Project Fiche: No. 6

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

@CyberCrime

1. Basic information

1.1	**CRIS Number:**	*2010/xxx-xxx*
1.2	**Title:**	Regional Cooperation in Criminal Justice: Strengthening capacities in the fight against cybercrime (@CyberCrime)
1.3	**ELARG Statistical code:**	01.24 - Justice, freedom and security
1.4	**Location** and Beneficiaries	Western Balkans: Albania, Bosnia and Herzegovina, Croatia, the former Yugoslav Republic of Macedonia, Montenegro, Serbia as well as Kosovo under UNSCR 1244/99 Turkey

Implementing arrangements:

1.5	**Contracting Authority (EC):**	European Community represented by the Commission of the European Communities on behalf of the Beneficiaries.
1.6	**Implementing Agency:**	Not applicable
1.7	**Beneficiary:**	The main beneficiaries are criminal justice authorities (judges, prosecutors and law enforcement agencies, 24/7 points of contact and financial investigators, ministries, parliaments or other institutions involved in cybercrime legislation, private sector representatives, including in particular service providers and the financial sector.

[1] Cybercrime is understood as "criminal acts committed using electronic communications networks and information systems or against such networks and systems". The term cyber crime is applied to three categories of criminal activities. The first covers traditional forms of crime such as fraud or forgery, though in a cybercrime context relates specifically to crimes committed over electronic communication networks and information systems. The second concerns the publication of illegal content over electronic media. The third includes crimes unique to electronic networks, i.e. attacks against information systems, denial of service and hacking. Common to each category of crime is that they may be committed on a mass-scale and with a great geographical distance between the criminal act and its effects. Consequently the technical aspects of applied investigative methods are often the same (Communication from the Commission "Towards a general policy on the fight against cyber crime" of 22 May 2007, COM(2007) 267 final).

Financing:

1.8 Overall cost (VAT excluded)[2]: EUR 2 777 778

1.9 EC contribution: EUR 2 500 000

1.10 Final date for contracting: 30 November 2011

1.11 Final date for execution of contracts: 30 November 2013

1.12 Final date for disbursements: 30 November 2014

2. Overall Objective and Project Purpose

2.1 Overall Objective

Improve Beneficiaries' capacities to prevent and combat cyber crime.

2.2 Project purposes

To strengthen cross-border and international operational cooperation between law enforcement and judicial authorities of the Beneficiaries and EU Member States in investigations and prosecutions of cybercrime.

2.3 Link with AP/NPAA / EP/ SAA[3]

This project takes into account the objectives and priorities set out in the European and Accession Partnerships with the Beneficiaries, which contain relevant provisions on justice, freedom and security and provide the long-term basis for continued cooperation in the field. The 2008 European and Accession Partnerships confirm the importance of regional cooperation in the fight against organised crime and terrorism.

Regarding regional issues and international obligations, the Beneficiaries still need to enhance cooperation with their neighbours, notably on cross-border cooperation, the fight against organised crime, trafficking and smuggling. In the context of organised crime, stronger trans-national cooperation should be ensured and the legal provisions prohibiting the extradition of nationals and as well as the transfer of serious criminal proceedings amended.

Albania
In Albania organised crime remains a very serious problem. Efforts against organised crime remain hampered by corruption and weak witness protection. IT problems hinder the use of criminal intelligence. Strengthening the rule of law, reform of the judicial system and the fight against corruption and organised crime are key priorities of the reform process in Albania.

Bosnia and Herzegovina
In the absence of a revised strategy, Bosnia and Herzegovina needs to prepare and implement all the action plans provided for by the national strategy to combat organised crime and corruption and

[2] The total cost of the project should be net of VAT and/or other taxes. Should this not be the case, the amount of VAT and the reasons why it should be considered eligible should be clearly indicated.

[3] AP = Accession Partnership; NPAA = National Programme for the Adoption of the Acquis (for Candidate Countries), National Action Plan (for Potential Candidates); EP= European Partnership; SAA = Stabilisation and Association Agreement

reinforce international cooperation with law enforcement agencies, including the correct implementation of international conventions.

Croatia
Considerable efforts are still needed to ensure administrative and enforcement capacity, particularly in terms of inter-agency cooperation as well as to prevent corruption and to fight organised crime.

Kosovo
The fight against organised crime remains a major challenge. The legislative framework to tackle organised crime is still incomplete, particularly in the area of witness protection, undercover agents, confiscation of assets, the anti-mafia law and the law on organised crime itself. There is a need to improve the effectiveness of investigations of crime; strengthen investigative and internal control capacities of the Kosovo Police and strengthen its leadership; fight against organised crime and terrorism; further strengthen local capacity in the organised crime directorate within the Kosovo Police Service; and ensure that the Financial Intelligence Centre effectively fulfils its role in collecting and analysing data in relation to money laundering.

Montenegro
Money laundering remains an area of serious concern. Police capacities are limited and there is not yet a proper monitoring of financial transactions beyond the banking system, especially in relation to real estate and foreign investment. There is a need to further strengthen the professional capacity of the police, specialised training, and development of intelligence and risk analysis tools. Efforts to fight corruption and organised crime need to be enhanced. Montenegro has to establish efficient institutional mechanisms for inter-agency cooperation and to upgrade the capacity of the police department in the fight against organised crime; upgrade capacity to use special investigative means in line with appropriate guarantees and strengthen criminal intelligence; adopt the legislation and develop the capacity to seize assets and proceeds of crime; increase the efficiency of international cooperation and implementation of the relevant international conventions on terrorism and preventing and fighting organised crime; improve cooperation and the exchange of information between all branches of the security services and with other states; and prevent the financing and preparation of acts of terrorism.

Serbia
Some progress has been made in fighting organised crime. However, organised crime continues to pose a serious problem for Serbia and more concerted efforts are needed. The action plan to implement the national strategy on fighting organised crime has not been adopted and the specialised police services lack the necessary capacity to carry out their duties fully. There has been little progress in the protection of personal data and current legislation is not in line with European standards. International police cooperation and the capacities of the specialised police services to investigate financial crime remain insufficient. Owing to the large number of police departments involved in the fight against organised crime, internal coordination is a challenge. Final convictions in organised crime cases are rare. A common database on information related to organised crime has not been set up. Preparations in the area of the fight against organised crime remain at an early stage, which is a matter of concern and affects the rule of law and the business environment.

The former Yugoslav Republic of Macedonia
Police cooperation and fight against organised crime remains a serious concern in the country. The former Yugoslav Republic of Macedonia needs to further intensify the fight against organised crime, notably by increasing the number of investigations with the use of special investigative measures and by creating an integrated intelligence system for inter-agency use in the fight against organised crime, including trafficking in human beings, arms and drugs. An action plan for setting up a National Intelligence Database (NID) to connect law enforcement agencies is currently being

implemented. The feasibility study has already been finalised and approved and the tender procedures for the setting up of the NID are planned to start by the end of 2009. Amendments to the Criminal Code including, among others, provisions relevant for the implementation of the Council of Europe Convention on Cybercrime and its Additional Protocol on Racism and Xenophobia are currently undergoing parliamentary procedures.

Turkey

According to the latest Progress Report, key pending issues are related to effective implementation of relevant Council of Europe conventions, especially on mutual legal assistance and on extradition. Turkey has not signed key international conventions, such as the Second Additional Protocol to the Council of Europe Convention on mutual legal assistance or the Convention on cybercrime. Following adoption of a Law on cybercrime, an internet department was established under the telecommunications authority to take charge of monitoring, supervision and coordination and some implementing legislation was adopted.

This project proposal addresses the areas defined in the revised Accession Partnership (AP) and the National Program for the Adoption of the Acquis (NPAA) for Turkey's accession to the EU, as follows:

Link with AP: The Accession Partnership Document (2008) states as Short-Term Priorities, under Chapter 24 "Justice, freedom and security section": Implement the national strategy on organised crime; strengthen the fight against organised crime, drugs, trafficking in persons, fraud, corruption and money-laundering.

Link with NPAA: Priority 24.1 – Strengthening and improving the judicial and administrative capacity of the law enforcement forces and continuing to adopt, implement status and function of these bodies to meet EU Standards.

2.4 Link with MIPD

The IPA Multi-beneficiary Multi-annual Indicative Planning Document (MIPD) 2009-2011[4], section 2.3.1.3.3 – Fight against organised crime, corruption, terrorism, trafficking and smuggling, identifies support for regional cooperation between law enforcement agencies and judicial authorities to fight organised crime and terrorism, complementing efforts at a national level, particularly as it facilitates networking and sharing of best practices and lessons learned in the region. More specifically, the MIPD mentions that regional judicial cooperation programme will support enhanced cooperation in prosecution and investigation on criminal matters, the development of efficient communication procedures and mechanisms to exchange information and transfer proceedings, mutual assistance in penal matters, the approximation of judicial systems and legal frameworks towards EU standards and the *acquis,* networking as well as sharing of best practices and lessons learned in the region, the establishment of harmonised guidelines and protocols for the sharing of relevant information across borders thus building upon the achievements made by national projects and other regional initiatives.

3. Description of project

3.1 Background and justification

Organised crime and cybercrime

[4] COM(2009) 4518

Given the reliance of societies on information and communication technology, cybercrime is of increasing concern to many countries, including the Beneficiaries. Since serious and any other crime involve in many cases the use of Information and Communication Technologies (ICT) in one way or the other, law enforcement and criminal justice authorities need to be able to deal with electronic evidence. Furthermore, cybercrime is increasingly organised and aimed at generating criminal proceeds. Links between organised crime and cybercrime include that:

- ICT facilitate offences by organised criminal groups and networks, in particular economic crime;
- ICT create vulnerabilities at all levels of society and the economy that are exploited by criminal groups;
- ICT facilitate logistics, anonymity and reduce risks of criminal groups;
- ICT are used for money laundering;
- ICT facilitate global outreach of criminal groups;
- ICT shape criminal groups that increasingly take the form of networks.

Another risk is the terrorist use of the internet and threats against ICT. This may take the form of denial of service, attacks against critical infrastructure, recruitment, training or propaganda for terrorism, financing of terrorism or the use of ICT by terrorist groups for logistical purposes. Measures against organised and economic crime and other forms of serious crime, including terrorism, therefore need to include measures against cybercrime. As cybercrime is the most transnational of all crimes, efficient regional and international cooperation is required.

Convention on Cybercrime[5]

The Communication from the Commission "Towards a general policy on the fight against cyber crime" of 22 May 2007[6] and the Justice and Home Affairs Council Conclusions of 8-9 November 2007 expressed strong support to the Council of Europe Convention on Cybercrime in Europe and elsewhere around the world[7]. Furthermore, the Council conclusions of 27 November 2008 on a concerted work strategy and practical measures against cybercrime[8] state that that it is important to combat the various elements of cybercrime and invite the Member States and the European Commission to determine a joint working strategy, taking into account the content of the Council of Europe Convention on Cybercrime.

The Convention on Cybercrime serves as a framework of reference, and provides for:

- Substantive criminal law issues, that is, conduct that constitutes a criminal offence (illegal access and interception, system and data interference, misuse of devices, child pornography, computer-related fraud and forgery, copyright infringements and others);

[5] (CETS No.: 185) The Convention is the first international treaty on crimes committed via the Internet and other computer networks, dealing particularly with infringements of copyright, computer-related fraud, child pornography and violations of network security. It also contains a series of powers and procedures such as the search of computer networks and interception. Its main objective, set out in the preamble, is to pursue a common criminal policy aimed at the protection of society against cybercrime, especially by adopting appropriate legislation and fostering international co-operation. The Convention on Cybercrime is the predominant European and international instrument in this field.

[6] COM(2007) 267 final

[7] Council: i) Underlines the confidence placed in the Council of Europe Convention of 23 November 2001 on Cybercrime, supports and encourages implementation of the measures thereof and calls for the widest possible participation by all countries; ii) Attaches the greatest importance to promoting cooperation with non-member countries in preventing and combating cybercrime, more specifically, given the pivotal role of the Council of Europe Convention on Cybercrime by supporting the introduction of that globally oriented legal framework, in liaison with the Council of Europe, especially in countries where development and technical assistance is being provided.

[8] OJEU2009/C 62/05

- Procedural law issues, that is, measures for more effective investigations of any offence committed by means of a computer system or evidence of which is in electronic form. These procedural measures can, for example, be used in the case of terrorism, money laundering, trafficking in human beings, corruption or other serious crimes where ICT are involved (ie involvement of electronic evidence of the crime).
- Efficient international cooperation with general principles of cooperation (that is, general principles on international cooperation, principles related to extradition, principles related to mutual legal assistance, spontaneous information etc.) as well as specific provisions for more effective cooperation. These permit parties to the Convention to apply procedural tools also internationally. This Section also provides for the creation of a network of contact points which are available on a 24/7 basis to facilitate rapid cooperation.

Regional law enforcement and judicial cooperation

Regional law enforcement and judicial cooperation constitute an important part of the efforts to increase the efficiency of the fight against organised crime, in particular considering the trans-national nature of cyber crime. Regional actions in the fight against cyber crime are essential not only between the Beneficiaries, but also with international partners.

The Communication from the Commission on the Western Balkans of 5 March 2008[9] outlines that cooperation in the field of justice, freedom and security, notably in combating organised crime and corruption, are of particular importance for the Western Balkans and a core priority for their European agenda. The fight against corruption and organised crime is also defined as a top priority in the Enlargement Strategy and Main Challenges 2008-2009[10]. The Justice and Home Affairs Council meeting of 4-5 June 2009 took note of the EU Strategy and Action Plan to Combat Terrorism, in particular the importance to prevent the development of violent extremist websites. Terrorism and organised crime represent one of the most serious attacks on democracy, the rule of law and the area of freedom and security, whose development and reinforcement are essential EU objectives.

3.2 Assessment of project impact, catalytic effect, sustainability and cross border impact

Added value: Considering that cybercrime is the most transnational of all crimes, efficient regional and international cooperation is required. International prosecutions on the basis of cross-border law enforcement cooperation need to be increased through the strengthening of cross-border and international operational cooperation between law enforcement and judicial authorities of the Beneficiaries and EU Member States in investigations and prosecutions of cybercrime. Full implementation of the Convention on Cybercrime will also allow the Beneficiaries to cooperate with other non-European countries that are parties to the Convention and that are major stakeholders with regard to information and communication technologies. As most forms of crime today entail evidence on computer systems, the project will allow criminal justice authorities to cooperate with each other more effectively not only with regard to cybercrime in the narrow sense but also with respect to many other types of serious crime.

Impact: The project will have major impact on a variety of sectors varying from commerce to public order and to national security. In addition, transnational and cross border security will be considerably improved. Another important impact is that fight against cybercrime will be strengthened as the Beneficiaries will have a stronger and harmonised legal framework, up-to-date practices, well-trained staff and better skilled investigators, prosecutors and judges, closer cooperation between law enforcement and internet service providers, active 24/7 points of contact

[9] COM(2008) 127, 05.03.08
[10] COM(2008) 674 final, 05.11.08

and a full implementation of the Convention on Cybercrime. This will increase the security of information and communication technologies and thus contribute to enhanced trust in the information society.

The project will be regularly monitored and the performance evaluated to allow for the relevant readjustments. Action plans should be developed to assess progress. Several methods will be used to conduct performance monitoring, in particular regular implementation reviews on specific objectives and related activities and results and external monitoring via the European Commission Results Oriented Monitoring. Regular briefing sessions and reports are planned. Evaluation during implementation and/or at the end of the project may also take place.

Given the amount of coordination and information exchange required to counteract organised crime successfully, wide-ranging international support is crucial to establish effective prevention and response mechanisms. The project will contribute positively to coordination at a regional level although actual results in terms of impact in countering such crime are difficult to evaluate.

Catalytic effect: Most Beneficiaries are already members of international organisations and all have a good number of bilateral cooperation agreements. Training, study tours, workshops and seminars organised under this project will contribute to increasing interaction between the relevant services in each Beneficiary and across the region. The project should also be seen as a strong regional catalytic tool for law enforcement cooperation and for the identification and neutralisation of common cyber threats related to organised crime and terrorism. Strengthening the administrative and investigative capacities will also accelerate investigations, national and international cooperation among law enforcement agencies and the judicial authorities.

The project is highly appropriate to address social-cultural aspects. The fight against cyber crime is not only for the benefit of the Beneficiaries' authorities but also for their citizens who are increasingly participating in the information society. Given the nature of modern organised crime, and in particular cyber crime, the project is also highly beneficial for neighbouring countries and those countries that are linked with the criminal operations.

Sustainability: The potential sustainability of this project will vary in the region, depending upon the related stages of development of the services, local funding capacities and operational capabilities in terms of equipment and the need for extensive external/international support. The implementation of the project should result, *inter alia*, in amended/drafted laws, bylaws, strategy, action plans and working standards in accordance with the *acquis*, increased number of staff trained and working groups continuously functional and making decisions, opinions, proposals etc.

Ownership will depend on the relative development of each Beneficiary regarding, not least the capabilities of their laws, structures and services to fight organised crime.. Local personnel must be as far as possible involved at both national and regional levels.

3.3 Results and measurable indicators

Improved capacity and facilitated coordination and operational cooperation between law enforcement and judicial authorities of the Beneficiaries and EU Member States to fight cybercrime.

Specific results

Results and measurable indicators in relation to activity 1

1. *Harmonisation of legislation.* Amendments are available to bring relevant legislation fully in line with the EU *acquis*, in particular the Convention on Cybercrime and its Protocol on Xenophobia and Racism and related international standards on data protection, and thus harmonisation of legislation among the Beneficiaries.

Measurable indicators:

- Number and quality of laws drafted and adopted;
- Compliance of (draft) domestic legislation with the EU *acquis*, in particular the Convention on Cybercrime and its Protocol;
- Number of workshops organised and legal opinions prepared.

Results and measurable indicators in relation to activity 2

2. *Regional law enforcement and judicial cooperation.* Enhanced cross-border and international operational law enforcement and judicial cooperation, including exchange of information and best practices, for the purposes of investigations or proceedings concerning criminal offences related to cybercrime[11] and electronic evidence (extradition, mutual assistance, 24/7 contact point network for information exchange, cooperation between high-tech crime units).

Measurable indicators:

- Ratio of prosecutions and convictions for cyber crime (before and after the project);
- Number of cases where Beneficiaries cooperate with each other in cyber crime criminal proceedings;
- Number and timeliness of requests sent/received by 24/7 points of contact, and police units;
- Number and timeliness of requests for judicial cooperation sent/received by prosecutors, courts, Ministries of Justice;
- Number of joint initiatives/operations developed;
- Comparative analyses and exchange of experience on the functioning of high-tech crime units.

Results and measurable indicators in relation to activity 3

3. *Cybercrime training platform*. Pilot cybercrime training platform created and coordinated and interlinked training programmes for law enforcement authorities, prosecutors and judges from the Beneficiaries concerning investigation procedures, prosecution and adjudication of criminal offences related to cybercrime organised, in cooperation and coordination with Europol.

Measurable indicators:

- Number of persons trained;
- Quality and dissemination of training material;
- Training concepts developed and adopted for law enforcement, prosecutors and judges in coordination with the Europol training working group;
- Training materials available and translated for law enforcement, prosecutors and judges;
- Number of pilot training events organised;
- Level of institutionalisation of training platform and related cybercrime training.

[11] Reference to Chapter 3 of the Convention of Cybercrime: International cooperation.

Results and measurable indicators in relation to activity 4

4. *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.

Measurable indicators:

- Number of financial investigators who have received training in special procedures in cyber crime investigation;
- Number of financial investigations related to the internet;
- Agreements concluded between high-tech crime units, FIUs and the financial sector;
- Number of regional events to exchange good practices.

Results and measurable indicators in relation to activity 5

5. *Cooperation between law enforcement experts and Internet Service Providers* (ISPs) in investigations related to cybercrime through the application of national legislation and other relevant international instruments reinforced (cross-sector information exchange will be considered also in the light of existing rules on data protection).

Measurable indicators:

- Memoranda of understanding between ISPs and law enforcement agreed upon in each Beneficiaries;
- Level of implementation of the law enforcement – ISP guidelines of the Council of Europe and the JAI Council conclusions of November 2008;
- Number and timeliness of requests sent/received by law enforcement to ISPs;
- Number of regional events to exchange good practices and facilitate cooperation.

3.4 Activities:

Activity 1: Review legislation against the Convention on Cybercrime of the Council of Europe, organise workshops on cybercrime legislation, and regional/international conferences on good practices regarding cybercrime legislation.

Activity 2: Develop cross-border and international operational law enforcement and judicial cooperation and networking among the Beneficiaries, and with EU Member States, through the strengthening of the capacities of the 24/7 international police contact point network for information exchange, sharing of best practices and lessons learned, the establishment of harmonised law enforcement standards and procedures, for the purposes of investigations or proceedings on criminal offences related to cybercrime; carry out studies and organise regional workshops to prepare an analysis of high-tech crime units and draft recommendations for their strengthening.

Activity 3: Set-up a pilot cybercrime training platform for law enforcement experts on cybercrime investigations and forensic computing from the Beneficiaries, in cooperation with experts from EU Member States, as well as from Europol, the European Police College (CEPOL), and the European Judicial Training Network (ETJN), develop training concepts and organise training for prosecutors and judges on cybercrime investigations and electronic evidence.

Activity 4: Upgrade the capacity of financial investigators and officials of Financial Intelligence Units (FIU) providing training on analysis and investigation of criminal proceeds flows on the internet involving the Beneficiaries, organising workshops in financial investigation involving information and communication technologies, developing cooperation procedures/agreements between financial investigators, FIU and the private sector (including financial sector).

Activity 5: Organise seminars on cooperation methods between law enforcement authorities and Internet Service Providers (ISPs), workshops for law enforcement authorities to develop methods for cooperation with Internet Service Providers and vice-versa, including training on data protection standards in the Beneficiaries, seminars on the establishment of formal partnerships between law enforcement authorities and ISPs.

3.5 Linked activities

Prior and ongoing Regional or IPA Multi-beneficiary Programmes

The CARDS regional project 2002 – 2003 "*Development of Reliable and Functioning Policing Systems and Enhancing of Combating Main Criminal Activities, and Police Cooperation - CARPO*" provided assistance in developing reliable policing systems and tools against economic and organised crime in the Western Balkans. Important components of that project were the strengthening of capacities for financial investigations, for cross-border cooperation as well as for the use of special investigative techniques.

The ongoing CARDS 2006 regional project "*Support to Prosecutors' Network in South Eastern Europe*" includes a small number of activities related to cooperation against cybercrime (ie training on cybercrime for prosecutors and judges; enhancing the effectiveness of international co-operation against cybercrime).

The ongoing 30-month CARDS 2005 regional project, "*ILECUs*", supports the creation of special international law enforcement coordination units in the Beneficiaries with a view to supporting the exchange of information in international investigations and facilitating contacts on an operational level. These units will be integrated in national criminal intelligence models and supported by proper data protection and confidentiality regimes.

The ongoing CARDS 2006 regional project "*Development of monitoring instruments for judicial and law enforcement institutions in the Western Balkans*" will assess and commence improvement of the collection, analysis and use of police and judicial statistics.

National programmes and donor activities

Important police development actions, focusing on operational capacities, have been undertaken under EU Member States bilateral assistance. Networks of liaison officers drawn from the EU Member States have been established in the Beneficiaries. Police and judicial reform projects are also implemented at national level under the EC Twinning mechanism. Interpol, Europol, Eurojust, CEPOL, ETJN as well as the SECI Centre closely cooperate with EU Member States and are developing cooperation and working arrangements with the Beneficiaries in the area of police and criminal justice cooperation inter alia to fight organised crime in the region, including 'computer crime'[12]. Other financial measures support the development of key capacities in each Beneficiary including setting up financial intelligence units and specialised teams of prosecutors and judges to deal with organised crime cases.

[12] In the Europol Convention 'computer crime' is listed as 'serious form of international crime which Europol could deal with in addition to those already provided for in Article 2(2) in compliance with Europol's objective as set out in Article 2'. The general competence of Eurojust covers, inter alia, computer crime.

As regards other European and international tools and legal instruments touching upon issues related to cybercrime, special attention and focus are to be devoted to the predominant work of the Council of Europe, in particular the Convention on Cybercrime which entered into force on 1 July 2004[13]. The Convention contains common definitions of different types of cyber crime and lays the foundation for a functioning judicial cooperation between contracting states. A project against cybercrime implemented by CoE worldwide came to an end in February 2009. The second phase has started in March 2009 and will end in June 2011.

The European Commission has actively participated in international fora and cooperation initiatives, i.e. the G8 Lyon-Roma High-Tech Crime Group and Interpol-administered projects. The Commission is in particular closely following the work of the network of contact points which are available on a 24/7 basis to facilitate rapid international cooperation. The G8 network constitutes a mechanism to expedite contacts between participating states, with 24-hour points of contact for cases involving electronic evidence, and those requiring urgent assistance from foreign law enforcement authorities.

EC national programmes (CARDS, IPA)

Albania

The EU is providing technical assistance to the Albanian state police in order to bring them closer to EU standards. With EUR5.5 million, the EC is supporting the police assistance mission of the European Community to Albania ("PAMECA III"), which aims to improve the performance of the Albanian state police structures and to improve the trust of the Albanian citizens into the police force. The project, which shall be implemented until 2011, continues in the light of previous programmes, PAMECA I & II. Assistance has also been provided to the National Agency for Information Society (NAIS) in formulating proposals to the Ministry of Justice for amendments of the Penal Code and Penal Procedure Code in order to implement the Convention on Cybercrime; the proposed amendments were compliant with the EU *acquis*. The proposals have been adopted by the Ministry of Justice and were submitted to Parliament in early October 2008. Parliament adopted the proposed amendments on 27 November 2008.

Bosnia and Herzegovina

Activity 4 (Upgrade the capacity of financial investigators and officials of Financial Intelligence Units) of the Multi-beneficiary IPA 2010 programme "Regional Cooperation in Criminal Justice: Strengthening capacities in the fight against cybercrime" could be linked to the IPA 2007 national programme "Joint Training of SIPA Financial Intelligence Unit and Crime Investigation Unit, Prosecutors, Financial Regulatory Agencies and Institutions" aiming at strengthening the capacity of the Financial Intelligence and Criminal Investigation Units' (FIU and CIU) in investigating money laundering and financing cases and improving the cooperation with Prosecutors and financial regulatory agencies in cases of money laundering and financing terrorism

Croatia

The IPA 2009 HR2009-01-36-01 national programme, entitled "Capacity Building in the Field of Fight against Sexual Exploitation and Sexual Abuse of Children, and on Police Assistance to Vulnerable Crime Victims" has a significant "cyber crime" dimension, related to child pornography.

The former Yugoslav Republic of Macedonia

Police, anti-money laundering and anti-corruption as well as judicial reform projects are implemented at a national level but none of these projects are specifically dealing with cyber crime.

Montenegro

[13] Albania, Bosnia and Herzegovina, Croatia, Serbia and the former Yugoslav Republic of Macedonia have ratified the Convention. Montenegro has signed it, whereas Turkey is expected to do so soon.

Police, anti-money laundering and anti-corruption as well as judicial reform projects are implemented at a national level but none of these projects are specifically dealing with cyber crime.

Kosovo
Police, anti-money laundering and anti-corruption as well as judicial reform projects are implemented at a local level but none of these projects are specifically dealing with cyber crime.
Nevertheless, it is relevant to mention that the European Union Rule of Law Mission in Kosovo (EULEX) is the largest civilian mission launched under the European Security and Defence Policy (ESDP). It assists and supports the Kosovo authorities in the rule of law area, specifically in the police, judiciary and customs areas. It is a technical mission which monitors, mentors and advises. One of the strategic goals of EULEX is to ensure that cases of war crimes, terrorism, organised crime, corruption, inter-ethnic crimes, financial/economic crimes and other serious crimes, as well as property related issues, are properly investigated, prosecuted, adjudicated and enforced according to the applicable law.

Serbia
The joint EC/Council of Europe PACO Serbia Project against Economic Crime (December 2005 – May 2008) contained a specific component on cybercrime. As a result, Serbia ratified the Convention on Cybercrime in March 2009 and established specialised police, prosecution and judicial offices for cybercrime.

Turkey
The IPA 2009 twinning programme "Strengthening the Capacity against Cybercrime" aims to improve the investigative capacity of law enforcement authorities, adjudication capacity of criminal justice authorities by training and to enhance cooperation between national and international public and private sector bodies against cybercrime including exchange of information, expertise, best practices and to contribute to the implementation of the action plan against organised crime. Other completed projects that have directly or indirectly dealt with organised crime and cyber crime are: "Strengthening the Fight against Money Laundering"; "Strengthening the Fight against Organised Crime"; "Strengthening the struggle against money laundering, financial sources of crime and the financing of terrorism"; "Enhancement of the professionalism of the Turkish Gendarmerie in its law enforcement activities".

3.7 Lessons learned

Operational activities: According to the various evaluations and CARDS Monitoring reports, it is necessary to intensify the support to regional operational activities. Operational means, including the safe and secure exchange of data, for increased cross-border cooperation should be developed according to the EU best practices.

Ownership: ‘Ownership' of the projects should be secured at an early stage of the programming process. For the Multi-Beneficiary IPA 2010 "Regional Cooperation in Criminal Justice: Strengthening capacities in the fight against cybercrime (@CyberCrime)" programme coordination and involvement of the Beneficiaries was ensured at the identification phase of the project idea.

Implementation: Although a broad range of specific expertise is required for the regional projects, the contracting of consortia with too many partners for the coming police and judicial cooperation projects should be avoided, as the projects will have a specific and targeted approach, and coordination efforts should not be unnecessarily complicated by a saturation of partners.

Integrated national strategies: An integrated national strategy against organised crime and terrorism is needed, with coordination and cross–sectoral cooperation mechanisms, and with a strong supportive international component.

Ensure sustainability: Police and judicial staff must not only be trained to a high professional level, but also empowered to continue professional work once the programme ends. Proper handover of necessary equipment, information, documentation, curricula etc must be ensured.[14]

Avoid duplication: In order to avoid duplication and unnecessary cost, the best use of existing judicial and law enforcement tools and networks of national bodies has to be considered instead of creating new ones. Functional, thematic cross border networks of law enforcement authorities shall be reinforced to more effectively combat serious crime and prevent terrorism.

When to create new networks: Creation of new networks should be avoided in the field of witness protection. Existing networks and institutions already in charge of cross border co-operation should be supported so that they increase cooperation in the field of witness protection. In general where a gap is identified, programmes should facilitate the creation of regional networks for stakeholders (police, prosecutors, judges) and support the development of other regional and national initiatives in this area. Networks of stakeholders should serve, *inter alia*, as focal points for collecting and disseminating best practices and lessons learned.

Assess state of play: Rather than starting with an overall objective for the region as a whole and then applying a standard methodology, the programme shall start, in collaboration with the Beneficiaries, with assessing the current situation in the Beneficiaries and then tailor the appropriate regional approach based upon their specificities and needs.

Tailored made approach and synergies: The different stages of readiness of the Beneficiaries shall be taken into account during implementation. The project shall draw on the experience of the most advanced Beneficiaries in the alignment process to the *acquis* and develop synergies among them.

Resources and equipment: The most efficient use of available resources should be ensured, rather than providing new hardware. "While many police services will have legitimate requirements for infrastructure and equipment to support capacity-building, such equipment should only be supplied to meet requirements clearly identified in a needs assessment and an accompanying development plan. This should be clearly communicated at the outset of any reform programme or the promise of material resources may detract from or undermine the more pressing business of institutional reform"[15].

[14] OSCE, Implementation of Police-Related Programmes, Lessons Learned in South-Eastern Europe, SPMU Publication Series Vol. 7, Vienna, December 2008

[15] OSCE, Implementation of Police-Related Programmes, Lessons Learned in South-Eastern Europe, SPMU Publication Series Vol. 7, Vienna, December 2008

4. Indicative Budget (amounts in EUR)

				SOURCES OF FUNDING								
			TOTAL EXP.RE	IPA COMMUNITY CONTRIBUTION		NATIONAL CONTRIBUTION					PRIVATE CONTRIBUTION GRANT BENEFICIARY	
ACTIVITIES	IB (1)	INV (1)	EUR (a)=(b)+(c)+(d)	EUR (b)	%(2)	Total EUR (c)=(x)+(y)+(z)	% (2)	Central EUR (x)	Regional/ Local EUR (y)	IFIs EUR (z)	EUR (d)	% (2)
Contract 1	x		2 777 778	2 500 000	*90*	/	/	/	/	/	277 778	10
TOTAL IB			2 777 778	2 500 000	*90*	/	/	/	/	/	277 778	10
TOTAL INV			/	/	/	/	/	/	/	/	/	/
TOTAL PROJECT			**2 777 778**	**2 500 000**	**90**						**277 778**	**10**

Amounts net of VAT

(1) In the Activity row use "X" to identify whether IB or INV

(2) Expressed in % of the **Total** Expenditure (column (a))

5. Indicative Implementation Schedule (periods broken down per quarter)

Contracts	Launch of Call for Proposals	Signature of contract	Project Completion
Contribution Agreement	N/A	Q4 2010	Q1 2013

6. Cross cutting issues

6.1 Equal Opportunity

The project does not directly target equal opportunities but it will respect gender equality, not least through the inputs to upgrade legislation towards EU standards.

6.2 Environment

The most recent criminal phenomenon in South East Europe is related to the environment, i.e. eco-mafia. The programme should also contribute in tackling indirectly this form of organised crime.

6.3 Minorities

Minority and vulnerable groups' concerns will be reflected in all activities under the programme, in particular when it concerns public services, legislative matters and socio-economic development.

ANNEXES

I- Logical framework matrix in standard format

II- Amounts (in EUR) contracted and disbursed per quarter over the full duration of project

III- Description of Institutional Framework

IV - Reference to laws, regulations and strategic documents:

V- Details per EC funded contract (where applicable)

ANNEX I: Logical framework matrix in standard format

LOGFRAME PLANNING MATRIX FOR Project Fiche	**Regional Cooperation in Criminal Justice: Strengthening capacities in the fight against cybercrime @CyberCrime**	CRIS No.: 2010/xxx-xxx
	Contracting period expires: 30 November 2011	Disbursement period expires: 30 November 2014
	Total budget: EUR 2 777 778	IPA budget EUR 2 500 000

Overall objective	**Objectively verifiable indicators**	**Sources of Verification**
To improve Beneficiaries' capacities to prevent and combat cyber crime.	- Number of committed infractions related to cyber crime in the Beneficiaries - Ratio between committed cyber crime infractions and convictions	Reports of the competent authorities Statistical publications Local and national records (MoI, MoJ) SEE OCTA Report

Project purpose	**Objectively verifiable indicators**	**Sources of Verification**	**Assumptions**
Strengthen cross-border and international operational cooperation between law enforcement and judicial authorities of the Beneficiaries and EU Member States in investigations and prosecutions of cybercrime.	- Percentage of organised crime cases in Western Balkans and Turkey where law enforcement co-operation mechanisms were used - Number of joint operations/investigations carried out	Reports of the competent authorities Statistical publications Local and national records (MoI, MoJ) Project reports Monitoring reports Progress reports	Adequate political commitment and financial resources of Beneficiaries Timely and adequate resources available. Efficient cooperation between Beneficiaries and Grant beneficiary

Results	Objectively verifiable indicators	Sources of Verification	Assumptions
Improved capacity and facilitated coordination and operational cooperation between law enforcement and judicial authorities of the Beneficiaries and EU Member States to fight cybercrime. **1.** *Harmonisation of legislation.* Amendments are available to bring relevant legislation fully in line with the EU *acquis*, in particular the Convention on Cybercrime and its Protocol on Xenophobia and Racism and related international standards on data protection, and thus harmonisation of legislation among the Beneficiaries.	- Number and quality of laws drafted and adopted; - Compliance of (draft) domestic legislation with the EU *acquis*, in particular the Convention on Cybercrime and its Protocol; - Number of workshops organised and legal opinions prepared.	Project reports Country profiles Monitoring reports Reports of the Cybercrime Convention Committee SEE OCTA	Draft legislation is adopted by Parliaments
2. *Regional law enforcement and judicial cooperation.* Enhanced cross-border and international operational law enforcement and judicial cooperation, including exchange of information and best practices, for the purposes of investigations or proceedings concerning criminal offences related to cybercrime[16] and electronic evidence (extradition, mutual assistance, 24/7 contact point network for information exchange, cooperation between high-tech crime units).	- Ratio of prosecutions and convictions for cyber crime (before and after the project); - Number of cases where Beneficiaries cooperate with each other in cyber crime criminal proceedings; - Number and timeliness of requests sent/received by 24/7 points of contact, and police units; - Number and timeliness of requests for judicial cooperation sent/received by prosecutors, courts, Ministries of Justice; - Number of joint initiatives/operations developed; - Comparative analyses and exchange of experience on the functioning of high-tech crime units.	Project reports Country profiles Monitoring reports Reports of the Cybercrime Convention Committee SEE OCTA	
3. *Cybercrime training platform.* Pilot cybercrime training platform created and coordinated and interlinked training programmes for law enforcement authorities, prosecutors and judges from the Beneficiaries concerning	- Number of persons trained; - Quality and dissemination of training material; - Training concepts developed	Project reports Country profiles Monitoring reports Reports of the Cybercrime Convention	

[16] Reference to Chapter 3 of the Convention of Cybercrime: International cooperation.

investigation procedures, prosecution and adjudication of criminal offences related to cybercrime organised, in cooperation and coordination with Europol.	and adopted for law enforcement, prosecutors and judges in coordination with the Europol training working group; - Training materials available and translated for law enforcement, prosecutors and judges; - Number of pilot training events organised; - Level of institutionalisation of training platform and related cybercrime training.	Committee SEE OCTA	
4. *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.	- Number of financial investigators who have received special procedures' training in cyber crime investigation; - Number of financial investigations related to the internet; - Agreements concluded between high-tech crime units, FIUs and the financial sector; - Number of regional events to exchange good practices.	Project reports Country profiles Monitoring reports Reports of the Cybercrime Convention Committee SEE OCTA	
5. *Cooperation between law enforcement experts and Internet Service Providers* (ISPs) in investigations related to cybercrime through the application of national legislation and other relevant international instruments reinforced (cross-sector information exchange will be considered also in the light of existing rules on data protection).	- Memoranda of understanding between ISPs and law enforcement agreed upon in each Beneficiaries; - Level of implementation of the law enforcement – ISP guidelines of the Council of Europe and the JAI Council conclusions of November 2008; - Number and timeliness of requests sent/received by law enforcement to ISPs; - Number of regional events to exchange good practices and facilitate cooperation.	Project reports Country profiles Monitoring reports Reports of the Cybercrime Convention Committee SEE OCTA	

Activities	Means	Costs	Assumptions
Activity 1: Review legislation against the Convention on Cybercrime of the Council of Europe, organise workshops on cybercrime legislation, and regional/international conferences on good practices regarding cybercrime legislation. **Activity 2:** Develop cross-border and international operational law enforcement and judicial cooperation and networking among the Beneficiaries, and with EU Member States, through the strengthening of the capacities of the 24/7 international police contact point network for information exchange, sharing of best practices and lessons learned, the establishment of harmonised law enforcement standards and procedures, for the purposes of investigations or proceedings on criminal offences related to cybercrime; carry out studies and organise regional workshops to prepare an analysis of high-tech crime units and draft recommendations for their strengthening. **Activity 3:** Set-up a pilot cybercrime training platform for law enforcement experts on cybercrime investigations and forensic computing from the Beneficiaries, in cooperation with experts from EU Member States, as well as from Europol, the European Police College (CEPOL), and the European Judicial Training Network (ETJN), develop training concepts and organise training for prosecutors and judges on cybercrime investigations and electronic evidence. **Activity 4:** Upgrade the capacity of financial investigators and officials of Financial Intelligence Units (FIU) providing training on analysis and investigation of criminal proceeds flows on the internet involving the Beneficiaries, organising workshops in financial investigation involving information and communication technologies, developing cooperation procedures/agreements between financial investigators, FIU and the private sector (including financial sector). **Activity 5:** Organise seminars on cooperation methods between law enforcement authorities and Internet Service Providers (ISPs), workshops for law enforcement authorities to develop methods for cooperation with Internet Service Providers and vice-versa, including training on data protection standards in the Beneficiaries, seminars on the	The European Commission will conclude a Direct Grant (Contribution Agreement) with the Council of Europe (**no** Joint Management)	EUR 2 500 000	Very good management and communication capacities of Grant beneficiary + knowledge and experience of/in the Beneficiaries Efficient cooperation between Beneficiaries and Grant beneficiary Commitment of judicial and law enforcement services in implementing project activities in a professional manner

establishment of formal partnerships between law enforcement authorities and ISPs.			

ANNEX II: Amounts (in EUR) contracted and disbursed per quarter over the full duration of project

Contracted	**Q4 2010**	**Q1 2011**	**Q2 2011**	**Q3 2011**	**Q4 2011**	**Q1 2012**	**Q2 2012**	**Q32012**	**Q42012**
Contract 1	2 500 000								
Cumulated	**2 500 000**								
Disbursed	**Q1 2011**	**Q2 2011**	**Q3 2011**	**Q4 2011**	**Q1 2012**	**Q2 2012**	**Q3 2012**	**Q4 2012**	**Q1 2013**
Contract 1	1 000 000*				1 250 000**				250 000***
Cumulated	**1 000 000**				**2 250 000**				**2 500 000**

*First instalment of pre-financing (80% of the part of the forecast budget for the first 12 months of project implementation)

**Further annual instalment(s) of pre-financing

***Final payment

ANNEX III Description of Institutional Framework

The authorities responsible of the implementation of the project will be the relevant departments in the Ministries of Interior and Ministries of Justice of the Beneficiaries, including law enforcement agencies and judicial authorities (criminal police, financial investigators, 24/7 contact points, prosecutors' offices, courts) involved in investigation and prosecution of cyber crime cases.

ANNEX IV: Reference to laws, regulations and strategic documents

- Multi-beneficiary Multi-annual Indicative Planning Document 2009-2011
- Commission's Communication of 5 March 2008 "Western Balkans: Enhancing the European perspective"
- Commission's Communication of 5 November 2008 "Enlargement Strategy and Main Challenges 2008-2009" COM(2008) 674 final
- Commission's Communication of 27 January 2006 "The Western Balkans on the Road to the EU: Consolidation Stability and Raising Prosperity"
- Commission's Communication of 22 May 2007 "Towards a general policy on the fight against cyber crime" (COM(2007) 267 final)
- Convention on Cybercrime, CETS No.: 185, Council of Europe
- Justice and Home Affairs Council Meeting of 27-28 November 2008
- Justice and Home Affairs Council Meeting of 4-5 June 2009
- Work Programme of the Czech Presidency, Europe without Barriers, January 2009
- Council Action Oriented Paper on Improving Cooperation on Organised Crime, Corruption, Illegal Migration and Counter-terrorism, between the EU, Western Balkans and relevant ENP countries of 12 May 2006
- Council Decision of 18 February 2008 (2008/210/EC) on the principles, priorities and conditions contained in the European Partnership with Albania and repealing Decision 2006/54/EC
- Council Decision of 18 February 2008 (2008/211/EC) on the principles, priorities and conditions contained in the European Partnership with Bosnia and Herzegovina and repealing Decision 2006/55/EC
- Council Decision of 12 February 2008 (2008/119/EC) on the principles, priorities and conditions contained in the Accession Partnership with Croatia and repealing Decision 2006/145/EC
- Council Decision of 18 February 2008 (2008/212/EC) on the principles, priorities and conditions contained in the Accession Partnership with the former Yugoslav Republic of Macedonia and repealing Decision 2006/57/EC
- Council Decision of 22 January 2007 (2007/49/EC) on the principles, priorities and conditions contained in the European Partnership with Montenegro
- 2008/157/EC: Council Decision of 18 February 2008 on the principles, priorities and conditions contained in the Accession Partnership with the Republic of Turkey and repealing Decision 2006/35/EC
- Council Decision of 18 February 2008 (2008/213/EC) on the principles, priorities and conditions contained in the European Partnership with Serbia including Kosovo as defined by United Nations Security Council Resolution 1244 of 10 June 1999 and repealing Decision 2006/56/EC
- Council and Commission Decision of 13 December 2004 concerning the conclusion of the Stabilisation and Association Agreement between the European Communities and their Member States, of the one part, and the Republic of Croatia, of the other part -

Stabilisation and Association Agreement between the European Communities and their Member States, of the one part, and the Republic of Croatia, of the other part

- Council and Commission Decision of 26 March 2001 concerning the conclusion of the Stabilisation and Association Agreement between the European Communities and their Member States, of the one part, and the former Yugoslav Republic of Macedonia, of the other part - Stabilisation and Association Agreement between the European Communities and their Member States, of the one part, and the former Yugoslav Republic of Macedonia, of the other part
- Council and Commission Decision of 22 May 2006 concerning the conclusion of the Stabilisation and Association Agreement between the European Communities and their Member States, of the one part, and the Republic of Albania, of the other part - Stabilisation and Association Agreement between the European Communities and their Member States, of the one part, and the Republic of Albania, of the other part
- Albania 2008 Progress Report
- Bosnia and Herzegovina 2008 Progress Report
- Croatia 2008 Progress Report
- The former Yugoslav Republic of Macedonia 2008 Progress Report
- Montenegro 2008 Progress Report
- Serbia 2008 Progress Report
- Kosovo 2008 Progress Report
- Turkey 2008 Progress Report

ANNEX V: Details per EC funded contract

To implement these activities, the European Commission will conclude a Direct Grant (Contribution Agreement) with the Council of Europe (**no** Joint Management) based on Article 168(1)(f) of the Implementing Rules of the Financial Regulation. As an International Organisation, Council of Europe has a predominant competence in coordinating and facilitating the development of benchmarks, methodologies and approaches for the fight against cyber crime.

	Type of Contract	**Amount in EUR**	**Duration**
Contract 1	Direct Grant (Contribution Agreement)	2 500 000	24 months

Council of Europe should contribute with a minimum of 10% of the total eligible cost of the project.

Renting costs may be eligible under this IPA programme.