in local languages	on-going	Result 5: Activity 5.2
Aug – Nov 11	Strasbourg	Preparation of good practices document on high-tech crime units	completed	Result 3: Activity 3.2
12-15 Sep 11 Budva, Montenegro		Steering Committee meeting (12 Sep)	completed	All
		Regional workshop with specialised prosecution departments and high-tech crime units (13-14 Sep)	completed	Result 3: Activity 3.1
		Regional workshop on 24/7 (15 Sep)	completed	Result 3: Activity 3.2
Sep 11-Apr 13	All countries/areas	MSc programme in Forensic Computing and Cybercrime Investigation offered by University College Dublin	on-going	Result 4: Activity 4.6
19 October 11	Sofia, Bulgaria	Regional Conference on Cybersecurity and Cybercrime for South East Europe	completed	Result 3: Activity 3.6
27-28 Oct 11	Croatia, Zagreb	Stopping sexual violence against children - ratifying and implementing the Council of Europe Convention on Protecting Children Against Sexual Exploitation and Sexual Abuse (CETS No. 201	completed	Result 2: Activity 2.1
8-10 Nov 11	Rome	Participation in G8 24/7 training event	completed	Result 3: Activity 3.1
21-25 Nov 11	Strasbourg	Participation in the Octopus Conference and Cybercrime Convention Committee (T-CY) meeting	completed	Result 3: Activities 3.1, 3,4, 3,6, 6,2
21/23 Nov 11	Strasbourg	International training meetings for 24/7 points of contact and high-tech crime units with regard to international law enforcement cooperation	completed	Result 3: Activity 3.4

		and information exchange (workshop in the Octopus conference)		
16 Dec 11	Zagreb, Croatia	Visit to the Judicial Academy to discuss the establishing a pilot centre for judicial training	completed	Result 5: Activity 5.4
27 Jan 12	Belgrade, Serbia	Specific workshop on legislation	completed	Result 2. Activity 2.2
Jan – Oct 12	Strasbourg	Prepare a guiding paper on electronic evidence with involvement of experts from EU MS, Asia and Latin America in cooperation with the global Project on Cybercrime (draft to be discussed in the Octopus Conference 2012)	on-going	Result 4: Activity 4.5
Jan –Dec 12	countries/areas	Support the conclusion of memoranda of understanding between law enforcement and (associations of) ISPs in each project area	on-going	Result 7: Activity 7.3
Jan-Dec 12	all countries/areas	Support the integration of basic and advanced courses into initial and in-service training curricula	on-going	Result 5: Activity 5.5
Jan 12-March 13	Zagreb, Croatia	Support the establishment of a Pilot Centre in Croatia	on-going	Result 5: Activity 5.4
Jan-Dec 12	all countries/areas	Support the implementation of the LEA Training Strategy	on-going	Result 4: Activity 4.1
Jan-Dec 12	Strasbourg	Preparation of a training manual on international police and judicial cooperation against cybercrime	on-going	Result 3: Activity 3.7
14-15 Feb 12	Paris, France	Expert Meeting on Electronic Evidence Guide	completed	Result 4: Activity 4.5
20-24 Feb 12	Zagreb, Croatia	Train the trainers regional course, basic module (Judiciary and Prosecution)	completed	Result 5. Activity 5.3 Result 5. Activity 5.6
27-29 Feb 12	Kyiv, Ukraine	Joint event with CyberCrime@EAP[22]: Regional training course for cybercrime investigators, financial investigators, intelligence units on criminal money flows on the internet	completed	Result 6: Activity 6.2
26 March 12	Bosnia and Herzegovina	Specific workshop on legislation	completed	Result 2: Activity 2.2
28-29 March 12	Skopje, The Former Yugoslav Republic of Macedonia"	Regional workshop to provide advice to prosecution services and ministries of justice regarding the handling of international cooperation requests	completed	Result 3: Activity 3.5
30 March 12		3rd Steering Committee Meeting	completed	All results

[22] Joint regional project of the European Union and the Council of Europe on cooperation against cybercrime under the Eastern Partnership Facility CyberCrime@EAP)
For more information see: www.coe.int/cybercrime

April-May 12	All	Basic Training Course for judges and prosecutors Albania (16-18 April, 2012); BIH (9-11 May, 2012); Croatia (11-13 April, 2012); Kosovo* (19-21 April, 2012); Montenegro (23-25 April, 2012); Serbia (17-19 May, 2012); Turkey (2-4 May, 2012); "The FYR Macedonia" (26-28 April, 2012)	completed	Result 5. Activity 5.6
April – Dec 12	Strasbourg	Develop training modules for advanced training (module 2) courses and make them available in local languages	on-going	Result 5: Activity 5.2
9 May 12	Sarajevo, Bosnia and Herzegovina	Meeting with the TEAM for tracking of implementation of criminal legislation - support of amendments to legislation	completed	Result 2: Activity 2.2
15-16 May 12	The Hague	Participation in the ECTEG Meeting	completed	Result 4: Activity 4.1
29-31 May 12	Germany	Expert Meeting on Electronic Evidence Guide	completed	Result 4: Activity 4.5
May-June 12	Strasbourg	Recommendations and legal advice provided to draft legislative amendments in Bosnia and Herzegovina	completed	Result 2: Activity 2.2
4-8 June 12	Strasbourg	Participation in the Octopus Conference and the Committee of the Convention (T-CY)	planned	All results
		International workshop on trans-border access to data	planned	Result 4: Activity: 4.5
		International workshop on public-private information exchange	planned	Result 7. Activity: 7.4
		Side event on electronic evidence	planned	Result 4: Activity: 4.5
June/July 12	Croatia	Regional workshop to finalise the basic judicial training pack	planned	Result 5: Activity: 5.1
June 12	Dublin, Ireland	MSc programme: Residential workshops at UCD	planned	Result 4: Activity 4.6
July 12	Project areas	Advanced Training Course (Judiciary and Prosecution)	planned	Result 5. Activity 5.6
4-5 Sep 12	"The Former Yugoslav Republic of Macedonia"	Workshop on electronic evidence (legal and practical aspects) for institutions of the criminal justice chain (investigators, forensic experts, prosecutors, judges) (in cooperation with CyberCrime@EAP)	planned	Result 4: Activity: 4.5
6 Sep 12	"The Former Yugoslav Republic of Macedonia"	4th Steering Committee Meeting	planned	All
Oct/Nov 12	All countries/areas	Carry out a cycle of regional assessments		Result 8: Activity 8.2

Sep 12-Jan 13	Strasbourg	Drafting of an agreement on regional priorities regarding cybercrime taking into account European policies based on the results of assessment visits (September - October 2012) and adopted reports (October 2012)	planned	Result 1: Activity 1.3
Oct/Nov 12	Turkey, "The Former Yugoslav Republic of Macedonia", Croatia, Kosovo*	Advanced Training Courses for judges and prosecutors	planned	Result 5: Activity: 5.6
Oct 12/Feb 13	TBD	Train the trainers regional course 1 training course for law enforcement		Result 4: Activity 4.3
5 Nov 12	Baku, Azerbaijan	Workshop on safeguards and conditions (in cooperation with Cybercrime@EAP)		Result 1: Activity 1.3
6-9 Nov 12	Baku, Azerbaijan	Participation in the Internet Governance Forum		Result 1: Activity 1.3; All results
Nov 12	Istanbul, Turkey	Regional workshop to support the establishment of trusted fora for regular information exchange between financial investigators, FIU and the private sector (including financial sector) (in cooperation with CyberCrime@EAP)		Result 6: Activity 6.3
		Regional meeting for the training of LEA and ISP staff responsible for cooperation and for developing standard procedures for cooperation		Result 7: Activity 7.4
Dec 12	Lyon/Paris	Study visits to Interpol and French HTCU		Result 3: Activity 3.3
Jan 13	Turkey	Regional workshop on effectiveness of the legislation		Result 2: Activity 2.1
Jan 13	TBD	Regional conference on the assessment reports and regional agreement		Result 1: Activity 1.4, Activity 1.3 Result 8: Activity 8.3
Feb 13	Serbia	Regional training meeting on international judicial cooperation		Result 3: Activity 3.6
Mar 13	Romania	Study visit to Romania		Result 3: Activity 3.2
Apr 13	TBD	Regional conference (also closing event)		Result 8: Activity 8.3

7.3 Indicative action plan

Activity	*Year 1 (Nov 2010 – Oct 2011)*												*Year 2 (Nov 2011 – Oct 2012)*												*Year 3 (Nov 12-Apr 13*					
Month	11	*12*	*1*	*2*	*3*	*4*	*5*	*6*	*7*	*8*	*9*	*10*	*11*	*12*	*1*	*2*	*3*	*4*	*5*	*6*	*7*	*8*	*9*	*10*	*11*	*12*	*1*	*2*	*3*	*4*
Launching conference																														
Steering group meetings																														
Project evaluation																														
Closing conference																														
Result 1: Cybercrime policies and strategies																														
1.1 Situation report																														
1.2 Regional workshop for policy- and decision-makers/prepare report on safeguards.																														
1.3 Drafting agreement																														
1.4 Follow up high-level workshop																														
Result 2: Legislation																														
2.1 Regional review																														
2.2 Advice on legislation																														
2.3 Online resource																														
Result 3: Regional and international cooperation																														
3.1 Advice on 24/7 CP																														
3.2 Advice on HTCU																														
3.3 Interpol NCRP																														
3.4 Training meetings 24/7 and HTCU																														
3.5 Advice on MLA																														
3.6 Training meetings for prosecution and MoJ																														
3.7 Training manual																														
Result 4: Law enforcement training strategy																														

Activity	*Year 1 (Nov 2010 – Oct 2011)*												*Year 2 (Nov 2011 – Oct 2012)*												*Year 3 (Nov 12-Apr 13*					
Month	11	*12*	*1*	*2*	*3*	*4*	*5*	*6*	*7*	*8*	*9*	*10*	*11*	*12*	*1*	*2*	*3*	*4*	*5*	*6*	*7*	*8*	*9*	*10*	*11*	*12*	*1*	*2*	*3*	*4*
4.1 Proposal for strategy																														
4.2 Training trainers																														
4.3 Training course																														
4.4 Centre of excellence																														
4.5 Multi-disciplinary training courses																														
4.6 Masters programme																														
Result 5: Judicial training																														
5.1 Analysis of training systems																														
5.2 Develop training modules																														
5.3 Training trainers																														
5.4 Pilot centre for judicial training																														
5.5 Training curricula																														
5.6 Training courses																														
Result 6: Crime proceeds																														
6.1 Typology meetings																														
6.2 Joint training courses																														
6.3 Trusted fora																														
Result 7: LEA-ISP cooperation																														
7.1 Assessments																														
7.2 Regional meeting																														
7.3 MoUs																														
7.4 Regional training meetings																														
Result 8: Regional progress assessments																														
8.1 Methodology																														
8.2 Assessment cycle																														
8.3 Regional meeting for adoption of reports																														

7.4 Financial situation (21 May 2012)

Contract value:	2 777 778.00 €	
EU Contribution:	2 500 000.00 €	90%
CoE Contribution:	277 778.00 €	10%
Total payments received:	2 225 204.67 €	
Balance pending:	27 4 795.33 €	
Programme implementation (Actual expenses):		
a. Total expenditure level:	1 455 388.00 €	52.39 %
- amount spent	1 152 515.00 €	
- amount committed	302 873.00 €	
b. Expenditure level relative to work plan (amount spent and committed/total budget elapsed contract duration):		26.20%
Remaining budget:	1 322 390.00 €	